NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

7 January 2008

DOCUMENT
AC/35-D/2001-REV2

NATO SECURITY COMMITTEE

DIRECTIVE on PHYSICAL SECURITY

Note by the Chairman

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

2. This revision reflects approved changes in the area dealing with access to NATO Class I security areas by Individuals from Non-NATO Nations / International Organisations.

3. This document has been approved by the NATO Security Committee under the silence period (AC/35-WP(2007)0008 refers) and will be subject to periodic review.

(Signed) Michael T. Evanoff

Annex: 1

Action Officer: Robert Keil, NOS/POB, Ext. 4084
Original: English

ANNEX 1
AC/35-D/2001-REV2

DIRECTIVE ON PHYSICAL SECURITY

INTRODUCTION

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

(a) security requirements;

(b) physical security measures;

(c) minimum standards for the storage of NATO classified information;

(d) protection against technical attacks; and

(e) physical security of communication and information systems (CIS).

SECURITY REQUIREMENTS

2. In accordance with the requirements of NATO Security Policy, all premises, buildings, offices, rooms, and other areas in which NATO classified information and material is stored and/or handled shall be protected by appropriate physical security measures. In deciding what degree of physical security protection is necessary, account shall be taken of all relevant factors, such as :

(a) the level of classification and category of information;

(b) the quantity and form of the information (hard copy/computer storage media) held;

(c) the security clearance and need-to-know of the staff;

(d) the locally-assessed threat from intelligence services which target NATO and/or its member nations, sabotage, terrorist, subversive or other criminal activities; and

(e) how the information will be stored.

3. Physical security measures shall be designed to:

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

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

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

(d) detect and act upon all security breaches as soon as possible.

PHYSICAL SECURITY MEASURES

4. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and INFOSEC measures, details of which will be found respectively in Enclosures “C”, “E” and “F” of NATO Security Policy and supporting directives. Sensible management of security risks will involve establishing the most efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these areas. Such efficiency and cost-effectiveness is best achieved by defining physical security requirements as part of the planning and design of facilities, thereby reducing the need for costly renovations.

5. Physical security programmes shall be based on the principle of “defence in depth”, and although physical security measures are site-specific, the following general principles shall apply. It is first necessary to identify the locations that require protection. This is followed by the creation of layered security measures to provide “defence in depth” and delaying factors. The outermost physical security measures shall define the protected area and deter unauthorised access. The next level of measures shall detect unauthorised or attempted access and alert the guard force. The innermost level of measures shall sufficiently delay intruders until they can be detained by the guard force. Consequently, there is an interrelationship between the reaction time of the guard force and the physical security measures designed to delay intruders.

6. Regular maintenance of security systems is necessary to ensure that equipments operate at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures and the complete security system. This is particularly important if there is a change in use of the site or elements of the security system. This can be achieved by exercising incident response plans.

Security Areas

7. Areas in which information classified NC and above is handled and stored shall be organised and structured so as to correspond to one of the following:

(a) **NATO Class I Security Area**: an area in which information classified NC and above is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information. Such an area requires:

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

(ii) an entry control system which admits only those individuals appropriately cleared and specifically authorised 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) **NATO Class II Security Area**: an area in which information classified NC and above is handled and stored in such a way that it can be protected from access by unauthorised individuals by controls established internally. Such an area requires:

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

(ii) an entry control system which admits unescorted access only to those individuals who are security cleared and specifically authorised to enter the area. For all other individuals, provision shall be made for escorts or equivalent controls, to prevent unauthorised access to NATO classified information and uncontrolled entry to areas subject to technical security inspection.

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

Access to NATO Class I Security Areas by Individuals from Non-NATO Nations / International Organisations

9. Individuals from non-NATO Nations / International Organisations who, because of their assignment and official duties, need regular interface with NATO staffs may be granted access to a NATO Class I Security area. The following criteria shall be applied to those Individuals:

(a) access is only granted on a case-by-case basis;

(b) Individuals must be escorted at all times;

(c) during the time of the access, all classified NATO information inside the Class I security area must be appropriately secured, or protected, as applicable so that the access to the Class I security area does not automatically constitute access to classified NATO information;

(d) the requirements of Appendix 2 to the Directive “Criteria for Access to NATO Class I/II Security Areas by Individuals from Non-NATO Nations and International Organisations” apply; and

(e) access to Open Storage Areas is prohibited.

Access to NATO Class II Security Areas by Individuals from Non-NATO Nations / International Organisations

10. Individuals from non-NATO nations / International Organisations who, because of their assignment and official duties, need regular interface with NATO staffs may be granted unescorted access to a NATO Class II Security Area. Such individuals may also be assigned office space within a NATO Class II Security Area in order to fulfil their assignment and official duties.

The granting of unescorted access and/or the assignment of office space shall be handled on a case-by-case basis, and shall be in accordance with the criteria set out in Appendix 2 to this Directive.

Administrative Zones

11. An Administrative Zone may be established around or leading up to NATO Class I or Class II security areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

Specific Physical Security Measures

12. This section provides information on various physical security measures and how they can contribute to the security framework of an organisation or site.

Perimeter

13. A perimeter fence will form a useful physical barrier and will identify the boundary of an area requiring security protection. The level of protection offered by a fence will depend on its height, construction, the material used and any additional security features used to increase its performance and effectiveness such as topping, Perimeter Intrusion Detection Systems (PIDS), lighting or CCTV.

14. The effectiveness of any security perimeter will depend, to a large extent, on the level of security at the points of access. Gates shall be constructed to the same security standard as the fence; and some form of access control shall be in place, otherwise the security of the fence will be negated.

Security lighting

15. Security lighting can offer a high degree of deterrence to a potential intruder in addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system. The standard of lighting should, however, meet the minimum requirement of the CCTV and its installation be appropriate to the site conditions.

Intrusion Detection Systems (IDS)

16. Perimeter Intrusion Detection Systems (PIDS) may be used on perimeters to enhance the level of security offered by the fence. PIDS may be installed as covert devices (although this is usually for aesthetic reasons) or overtly to act as a deterrent. PIDS are inherently prone to false alarm and should therefore normally only be used with an alarm verification system such as CCTV.

17. In accordance with the principle of “defence in depth”, IDS may be used in rooms and buildings in place of, or to assist, guards. To be effective, an IDS should have a response force that will react within a reasonable timescale in the event of an alarm being given.

Access Control

18. Control of access may be exercised over a site, a building or buildings on a site or to areas or rooms within a building. The control may be electronic, electro-mechanical, by a guard or receptionist, or physical. A pass or personal recognition system governing the regular staff shall control entry into Class I or II security areas.

Guards

19. The employment of guards can provide a valuable deterrent to individuals who might plan covert intrusion. The guards’ duties and the need for and frequency of patrols shall be decided by considering the level of risk and any other security systems or equipment that might be in place. Guards shall be provided with adequate written guidance to ensure specifically assigned tasks are conducted as required. Guards shall require a means of communication with their control centre.

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

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

Closed Circuit Television (CCTV)

22. CCTV is a valuable aid to security guards in verifying incidents and PID alarms on large sites or perimeters. The effectiveness of such a system will, however, depend on the selection of suitable equipment and its installation and on the monitoring of the control centre. Detailed professional advice shall be sought.

Entry and Exit Searches

23. NATO establishments shall undertake random entry and exit searches which are designed to act as a deterrent to the unauthorised introduction of material into, or the unauthorised removal of NATO classified information from a site or building. Entry and exit searches may be made a condition of entry to a site or building. A warning notice shall be displayed to indicate that random entry and exit searches may be undertaken.

Visitor Control

24. The nationality of the visitor, his/her clearance and need-to-know, and any special control requirements determine whether the visitor shall be permitted escorted or unescorted access to a NATO establishment. The type of control over visitors is described below:

(a) **Escorted**. Visitors who require an escort within an area shall be accompanied at all times. If they need to visit a number of different departments or other members of staff, they shall be formally handed over from one escort to the next with any accompanying documentation. They may be required to wear a pass that identifies them as a visitor; and

(b) **Unescorted**. Visitors who are permitted unescorted entry to an area, or parts of it shall be required to wear a pass that identifies them as a visitor. It should be noted that a visitor pass system is effective only if all regular staff are required to wear a pass.

Approved Equipment

25. For vaults and open storage areas constructed within a Class I or a Class II security area where information classified NC or higher is stored on open shelves or displayed on charts, maps, etc., the walls, floors, ceilings and door(s) with lock(s) must be approved, under the responsibility of the NSA.

MINIMUM STANDARDS FOR THE STORAGE OF NATO CLASSIFIED INFORMATION

26. NATO security policy sets out the minimum standards for the storage of NATO classified information. This section expands upon the security policy.

27. **COSMIC TOP SECRET (CTS).** CTS information shall be stored within a class I or II security area under one of the following conditions :

(a) in a nationally-approved security container with one of the following supplemental controls:

(i) continuous protection by cleared guard or duty personnel;

(ii) inspection of the security container not less than every two hours, at randomly timed intervals, by cleared guard or duty personnel; or

(iii) a nationally-approved Intrusion Detection System (IDS) in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed to remove or break open the security container, or overcome the physical security measures in place.

(b) an open storage area constructed in accordance with Annex to this directive, which is equipped with an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry; or

(c) an IDS-equipped vault in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

28. **NATO SECRET (NS).** NS information shall be stored within a class I or II security area by one of the following methods :

(a) in the same manner as prescribed for CTS information; or

(b) in a nationally-approved security container or vault without supplemental controls; or

(c) an open storage area, in which case, one of the following supplemental controls is required :

(i) the location that houses the open storage area shall be subject to continuous protection by cleared guard or duty personnel;

(ii) cleared guard or duty personnel shall inspect the open storage area once every four hours; or

(iii) an IDS in combination with a response force that will, after an alarm annunciation, arrive at the location within the estimated timeframe needed for forced entry.

29. **NATO CONFIDENTIAL (NC).** NC information shall be stored in the same manner as prescribed for CTS or NS information except that supplemental controls are not required.

30. **NATO RESTRICTED (NR).** NR information shall be stored in a locked container.

Control of keys and combinations

31. Keys of security containers shall not be taken out of office buildings. Combination settings of security containers shall be committed to memory by individuals needing to know them. Spare keys and a written record of each combination setting for use in an emergency shall be held in sealed opaque envelopes by the government department or NATO civil or military body concerned. Working and spare security keys shall be kept in separate containers. The record of each combination shall be kept in a separate envelope. The keys, combinations and the envelopes shall be given security protection no less stringent than the information to which they give access.

32. Knowledge of combination settings of security containers shall be restricted to the smallest possible number of individuals. As a minimum, settings shall be changed :

(a) on first being taken into use;

(b) whenever a change of personnel possessing the combination occurs,

(c) whenever a compromise has occurred or is suspected; and

(d) at intervals not exceeding 12 months.

Physical protection of Copying and Telefax machines

33. Copying and telefax machines shall be physically protected to the extent necessary to ensure that only authorised individuals can use them and that all NATO classified information is controlled in accordance with the requirements of NATO security policy and supporting directives.

PROTECTION AGAINST TECHNICAL ATTACKS

Eavesdropping

34. Offices or areas in which information classified NS and above is regularly discussed shall be protected against passive and active eavesdropping attacks, by means of sound physical security measures and access control, where the risk warrants it. The responsibility for determining the risk shall be co-ordinated with technical specialists and decided by the appropriate security authority.

35. **Protection against passive eavesdropping attacks** - the leakage of NATO classified information via insecure communications or by overhearing directly or by unintentional electromagnetic emissions - may involve seeking technical security advice as described in paragraph 36 below and may involve soundproofing walls, doors, floors and ceilings of designated sensitive areas.

36. **Protection against active eavesdropping** - the leakage of NATO classified information by wired microphones, radio microphones or other implanted devices - requires a technical and/or physical security inspection of the fabric of the room, its furnishings and fittings and its office equipment, including office machines (mechanical and electrical) and communications. These inspections shall be undertaken by trained security staff authorised by the appropriate security authority.

Technically Secure Areas

37. Areas which have been specifically identified as requiring protection against audio eavesdropping are to be designated as technically secure areas and entry to them shall be specially controlled. Rooms must be locked and /or guarded in accordance with physical security standards when not occupied and any keys treated as security keys. Such areas shall be subject

to regular physical and/or technical inspections; the periodicity of inspections shall be determined by the appropriate security authority. Inspections shall also be undertaken following any unauthorised entry or suspicion of such and entry by external personnel for maintenance work or redecoration.

38. No item of furnishings or equipment shall be allowed into these areas until it has been thoroughly examined physically for eavesdropping devices by trained security staff. A record of the type, serial and inventory numbers shall be maintained of equipment and furniture moved into and out of these technically secure areas. The areas shall be kept locked by an approved method when not occupied, and keys, if used, shall be treated as security keys.

39. Telephones shall not normally be installed in areas which are technically secure. However, where their installation is unavoidable, they shall be provided with a positive disconnect device or shall be physically disconnected when classified discussions take place.

40. The presence of mobile telephones and other electronic items equipped with electro-acoustic parts shall be prohibited in technically secure areas.

41. Regular technical security inspections may need to be carried out in areas where exceptionally sensitive conversations are held in order to supplement physical searches for quick plant devices and to investigate a telephone system or an electrical or other service which could be used as an attack medium. They may also be necessary to determine the vulnerabilities of sensitive areas, including vulnerabilities arising from the local threat from intelligence services which target the Alliance and/or its member nations.

Examination of electrical / electronic equipment

42. Before being used in those areas where meetings are held or work is being performed which involves information classified NS and above, and in circumstances where the threat is assessed as high, communications equipment and electrical or electronic equipment of any kind shall be examined by technical or communications security experts to ensure that no intelligible information is inadvertently or illicitly transmitted by such equipment beyond the perimeter of the appropriate security area.

Overlooking

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

PHYSICAL SECURITY FOR COMMUNICATION AND INFORMATION SYSTEMS (CIS)

44. Specific consideration should be given to the physical security of CIS areas and the appropriate directives and guidance should be consulted.

APPENDIX 1
ANNEX 1
AC/35-D/2001-REV2

OPEN STORAGE AREAS

1. Open Storage Areas are those authorised by the Head of the civil or military body for open storage of classified information. These areas shall be constructed in accordance with the following standards:

(a) **Construction** - the perimeter walls, floors, and ceiling shall be permanently constructed and attached to each other. All construction must be done in a manner so as to provide visual evidence of unauthorized penetration;

(b) **Doors** - doors shall be constructed of wood, metal or other solid material. Entrance doors shall be secured with a built-in nationally approved three-position combination lock. When special circumstances exist, the Head of the civil or military body may authorise other locks on entrance doors for NS and NC storage. Doors other than those secured with the aforementioned locks shall be secured from the inside with either deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar which extends across the width of the door, or by other means approved by the agency head;

(c) **Vents, Ducts, and Miscellaneous Openings** - all vents, ducts, and similar openings in excess of 96 square inches / 620 square centimetres (and over 6 inches / 15 centimetres in its smallest dimension) that enter or pass through an open storage area shall be protected with either bars, expanded metal grills, commercial metal sounds baffles, or an intrusion detection system;

(d) **Windows** -

(i) all windows that might reasonably afford visual observation of classified activities within the facility shall be made opaque or equipped with blinds, drapes, or other coverings;

(ii) Windows at ground level, or other easily reachable windows (for example, from roofs, verandas, and building annexes) will be constructed from or covered with materials that provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Open storage areas that are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable, either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by the motion detection sensors within the area).

CRITERIA for ACCESS to NATO CLASS I/II SECURITY AREAS by INDIVIDUALS from Non-NATO NATIONS and INTERNATIONAL ORGANISATIONS

1. The granting of access as set out in paragraphs 9 and 10 of this directive will increase the risk of compromise of NATO classified information. In order to mitigate some of the increased risk, the following criteria shall be applied prior to granting access to a NATO Class I Security Area, unescorted access to NATO Class II Security Areas, or assigning office space within a NATO Class II Security Area :

(a) access is necessary in support of a specified NATO programme, project, contract, operation, or related task;

(b) individuals shall only belong to a non-NATO nation / international organisation which has signed a Security Agreement with NATO and has been certified by the NATO Office of Security (NOS) as being able to appropriately protect released NATO classified information;

(c) the individual is in possession of an appropriate and valid NATO Personnel Security Clearance (PSC) based on a clearance procedure no less rigorous than that required for a NATO national in accordance with NATO security policy and supporting directives;

(d) for access to NATO classified information, the established release procedures (the latest version of AC/35-D/2002 refers) shall be observed;

(e) the approval of access rights is reserved to the NOS and shall take place in accordance with the requirements of paragraph 3 below;

(f) non-NATO individuals who have been granted access shall be clearly recognisable by unique access passes or badges. The access pass or badge shall not provide access to any other NATO Security Area;

(g) non-NATO individuals have signed the "Certificate of Acknowledgement of Responsibilities" associated with the security protection of NATO classified information;

(h) non-NATO individuals shall not have escorting privileges, exchange pass arrangements with other NATO civil or military bodies, or access to NATO registries / sub-registries; and

(i) where office space is allocated within a NATO Class II Security Area, effective measures shall be implemented to prevent the unauthorised disclosure of NATO classified information, whether in hard-copy form or associated with a NATO communication and information system (CIS).

2. The successful implementation of the above measures rests on the continuing development of sound security education and awareness for all staffs working in areas to which non-NATO individuals are granted access. It is, therefore, imperative that Security

Officers develop appropriate security education programmes and oversee the implementation of these measures.

3. The procedure to obtain approval for access rights is as follows :

(a) Heads of Division / Office shall confirm in writing to the Director, NOS (through the appropriate chain of command) that the non-NATO individual has a requirement for access to a particular area within a NATO Class II Security Area;

(b) the request shall be supported by documentation specifying the duration of the requirement, the full identifying particulars of the individual and the rationale for seeking access rights;

(c) the NOS shall approve an individual's suitability for access on a case-by-case basis. Approval shall be based on confirmation that :

- a Security Agreement and a Code of Conduct has been signed between NATO and the non-NATO nation / international organisation;

- the NOS has certified the non-NATO nation / international organisation as being able to appropriately protect released NATO classified information;

- the individual is in possession of an appropriate and valid NATO Personnel Security Clearance (PSC);

- the individual has signed a "Certificate of Acknowledgement of Responsibilities" associated with the security protection of NATO classified information;

(d) approved individuals shall receive a unique access pass or badge which indicates that the individual is permitted unescorted access to a specific zone in the NATO Class II Security Area;

(e) NATO staffs and non-NATO individuals from the Divisions / Offices involved in these arrangements shall be briefed by the appropriate local security authority / staffs.

4. On completion of the requirement to support a specified NATO programme, project, contract, operation, or related task, the granting of unescorted access to a NATO Class II Security Area shall be withdrawn. Non-NATO individuals who cease to be employed in the Divisions / Offices involved in these arrangements shall be made aware of, and acknowledge in writing, their responsibilities for the continued safeguarding of NATO classified information.

5. The implementation of the arrangements shall be subject to periodic security inspection by the appropriate Security Authority (NOS, SHAPE J2 for ACO, or ACT Office of Security for ACT).