NATO NORTH ATLANTIC COUNCIL
OTAN CONSEIL DE L'ATLANTIQUE NORD

NATO UNCLASSIFIED

25 November 2020

DOCUMENT
AC/35-D/2001-REV3

SECURITY COMMITTEE

DIRECTIVE ON PHYSICAL SECURITY

Note by the Acting Chair

1. At Annex is the third revision of the Directive on Physical Security which is published in support of the Security Within the North Atlantic Treaty Organization, C-M(2002)49-REV1. It is binding and mandatory in nature. This document replaces AC/35-D/2001-REV2 which should be destroyed.

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

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

(Signed) Marco Criscuolo

Annex 1

Action Officer: R. Grumberg, NOS (Ext: 9182)
Original: English

DIRECTIVE ON PHYSICAL SECURITY
TABLE OF CONTENTS

DIRECTIVE ON PHYSICAL SECURITY

INTRODUCTION

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

(a) basic principles;

(b) general physical security requirements;

(c) specific physical security measures;

(d) storage requirements for NATO Classified Information;

(e) physical protection of communication and information systems; and

(f) protection against technical attacks.

BASIC PRINCIPLES

2. All premises, buildings, offices, rooms, and other areas in which NATO Classified Information is stored, handled and/or discussed 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, including:

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

(b) the quantity and form of the classified information (hard copy**,** and/or electronic**)** stored and/or handled;

(c) access control and enforcement of the need-to-know principle;

(d) the threat from hostile intelligence services which target NATO and/or NATO Nations, and the locally-assessed threat of terrorism, espionage, subversion, sabotage, and (organized) crime; and

(e) how the classified information will be stored (e.g. hard copy or electronic and encrypted).

3. Physical security measures shall be designed to:

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

(b) deter, impede and detect actions from the insider threat;

(c) allow for segregation of personnel in their access to NATO Classified Information in accordance with their level of Personnel Security Clearance (PSC) and the need-to-know principle; and

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

4. National Security Authorities/Designated Security Authorities (NSAs/DSAs) and other competent security authorities and NATO Civil and Military bodies are responsible for ensuring that security plans have been prepared in order to prevent NATO Classified Information from falling into unauthorised or hostile hands in the event of an emergency. Such plans shall consist of the emergency evacuation and/or destruction of classified information. As a minimum they shall include:

(a) specific emergencies for which classified information shall be evacuated and/or destroyed;

(b) emergency evacuation/destruction procedures outlining the authority (primary and alternate) responsible for initiating its execution;

(c) communication methods;

(d) the mechanisms of destruction or methods of evacuation;

(e) identification of alternate storage locations for evacuation; and

(f) prioritization of items for emergency destruction or evacuation.

GENERAL PHYSICAL SECURITY REQUIREMENTS

5. Physical measures represent only one aspect of protective security and shall be supported by sound personnel security, security of information, and communication and information systems (CIS) security measures, details of which can be found in Enclosures C, E and F of C-M(2002)49 and the supporting directives. Sensible management of security risks will involve establishing the most proportionate, efficient and cost-effective methods of countering the threats and compensating for vulnerabilities by a combination of protective measures from these domains. Such efficiency and cost-effectiveness shall be achieved by defining physical security requirements as part of the planning and design of facilities and seeking direction from the relevant security authority, thereby reducing the need for costly renovations.

6. Physical security programmes shall be based on the principle of “defence in depth”, using an appropriate combination of complementary physical security measures which provide a degree of protection meeting the requirements associated with the criticality and vulnerability of the organization and its information. Although physical security measures are site-specific, and determined by a number of factors (e.g. locally-assessed threat, building construction and architecture, environmental considerations, site location), the following general principles shall apply:

(a) it is first necessary to identify the assets that require protection. This is followed by the creation of layered security measures to provide “defence in depth” and delaying factors;

(b) the outermost physical security measures shall define the protected area and deter unauthorised access;

(c) the next layer of measures shall detect unauthorised or attempted access and alert the guard force;

(d) the innermost layer 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.

7. Equipment that provides physical security (e.g. CCTV, IDS, secure cabinets) shall be regularly maintained to ensure that it operates at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures as well as the complete security system. This is particularly important if there is a change in use of the site or specific elements of the security system. This can be achieved by regularly exercising incident response plans (normally, on an annual basis).

8. The local security authority shall carefully assess the presence of any electronic systems or mobile devices with recording and/or transmitting capabilities (e.g. mobile phones, smart phones and/or watches, tablets, laptops, Internet of Things devices) in areas where NATO Classified Information is stored, handled or discussed. The supporting document on the use of mobile devices on NATO premises (AC/35-D/1042) can be used to develop security requirements and local regulations regarding the use of mobile devices.

Security Areas

9. Security Areas are areas in which information classified NATO CONFIDENTIAL (NC) and above is stored**,** handled, or discussed. The provisions of the following paragraphs apply equally to Security Areas of fixed and temporary nature, as appropriate. Such areas shall be organised and structured so as to correspond to one of the following:

(a) NATO Class I Security Area: a particularly sensitive area in which information classified NC and above is stored, handled, or discussed in such a way that entry into the area constitutes, for all practical purposes, access to NATO Classified Information and therefore unauthorised entry would constitute a security breach. Such areas may include operations rooms, communications centres or archive facilities and require:

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

(ii) an entry control system which grants access only to those individuals appropriately cleared and specifically authorised[1] to enter the area;

(iii) a determination of the level of security classification and the category of the information (e.g. ATOMAL, BOHEMIA) normally stored in the area, i.e. the information to which entry gives access; and

(iv) a clear indication that entrance into such areas requires specific authorisation by the local security authority. This indication may include the level of security classification and/or the sensitivity of the area.

(b) NATO Class II Security Area: an area in which information classified NC and above is stored, handled, or discussed in such a way that it can be protected from access by unauthorised individuals utilizing internally established controls. Such areas may include working offices or meeting rooms where NATO Classified Information is stored, handled or discussed. These areas require:

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

[1] Specifically authorised refers to those personnel who have been formally recognised as having a need-to-know and access based on the nature of their employment responsibilities, and are included on an access control list, as well as individuals who have been formally authorised by the head of the organization in question on an ad hoc basis to perform a specific role or duty.

(ii) an entry control system which permits unescorted access only to those individuals who are security cleared and authorised to enter the area; and

(iii) an escort or equivalent control mechanism to deal with those individuals who do not meet the criteria described in sub-paragraph (b) (ii) above in order to prevent unauthorised access to NATO Classified Information and uncontrolled entry to areas, which have been specifically designated as protected against technical attacks**,** eavesdropping, and overhearing.

10. All security areas (e.g. offices, meeting and conference rooms, technically secure areas, etc.) where NATO Classified Information is discussed shall be periodically evaluated for risks of overhearing. Where the relevant security authority determines such risks exist, classified discussions should be prohibited, or appropriate corrective procedural measures (e.g. identifying meetings rooms established for classified discussions) or technical measures (e.g. soundproofing walls, doors, and ceilings, installing sound attenuation systems, etc.) shall be taken.

11. Those Security Areas which are not occupied by duty personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that they are properly secured unless an IDS used for this purpose is activated.

12. An appropriate Access Control (e.g. pass or personal recognition system) governing the regular staff shall control entry into Class I or Class II Security Areas.

Administrative Zone

13. An Administrative Zone shall be established around or leading to NATO Class I or Class II Security Areas. Only information classified at the level of NATO RESTRICTED (NR) may be stored, handled or discussed in Administrative Zones. Such areas require a visibly defined perimeter, within which the possibility exists for the control of individuals and vehicles. However, individuals are not required to be escorted.

Technically Secure Areas

14. Technically Secure Areas, either fixed or temporary, are areas**,** which have been specifically identified as requiring protection against technical attacks and eavesdropping.

15. Technically Secure Areas shall be subject to regular physical and technical[2] inspections and entry to them shall be strictly controlled. The following measures shall be applied to protect against technical attacks and eavesdropping:

(a) implementation of the appropriate level of physical and technical security measures to enforce risk-based access controls. The responsibility for determining the risk is shared between the appropriate technical specialists and the security authority which provides advice to the risk owner for a decision/approval;

[2] Technical inspection refers to electronic sweeping or surveying of an area to determine the potential presence of information collection devices (microphones, cameras, etc.) or communication jamming devices.

(b) such areas shall be locked and/or guarded when not occupied and any keys shall be treated as security keys[3]. Regular physical and/or technical inspections, in accordance with the requirements of the appropriate security authority, shall be undertaken. Such inspections shall also be conducted following any unauthorised entry or suspicion thereof, as well as following the entry of any external personnel (e.g. for the purposes of maintenance work, re-decoration);

(c) no item, furnishing or equipment shall be allowed into these areas until it has been thoroughly examined for eavesdropping devices by trained security staff. An appropriate record of items, furnishings and equipment moved into and out of these areas shall be maintained;

(d) the presence of any electronic systems or mobile devices with recording and/or transmitting capabilities (e.g. mobile phones, smart phones and/or watches, tablets, laptops, Internet of Things devices) shall be prohibited;

(e) telephones and other video conference devices shall normally not be installed in such areas. However, where their installation is unavoidable, they shall be physically disconnected when classified discussions take place. This does not apply to appropriately installed and approved communication devices (e.g. classified phone-lines, video conferencing equipment).

SPECIFIC PHYSICAL SECURITY MEASURES

16. This section provides information on various specific physical (e.g. perimeter, doors, locks), technical (e.g. intrusion detection system, closed circuit television) security measures and procedures (e.g. visitor control, control of keys, offices space separation) and how they can contribute to the security framework of an organization or site.

Perimeter

17. A perimeter forms a physical barrier and identifies the boundary of an area requiring security protection.

18. A perimeter is used to:

(a) create a physical and psychological deterrent to accidental entry into an area;

(b) deter unauthorised entry by overt or covert means;

(c) delay intrusion into an area in order to give time for reaction by the security guards or forces; and

(d) facilitate identification and control procedures by channelling the flow of authorised persons and vehicles through fixed entry points.

[3] Security keys are those which operate the locks fitted to: secure cabinets provided for the storage of classified information; doors of secure rooms or areas; doors of secure rooms or areas which have been subject to technical security inspections; and security cabinets used for the circulation of classified documents. Security Keys are to be handled as and protected in the same manner as the classified information to which they grant access.

19. The level of protection offered by a perimeter fence depends on its design, construction material, height, foundation type and depth, and any additional security features used to increase its performance and effectiveness (e.g. topping, perimeter intrusion detection system, lighting, closed circuit television). Some buildings may not have perimeter fences, but may have other barriers and infrastructure that act as a physical barrier.

20. A perimeter barrier only delays a determined intruder for a short period of time and should therefore be supplemented by an intrusion detection system (IDS), closed circuit television (CCTV), security lighting and periodic but random patrols by the appropriate security guards or forces.

21. The effectiveness of a perimeter also depends on the level of security at the entry points. Therefore, the gates shall be constructed to the same security standard as the perimeter and some form of access control shall be in place.

Intrusion Detection Systems

22. Perimeter Intrusion Detection Systems (PIDS) may be used to enhance the level of security offered by perimeter fences. 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.

23. 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 timeframe in the event of an alarm being activated.

Access Control

24. The term “access control” encompasses a pass or personal recognition system including arrangements for controlling and escorting contractors and visitors.

25. Access control may be exercised over a site, a building or buildings on a site, or areas, zones or rooms within a building. The control mechanism may be electronic, electro-mechanical, or physical. It may also be exercised by a guard or a receptionist. A pass or personal recognition system governing the regular staff shall control entry into Class I or Class II Security Areas.

26. In cases where a pass recognition system is in place within the establishment, security passes shall be worn visibly at all times in order to permit recognition and identification.

Office space separation

27. Appropriate measures shall be taken in order to prevent NATO Classified Information from being accessed by unauthorised individuals through physical proximity or surveillance. Factors such as the number of staff working in or having access to the area, the position of windows and the possibility of viewing the interior of the room from outside, as well as the light conditions (daylight, artificial) shall be taken into consideration. Precautions shall also be taken against overhearing and eavesdropping.

Guards

28. The employment of guards can provide a valuable deterrent to individuals who might plan covert intrusion. The guards’ duties and the frequency of patrols shall be decided by considering the level of risk and 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.

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

30. When a security incident occurs on site, a response force is required to react. This response force shall be comprised of an appropriate number of security personnel (normally, a minimum of two guards), as determined by the appropriate security authority. Any response to an incident shall not be to the detriment or weakening of protection elsewhere on the site. Guard force response to alarms or emergency signals shall be tested and shall be within a time limit evaluated as capable of preventing an intruder accessing NATO Classified Information.

Closed Circuit Television

31. The use of CCTV is a valuable aid to security guards in verifying incidents and IDSs on large sites or perimeters. The effectiveness of such a system will, however, depend on the selection and installation of suitable equipment as well as the monitoring of the system undertaken in the control centre. Expert advice shall be sought when establishing the optimal CCTV design elements such as: camera technical characteristics, camera installation locations, CCTV system redundancies, and CCTV control centre monitoring array layout and ergonomics. Care shall be taken to ensure that audio and visual data captured by CCTV does not put NATO Classified Information at risk of overlooking.

Security Lighting

32. In addition to providing the illumination necessary for effective surveillance either directly by the guards or indirectly through a CCTV system, security lighting can offer a high degree of deterrence to a potential intruder. The standard of lighting shall meet the minimum requirement of the CCTV and shall be installed in a manner which is appropriate to the site conditions.

Secure Cabinets and Office Furniture

33. Secure Cabinets and Office Furniture used for storing NATO Classified Information represent the last line of a defence-in-depth approach to security. Their time-delay capability is ascertained by comprehensive tests in order to determine their resistance capability to undetected access and to those forms of attack to which they are reasonably likely to be subjected. Such equipment shall be appropriately approved for the level of classified information held (as set out in paragraphs 50-54 of this Directive). When selecting equipment for storing NATO Classified Information the following criteria shall be taken into account**:**

(a) the threat to security in the area in which the information is stored;

(b) the classification level of the information to be stored;

(c) the level of protection provided by the cabinet or furniture and its lock; and

(d) the combination of ancillary measures protecting the environment of the cabinet or furniture.

Locks

34. Lock and key systems shall be selected to provide protection commensurate with the level of access control required, the information to be protected and the type of construction and material in which they will be installed.

35. Mechanical lock cylinders shall provide protection against key bumping, physical attack (e.g. drilling, chiselling, twisting, extraction) and unauthorised key duplication. Site key management systems shall have a moderate number master key groups. External locks shall be selected with adequate corrosion resistance for the local environment.

36. Electronic locks shall provide adequate protection against unauthorised electronic key (e.g. magnetic strip, smart chip, token, etc.) duplication and shall provide active indications of low battery levels and system faults. Site electronic key management systems shall limit the number of electronic master keys that provide access to a large number of electronic locks and shall limit the validity period of electronic keys. Electronic locks shall maintain a record of electronic key-lock access authorizations.

Control of Keys and Combinations

37. Keys of Secure Cabinets shall not be taken off the site. As a general rule such keys should not be taken out of the same office building where the cabinet is situated. Combination settings of Secure Cabinets as well as combination settings for activating/deactivating an IDS shall be committed to memory by individuals needing to know them. Knowledge of combination settings shall be restricted to the smallest possible number of individuals. As a minimum, the 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, unless otherwise authorised by the relevant security authority, subject to security risk assessment.

38. Spare keys and a written record of each combination setting for use in an emergency shall be held in sealed opaque envelopes by the local security authority.

39. Working and spare security keys shall be kept in separate cabinets. The record of each combination shall be kept in a separate envelope.

40. Keys, combinations and envelopes shall be afforded a level of security protection no less stringent than the information to which they give access.

Approved Equipment

41. The walls, floors, ceilings, and doors of vaults and open storage areas constructed within a Class I or a Class II Security Area where information classified NC and above is stored on open shelves or visibly displayed (e.g. on charts, maps), shall be approved by the appropriate security authority.

42. NATO Nations shall only use equipment which has been approved for the protection of NATO Classified Information by an appropriate security authority.

43. NATO Civil and Military Bodies shall ensure that any equipment purchased has been approved for use by one of the NATO Nations in similar conditions. NATO Civil and Military bodies may also purchase equipment approved for use by an appropriate security authority based on a completed risk assessment that supports the reduction or mitigation of the identified risk(s).

Visitor Control

44. An appropriate Visitor Control System shall be in place to determine whether a visitor may be permitted access to a site, building, or area where NATO Classified Information is stored, handled and/or discussed.

45. Official visits should normally be notified in advance by the visitor's parent organization. As a minimum, the official notification should include a description of the official identifying document, for example, passport or identity card.

46. Visitors can either be escorted or unescorted, however, an appropriate level of control over visitors shall be maintained, as set out in the following paragraph.

47. Procedures for the control of visitors may vary depending on local security requirements. In every case the following minimum requirements apply to escorted or unescorted visitors:

(a) escorted:
visitors shall be accompanied at all times by staff or guards with the appropriate level of PSC. They may be required to wear a pass that identifies them as a visitor. Full details of visitors should be recorded;

(b) unescorted:
individuals with an appropriate PSC and the need-to-know may be provided with a temporary unaccompanied entry to an area, or parts of it. However, such visitors shall be required to wear a pass that identifies them as a visitor and shall be required to return their temporary pass as soon as their business within the organization is completed. Full details of visitors shall be recorded, including entry and exit times. Visitors who are unescorted are not permitted to escort other visitors.

Entry and Exit Searches

48. Random entry and exit searches, designed to act as a deterrent to the introduction of unauthorised material or the unauthorised removal of classified or non-classified material may be undertaken in sites or buildings where NATO information is stored or handled.

49. 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.

MINIMUM STANDARDS FOR STORAGE OF NATO CLASSIFIED INFORMATION

50. NATO Classified Information shall be stored in areas, Secure Cabinets and/or Office Furniture designed to deter and detect unauthorised access to the information.

51. **COSMIC TOP SECRET (CTS)**

Information classified CTS shall be stored within a Class I or Class II Security Area under one of the following conditions:

(a) in an approved secure cabinet with one of the following supplemental controls:

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

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

(iii) an approved 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 secure cabinet, or overcome the physical security measures in place.

(b) in an open storage area constructed in accordance with Appendix 1 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) in 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.

52. **NATO SECRET (NS)**

Information classified NS shall be stored within a Class I or Class II Security Area by one of the following methods:

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

(b) in an approved secure cabinet or vault without supplemental controls; or

(c) in 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 not less than 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.

53. **NATO CONFIDENTIAL (NC)**

Information classified NC shall be stored in a Class I or Class II Security Area in an approved secure cabinet.

54. **NATO RESTRICTED (NR)**

Information classified NR shall be stored in a locked cabinet or Office Furniture (e.g. office desk drawer) within an Administrative Zone**,** Class I Security Area**,** or Class II Security Area. Information classified NR may also be stored in a locked cabinet, vault, or open storage area approved for information classified NC or higher.

PHYSICAL PROTECTION OF COMMUNICATION AND INFORMATION SYSTEMS

55. Areas in which NATO Classified Information is presented or handled using information technology, or where potential access to such information is possible, shall be established in a way that the aggregate requirement for confidentiality, integrity and availability is met.

56. Areas in which CIS are used to display, store, process, or transmit information classified NC and above, or where potential access to such information is possible, shall be established as NATO Class I or Class II Security Areas or the national equivalent.

57. Areas in which CIS are used to display, store, process or transmit information classified NR, or where potential access to such information is possible, may be established as Administrative Zones.

58. Access to areas where critical CIS components (such as servers, network, storage, and cryptographic equipment) are housed and managed shall be specifically controlled and limited to only authorised personnel associated with security and system/network/crypto administration.

59. In order to identify an appropriate level of protection for CIS handling NATO Classified Information the Enclosure F to C-M(2002)49 and its supporting directives shall be used.

Physical Protection of Printers, Copiers and Shredders

60. Printers, copiers, shredders and other equipment used to reproduce or destroy NATO Classified Information shall be physically protected to the extent necessary to ensure that only authorised individuals can use them and that NATO Classified Information is controlled in accordance with the requirements of NATO Security Policy and its supporting directives.

PROTECTION AGAINST TECHNICAL ATTACKS

61. 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.

62. Protection against passive eavesdropping attacks (i.e. leakage of NATO Classified Information via insecure communications or by unintentional electromagnetic emissions) may involve seeking technical security advice.

63. Protection against active eavesdropping (i.e. 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.

Examination of Electrical / Electronic Equipment

64. 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, based on a security risk assessment, 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 Class I and Class II Security Area.

OPEN STORAGE AREAS

1. Open Storage Areas are those authorised by the appropriate security authority for open storage of NATO 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 unauthorised penetration.

(b) **Doors**
doors shall be constructed of wood, metal or other solid material. Entrance doors shall be secured with a built-in an approved three-position combination lock. When special circumstances exist, the appropriate security authority 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 appropriate security authority.

(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 grilles, 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; and

(ii) windows at ground level, or other easily reachable windows (e.g. 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).