Department of Homeland Security
Management Directive System
MD Number: 11046
Issue Date: 2/22/2005

OPEN STORAGE AREA STANDARDS FOR COLLATERAL CLASSIFIED INFORMATION

I. Purpose

This directive establishes DHS policy for open storage of collateral-level classified material, and provides the requirements for constructing and operating open storage areas within the Department of Homeland Security (DHS).

II. Scope

This directive applies to all persons who are permanently or temporarily assigned, attached, detailed to, or under contract with DHS. It also applies to other officials outside the Federal government that have been provided access to classified information within the continental United States.

III. Authority

A. Executive Order 12829, “National Industrial Security Program.”

B. Executive Order 12958, as amended, “Classified National Security Information.”

C. 6 CFR, Part 7, “Department of Homeland Security, Classified National Security Information.”

D. 32 CFR, Part 2001/2004, Implementing Directive for EO 12958, as amended.

E. Underwriters Laboratories Standard 634, “Standard for Connectors & Switches for Use with Burglar-Alarm Systems.”

F. Underwriters Laboratories Standard 2050, “Standard for Safety of National Industrial Security Systems.”

IV. Definitions

A. ***Classified National Security Information ("Classified Information")***: Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

B. ***Open Storage Area***: A room or area constructed and operated pursuant to this directive, for the purpose of safeguarding national security information that, because of its size or nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

C. ***Organizational Element (OE)***: As used in this directive, Organizational Element is as defined in DHS MD Number 0010.1, "Management Directive System and DHS Announcements."

D. ***Portable Electronic Device (PED)***: Any non-stationary electronic apparatus with singular or multiple capabilities of recording, storing, processing, and/or transmitting data, video/photo images, and/or voice emanations. This definition generally includes, but is not limited to, laptops, PDAs, pocket PCs, palmtops, Media Players (MP3s), memory sticks (thumb drives), cellular telephones, PEDs with cellular phone capability, and pagers.

E. ***Security Liaison***: An official who is assigned responsibility for implementing and managing an Organizational Element's security program as a secondary or additional duty.

F. ***Security Officer***: Authorized position within an Organizational Element whose primary duty is to serve as the lead official for developing, implementing, and managing security programs within the Organizational Element.

G. ***Security-in-Depth***: A security principal of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility.

V. Responsibilities

A. ***The Secretary of Homeland Security*** has designated the Chief Security Officer (CSO) as the Senior Agency Official (SAO). As the SAO, the CSO shall:

1. Direct and administer the DHS's program under which information is classified, safeguarded, and declassified.

2. Coordinate the DHS's classification management program and serve as the DHS point of contact on matters associated with the Information Security Oversight Office (ISOO).

3. Promulgate and publish directives, as necessary, for program implementation, and ensure procedures are established and implemented to prevent unauthorized and unnecessary access to classified information.

4. Promulgate implementing regulations, which shall be published in the Federal Register to the extent that they affect members of the public.

5. Establish and maintain security education and training programs.

6. Establish and maintain a self-inspection and periodic review program to assess the management and safeguarding of classified information created and/or possessed by DHS OEs.

7. Develop special contingency plans for the safeguarding of classified information used in or near hostile or potentially hostile areas.

8. Ensure the performance contract or other system used to rate civilian or military personnel performance includes the management of classified information as a critical element to be evaluated in the rating of:

a. Original Classification Authorities

b. Security Managers, security specialists, or other officials performing security functions involving the safeguarding of classified information

c. Other personnel whose duties involve the creation or handling of classified information.

9. Account for costs associated with the implementation of programs to protect classified information. Report such costs to the Information Security Oversight Office (ISOO) upon request.

10. Assign promptly personnel to respond to any request, appeal, challenge, complaint, or suggestion arising out of Executive Order 12958, as amended, that pertains to classified information that originated in an organizational element of DHS that no longer exists and for which there is no clear successor in function.

11. Report violations, take corrective measures, and assess appropriate sanctions as warranted, in accordance with Executive Order 12958, as amended.

12. Oversee DHS participation in special access programs authorized under Executive Order 12958, as amended.

13. Establish procedures to prevent unnecessary access to classified information, including procedures that:

a. Require that a need for access to classified information is established before initiating administrative clearance procedures; and

b. Ensure that the number of persons granted access to classified information is limited to the minimum consistent with operational and security requirements and needs.

14. Perform other management duties as required by the position of Senior Agency Official that the Secretary may designate.

B. ***The Chief, Administrative Security Division*** shall, under the direction and authority of the SAO/CSO, administer, manage, and provide oversight for all programs related to safeguarding classified information, as cited in this directive.

C. ***The Heads of Organizational Elements*** shall:

1. Ensure sufficient resources are in place to implement and manage the Information Security Program and the requirements of this directive.

2. Appoint a senior official within the OE to serve as the organizational element Security Officer/Security Liaison.

3. Issue additional written procedures as necessary for the effective implementation of this directive. Procedures written to augment or supplement this directive may exceed the requirements cited in this directive but shall not lessen them. When an OE chooses to exceed the standards as cited herein, sufficient justification must exist to warrant any increased expenditures.

D. ***The Organizational Element Security Officer/Security Liaison*** shall:

1. Serve as the advisor to the head of the OE for all matters relating to implementation of and compliance with the provisions of this directive.

2. Implement, monitor, manage, and oversee the provisions of this directive within his/her respective OE.

3. Act as liaison between the OE, OE counterparts, DHS headquarters security staff, and other security officials both inside and outside of government.

4. Implement a viable and robust security education and training program.

E. ***Supervisors and Managers*** shall:

1. Ensure that they are aware of and comply with the applicable provisions of this directive, and promote and ensure compliance by staff members.

2. Begin security education and awareness training upon initial assignment of an employee, and reinforce training periodically thereafter through routine office interaction, e-mail reminders, staff meetings and other office gatherings, or any other method or media contributing to an informed workforce.

F. ***All DHS personnel*** shall:

1. Be responsible for protecting classified information from unauthorized disclosure.

2. Be aware of and comply with the applicable provisions of this directive and report to appropriate officials infractions or violations that affect the safeguarding of classified information.

VI. Policy & Procedures

Policy.

1. Construction and accreditation of a collateral-level, open-storage facility shall be considered only when the volume or bulk of classified material, or the functions associated with processing the classified material, make the use of GSA-approved security containers impractical.

2. This directive prescribes the standards for openly storing classified national security information. OEs may exceed the standards cited in this directive, but may not lessen them. If an OE chooses to exceed the standards cited herein, sufficient justification must exist to warrant any increased expenditures.

3. Requests to waive requirements cited in this directive will be submitted, in writing, through the Security Officer/Security Liaison of the requesting OE to the DHS Chief Security Officer. Waiver requests shall include sufficient justification to support the request and identification of compensatory measures that will be implemented to mitigate deficiencies.

4. OEs that have open storage areas that were approved prior to the publication of this directive, will not need to have their areas re-certified unless a change has been made that affects the structure and measures in place at the time of the original certification, or the standards used for approval of the area are less than those required by this directive. In the latter instance, OE's shall bring the area(s) up to the standards cited herein within one year of publication of this directive, and the area shall be recertified in accordance with this directive.

B. ***Procedure***.

1. When an OE determines that an open storage area is appropriate, the OE shall submit a request and justification for an open storage area, as follows:

a. DHS Headquarters elements will submit requests through the OE's Security Officer/Liaison (if applicable) to the DHS Office of Security.

b. For OEs, other than DHS Headquarters, with a permanent Security Officer assigned, the request will be submitted to the Security Officer having jurisdiction over the requesting organization.

c. For OEs, other than DHS Headquarters, with no permanent Security Officer is assigned, requests will be submitted through the OE's Security Officer/Liaison (if applicable) to the DHS Office of Security.

2. Open storage areas shall be approved based on:

a. Operational justification. Open storage areas shall only be approved for operational reasons, not for convenience. Where open storage is requested to satisfy the installation of a classified information system, unless otherwise justified and approved, the open storage authorization shall be limited to the system only. All documents and removable media will require closed storage in an appropriate security container.

b. Compliance with construction standards cited in this directive. An Open Storage Survey Checklist (Attachment A) shall be used to verify that the open storage area meets required standards.

c. Completion of a Standard Operating Procedures (SOP) Guide for operating the area. A sample SOP is provided as Attachment B. This sample shall be modified and tailored to suit the specific open storage area.

d. Receipt of a Facility Approval Memo. The memo must be signed by the authorized approval authority (see section VI.B.3) for the area being approved, must specify the facility being approved, and must specify the maximum level of material authorized for open storage. A sample memorandum is provided as Attachment C.

3. Approval Authority:

a. The Chief of Administrative Security Division, DHS Office of Security, is the approval authority for DHS Headquarters open storage areas and any other open storage area requests not under the jurisdiction of an OE Security Officer.

b. The OE Security Officer is the approval authority for open storage areas within his/her respective jurisdiction.

c. Upon approval of an area for open storage of collateral classified information, the approval authority shall issue a memorandum to the requesting OE, citing the specific location, building, room number, etc.; level of classified information authorized for open storage; any restrictions; and any other information deemed appropriate.

d. A copy of the approval memorandum, Open Storage Survey Checklist, and SOP shall be maintained by the approving authority and within the approved open storage area.

4. Level of Storage.

a. TOP SECRET Storage. An open storage area for TOP SECRET material will meet the construction standards and intrusion detection alarm system (IDS) requirements cited in this directive, Section VI.I. Arrival on-scene to unannounced alarm activations shall be within five minutes from the time the alarm is received at the monitoring station. Arrival time may be extended to fifteen minutes when the facility employs a security-in-depth concept and such extension has been approved by the open storage area approval authority.

b. SECRET Storage. An open storage area for SECRET material will meet the construction standards cited in this directive. In addition, one or more of the following supplemental controls shall be in place:

(1) The location that houses the open storage area is subject to continuous protection by cleared guard or on-duty personnel;

(2) Cleared guard or on-duty personnel inspect the perimeter of the open storage area at least once every four hours (ensure facility is secured and sign SF-702);

(3) An intrusion detection alarm system (IDS) is installed that meets the standards cited in this directive. Arrival on-scene to unannounced alarm activations shall be within thirty minutes from the time the alarm is received at the monitoring station.

(4) In addition to one or more of the supplemental controls listed above, the area shall be supported by security-in-depth consisting of a minimum of two additional layers of security. Examples of methods for achieving security-in-depth are fencing, walls, and other perimeter barriers; video surveillance and monitoring; employee and visitor facility access controls; facility IDS; and random facility guard patrols. Where an IDS is not present, the two layers shall include, at a minimum, physical perimeter barriers through which personnel must pass and access is controlled prior to reaching the open storage area.

c. CONFIDENTIAL Storage. An open storage area for CONFIDENTIAL material will meet the construction requirements of this directive. However, supplemental protection is not required.

d. Portable Electronic Devices (PEDs). Portable Electronic Devices (PEDs) shall not be introduced into an open storage area without written approval from the Designated Approval Authority in consultation with the cognizant Information Systems Security Manager and Security Officer/Liaison. Approvals will be considered only when the risks associated with the use of such equipment are clearly identified and sufficiently mitigated. Restrictions on the introduction of PEDs into open storage areas shall be prominently posted and included in the Standard Operating Procedures.

5. General Construction Requirements.

a. These criteria and standards apply to all new construction, reconstruction, alterations, modifications, and repairs of existing areas. They will also be used in evaluating existing areas.

b. Only heavy-duty builder's hardware shall be used in construction. Hardware accessible from outside the area shall be pinned, brazed, or spot-welded to preclude removal.

c. When ducts, pipes, registers, sewers, and tunnels are of such size and shape as to permit unauthorized entry (in excess of 96 square inches in area and over 6 inches in its smallest dimension), they shall be secured by 18-gauge expanded metal or wire mesh, or, by rigid metal bars, steel welded vertically and horizontally six inches on center. The rigid metal bars shall be securely fastened at both ends to preclude removal. When wire mesh, expanded metal, or rigid metal bars are used, they must ensure that classified material cannot be removed through the openings with the aid of any type of instrument. Expanded metal, wire mesh, or rigid metal bars may be substituted by an intrusion detection system.

d. Doors

(1) Routine entrance/exit doors shall be kept to an absolute minimum. Where possible, only one single door shall be used for routine entry/exit.

(2) Doors shall be substantially constructed of wood or metal. When windows, louvers, baffle plates, or similar openings are used, they shall be secured with 18-gauge expanded metal or wire mesh securely fastened on the inside. If visual access is a factor, the windows shall be covered. When doors are used in pairs or a gap exposes the latching mechanism, an astragal (overlapping molding) shall be installed where the doors meet or exposure occurs. Hinge pins that are exposed to the outer perimeter of the area shall be peened, brazed, or spot-welded to preclude removal.

(3) Doors shall be equipped with a heavy-duty automatic door closer.

(4) For new construction or renovation, entrance doors shall be secured with a GSA-approved, built-in combination lock meeting Federal Specification FF-L-2740-A. The use of a GSA-approved, built-in combination lock not meeting Federal Specification FF-L-2740-A is approved for existing locations until October 2012, at which time such locks must be replaced with one meeting the proper specification. Other high security locks may be used on a case-by-case basis with the approval of DHS' Office of Security. Other doors shall be secured from the inside with a panic bolt (which can be actuated by an alarmed panic bar); a dead bolt; a rigid wood or metal bar (that shall preclude "springing"), which shall extend across the width of the door and be held in position by solid clamps, preferably on the door casing; or by other means approved by the DHS Office of Security, consistent with relevant fire and safety codes.

(5) Routine entrance doors shall be additionally equipped with a supplemental access control device (e.g., storage room key lock lever, card reader, cipher lock, etc.,) to control access into the area during working hours. Supplemental access control devices are for access control purposes only and do not provide sufficient security for an unattended open storage area.

e. Windows. Every effort should be made to construct open storage areas without windows. However, windows that open, which are less than 18 feet from an access point (for example, a fire escape, roof, ledge, door, or the ground), shall be protected from forced entry by metal bars (separated by no more than 6 inches), plus crossbars to prevent spreading, or 18-gauge expanded metal mesh securely fastened on the inside. When visual access of classified information is a factor, the windows shall be covered by any practical method, such as drapes, blinds, painting, or covering the inside of the glass. The ability to easily open the window should be eliminated by either permanently sealing it or installing a locking mechanism on the inside. During classified discussion and non-working hours, the windows shall be closed and securely fastened to preclude surreptitious entry.

f. Walls.

(1) Construction shall be of plaster, gypsum wallboard, metal panels, hardboard, wood, plywood, glass, wire mesh, expanded metal, or other materials offering resistance to, and evidence of, unauthorized entry into the area. If insert-type panels are used, a method shall be devised to prevent the removal of such panels without leaving visual evidence of tampering. If visual access is a factor, area barrier walls up to a height of 8 feet shall be of opaque or translucent construction.

(2) Ceilings shall be constructed of plaster, gypsum wallboard material, panels, hardboard, wood, plywood, ceiling tile, or other material offering similar resistance to and detection of unauthorized entry. 18-gague wire mesh, or other non-opaque material offering similar resistance to, and evidence of, unauthorized entry into the area shall be used if visual access to classified material is not a factor.

(3) The perimeter walls of the open storage area shall be true floor to ceiling (slab to slab), or, sufficiently modified to represent a secure enclosure. When wall barriers do not extend to the true ceiling and a false ceiling is created, walls shall be permanently constructed to extend above the false ceiling to the true ceiling using similar building materials as the existing walls or 18 gauge expanded metal mesh, or, the false ceiling shall be reinforced with 18-gauge expanded metal mesh to serve as the true ceiling. When expanded metal mesh is used, it must overlap the adjoining walls and be secured in a manner that precludes removal without leaving evidence of tampering. When there is a valid justification for not erecting a solid ceiling as part of the area, such as the use of overhead cranes for the movement of bulky equipment within the area, the approval authority shall ensure that surreptitious entry cannot be obtained by entering the area over the top of the barrier walls.

g. Sound Attenuation.

(1) Where classified discussions will be taking place, conduct a sound attenuation test to ensure normal conversational tone from inside the room cannot be heard intelligibly from outside the room, paying particular attention to vents, ducts, and other openings. If public address or other amplification systems are used in conjunction with classified information, conduct the test with these systems actively operating. Where sound from inside the room can be easily overheard from outside the room, acoustical security shall be incorporated in the form of sound masking or structural enhancements.

(2) Examples of sound masking include installation of a CD or audio tape player with separate speakers; white noise generators; or other vibrating or noise generating systems that can be installed along the inside perimeter of the area. Where sound traverses through vents, ducts, and other similar openings, install music speakers in or near the opening; or white noise generators in or near the opening.

(3) Examples of structural enhancements include the use of sound deadening high-density materials in wall construction; use of extra layers of drywall for wall construction; and use of door gaskets for doorframes. Where sound traverses through vents, ducts, and other similar openings, consider installing commercial sound baffles or waveforms.

h. Intrusion Detection Systems (IDS).

(1) The IDS shall be connected to, and monitored by, a central monitoring station. Alarm system installation shall conform to the requirements of this directive or to the standards set forth by Underwriters Laboratory (UL) Standard 2050. The OE Security Officer/Liaison will approve contingency protection procedures in the event of IDS malfunction.

(2) Central Monitoring Station.

(a) The central monitoring station may be located at the facility of a UL-listed:

i. Contractor Monitoring Station, formerly called a proprietary central station;

ii. Cleared commercial central station;

iii. Cleared protective signal service station (e.g., fire alarm monitor); or

iv. Cleared residential monitoring station.

NOTE: For the purpose of monitoring alarms, all provide an equivalent level of monitoring service.

(b) Trained alarm monitors shall be in attendance at the alarm monitoring station at all times when the IDS is in operation.

(c) The central monitoring station is required to indicate whether or not the system is in working order and to indicate tampering with any element of the systems. Necessary repairs will be made as soon as practical. Until repairs are completed, periodic patrols shall be conducted during non-working hours, unless an appropriately cleared employee is stationed at the alarmed site.

(d) When an IDS is used, it shall be activated immediately at the close of business at the alarmed area or container. A record shall be maintained to identify the person responsible for setting and deactivating the IDS. Each failure to activate or deactivate shall be reviewed by the central monitoring station and, upon appropriate determination, be referred to the appropriate security official for investigation. Such records shall be maintained for one year.

(e) Records shall be maintained for one year indicating time of receipt of alarm; name(s) of security force personnel responding; time dispatched to facility area; time security force personnel arrived; nature of alarm; and what follow-up actions were accomplished.

(3) Investigative Response to Alarms

(a) The following resources may be used to investigate alarms: proprietary security force personnel, central station guards, and subcontracted guard services.

(b) When the IDS is in operation, a sufficient number of properly trained proprietary security force personnel, cleared to the appropriate level of the area, shall be available at all times to be immediately dispatched to investigate each alarm.

(c) For a commercial central station, protective signaling service station, or residential monitoring station, response personnel dispatched shall be cleared only if they have the ability and responsibility to access the area or container(s) housing the classified material; i.e., keys to the facility have been provided or the personnel are authorized to enter the building or check the container or area that contains classified material.

(d) Uncleared guards may be dispatched by a signaling service station, or residential monitoring station to an alarm. However, OE developed response plans shall include notification to a cleared representative of the affected facility for each alarm annunciation. If an alarm activation resets in a reasonable amount of time and no physical penetration of the area or container is visible, then entrance into the area or container is not required. The uncleared guards shall remain on the premises until a designated, cleared representative of the facility arrives, or as instructed by the cleared facility representative.

(e) If the alarm activation does not reset or physical penetration is observed, then a cleared response team must be dispatched. The initial uncleared response team must stay on station until relieved by the cleared response team.

(f) Subcontracted guards must be under contract with either the central monitoring station or the cleared facility.

(g) The OE shall require a 15-minute response time for TOP SECRET-level open-storage areas, and a 30-minute response time for SECRET-level open-storage areas. Arrangements shall be made with the monitoring station to immediately notify a cleared representative of the facility on receipt of the alarm. The representative is required to go immediately to the facility to investigate the alarm, and to take appropriate measures to secure the classified material.

(4) Installation. The IDS at the facility, area, or container shall be installed by a UL listed alarm installing company or by a company approved by the OE's security office. When connected to a commercial central station, Contractor Monitoring Station protective signaling service, or residential monitoring station, the service provided shall include line security (i.e., the connecting lines are electronically supervised to detect evidence of tampering or malfunction). If line security is not available, then two independent means of transmitting the alarm signal from the alarmed area to the monitoring station must be provided.

(5) Certificate of Compliance. Evidence of compliance with the requirements of this directive will consist of a valid UL certificate for the appropriate category of service. This certificate will have been issued to the protected facility by UL, through the alarm installing company. The certificate serves as evidence that the alarm installing company: (a) is listed as furnishing security systems of the category indicated; (b) is authorized to issue the certificate of installation as representation that the equipment is in compliance with requirements established by UL for the category of service; and (c) is subject to the UL Field Counter Check Program, whereby periodic inspections are made of representative alarm installations by UL-certified personnel to verify the correctness of installation practices.

(6) Exceptional Cases.

(a) If the requirements set forth above cannot be met due to extenuating circumstances, the OE may request approval for an alarm system that is:

i. Monitored by a central control station but responded to by a local (municipal, county, state) law enforcement organization.

ii. Connected by direct wire to alarm receiving equipment located in a local (municipal, county, state) police station or public emergency service dispatch center. This alarm system is activated and deactivated by employees of the OE, but the alarm is monitored and responded to by personnel of the monitoring police or emergency service dispatch organization. Police department response systems may be requested only when:

(i.) The OE facility is located in an area where central control station services are not available with line security and/or proprietary security force personnel, or a contractually dispatched response to an alarm signal cannot be achieved within the time limits required; and

(ii.) It is impractical for the OE to establish a proprietary guard force at the location.

iii. Installation of these type systems must use UL listed equipment and be accomplished by an alarm installation company that is certified by UL for any of the following categories: Defense Industrial Security Systems; Proprietary Alarm Systems; Central Station Burglar Alarm Systems; or Police Station Connected Burglar Alarm Systems.

(b) An installation proposal, explaining how the system would operate, shall be submitted to the OE Security Officer/Liaison. The proposal must include sufficient justification for granting an exception and the full name and address of the police department that will monitor the system and provide the required response. The name and address of the UL-listed/ UL-certified company that will install the system and inspect, maintain, and repair the equipment shall also be furnished.

(c) The OE shall require a 15-minute response time from the police department for TOP SECRET-level open-storage areas, and a 30-minute response time for SECRET-level open-storage areas. Arrangements shall be made with the police to immediately notify an cleared representative of the facility on receipt of the alarm. The representative is required to go immediately to the facility to investigate the alarm, and to take appropriate measures to secure the classified material.

(d) In exceptional cases where central station monitoring service is available, but no proprietary security force of central station or subcontracted guard response is available, and where the police department does not agree to respond to alarms, and no other manner of investigative response is available, the OE Security Officer may approve cleared employees as the sole means of response.

i. System Requirements.

(1) Independent Equipment. When many alarmed areas are protected by one monitoring station, secure room zones must be clearly distinguishable from the other zones to facilitate a priority response. All sensors shall be installed within the protected area.

(2) Access and/or Secure Switch and Premise Control Unit (PCU). No capability should exist to allow changing the access status of the IDS from a location outside the protected area without prior approval of the OE Security Officer. All PCUs (alarm panel) must be located inside the secure area. All alarm keypads should be located near the entrance. Assigned personnel should initiate all changes in access and secure status. Operation of the PCU will be restricted by use of a keypad and or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the space shall cause an alarm to be transmitted to the monitor station.

(3) Motion Detection Protection. Secure areas that reasonably afford access to the container or area where classified data is stored, shall be protected with motion detection sensors (i.e., ultrasonic, passive infrared, etc.) Use of dual technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector shall cause an immediate and continuous alarm condition.

(4) Protection of Perimeter Doors. Each perimeter door shall be protected by a balanced magnetic switch (BMS) that meets the standards of UL 634.

(5) Windows. All readily accessible windows shall be protected by an IDS, either independently or by the motion detection sensors inside the space/facility.

(6) IDS Requirements for Continuous Operations Facilities. A facility that operates continuously may not require an IDS. This type of secure area should be equipped with an alerting system if occupants cannot observe all potential entrances into the room. Duress devices may also be required.

(7) False and/or Nuisance Alarm. Any alarm signal transmitted in the absence of a detected intrusion, or identified as a nuisance alarm, is a false alarm. A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. All alarms shall be investigated and the results documented. The maintenance program for the IDS should ensure that incidents of false alarms should not exceed one (1) in a period of thirty (30) days per zone.

VII. QUESTIONS.

Questions regarding this directive should be addressed to the DHS Office of Security.

ATTACHMENT A

DEPARTMENT OF HOMELAND SECURITY
OPEN STORAGE SURVEY REPORT

Survey Conducted By: (Name, Position/Title and Phone Number)
Program Office of Surveying Official:
Date of Survey:
Address of Room/Area Surveyed: (Full Mailing Address --Must include a geographical/street location; P.O. Box, will not suffice.)
Room Name and/or Number(s) Surveyed: (Identify specific number(s) and/or name of the room(s) requested for open storage)
Program Office Responsible for Surveyed Room:
Designated Responsible Official for Open Storage Area: (Name, Position/Title and Phone Number)
Purpose of Open Storage: (Circle One) **Classified Computer Connectivity ONLY** **Documents/Materials ONLY** **Both** (NOTE: Justification for classified computer connectivity is self-evident. However, justification for Open Storage of documents/materials must be provided prior to approval).
Highest Classification Level to be Openly Stored in the Area: (Circle One) **CONFIDENTIAL** **SECRET** **TOP SECRET**
Completion of this survey does not constitute approval for open storage of classified materials. The survey results, as recorded on this form, the Standard Operating Procedures (SOP) guide developed for operation of the specific area, and a memorandum from the program office citing the request for open storage, the classification level of the materials to be stored in the area, and the justification for open storage will be forwarded to the approval authority, as cited in DHS MD 11046. The approval authority will evaluate the request, the survey results, and the justification and will either approve or disapprove the request. Approval/disapproval will be in writing and will be forwarded to the requester.

No.	Description	Yes	No	N/A
A	**Wall Construction**			
1	Walls that serve as the perimeter of the room shall be of permanent construction consisting of: (Circle appropriate construction materials) Plaster Gypsum Wallboard Metal Panels Hardboard Wood Plywood Glass Expanded Metal Mesh Concrete Masonry Unit Other (Explain): Other Comments:			
2	Walls that serve as the perimeter of the room extend true floor to true ceiling. (If No, see Items 3 and 4) Other Comments:			

No.	Description	Yes	No	N/A
3	Where the perimeter walls of the room do not extend true-floor to true-ceiling, a barrier extension has been constructed of 18-gauge expanded metal mesh from the top of the rooms' perimeter wall to the true-ceiling, or The false ceiling has been reinforced with 18-gauge expanded metal mesh to serve as a true-ceiling. Other Comments:			
4	Wire mesh or expanded metal overlaps adjoining walls, which are secured in a manner to prevent removal without leaving evidence of tampering. Other Comments:			
B	**Doors**			
1	Only one door is used for routine entrance/exit.			
a.	The door is substantially constructed of: (Circle one) Wood Metal Other (Explain)			
b.	The door is equipped with a GSA Approved, Group 1R, built-in, dial type, three position combination lock (for existing facilities), or a built-in dial-type, combination lock meeting Federal Specification FF-L-2740, for example the Kaba-Mas X-09 (for new construction).			
c.	If the door hinge pins are located on the exterior they have been peened, pinned, brazed, spot-welded, equipped with non-removable pins, or otherwise made impervious to removal.			
d.	If vertical space exists between the door stiles (edge of door where two doors meet) or between the door and frame, the gap is protected by an astragal on the working door to cover the space between doors and prevent introduction of devices to forcibly separate the doors and unseat the deadbolt.			
e.	If a double door is used, the inactive door is equipped with manual deadbolts with a minimum one inch throw on the top and bottom of the door.			
f.	The door is equipped with a card reader, electric or mechanical cipher lock, or key lock for supplemental access control.			
g.	The door is equipped with an automatic door closer. Other Comments:			

No.	Description	Yes	No	N/A
2	Does the room have other perimeter doors?			
a.	Other perimeter doors are for emergency use only.			
b.	Emergency use only doors are of similar construction as the primary entrance/exit door.			
c.	If the door hinge pins are located on the exterior they have been peened, pinned, brazed, spot-welded, equipped with non-removable pins, or otherwise made impervious to removal.			
d.	Emergency use only doors are equipped with panic hardware for emergency exit, a manual deadbolt lock with a minimum one inch throw, or a rigid metal or wood bar extending across the width of the door and held in position by solid clamps. The door(s) have no hardware on the exterior. If local fire codes prohibit such hardware, explain alternatives.			
	Other Comments:			
C	**Ceilings**			
	The ceiling shall be of permanent construction consisting of: (Circle appropriate construction materials) Plaster Gypsum Wallboard Metal Panels Hardboard Wood Plywood Ceiling Tile Concrete Masonry Unit Other (Explain) Other Comments:			
D	**Windows**			
1	The room is equipped with windows along the perimeter walls. (If NO, go to Section E) Comments:			

No.	Description	Yes	No	N/A
2	Windows which open, that are less than 18 feet from an access point (for example, another window outside the area, roof, ledge, or door) shall be protected from forced entry by means no greater than the contiguous wall. When visual access of classified information is a factor, the windows shall be covered by any practical method, such as drapes, blinds, or painting or covering the inside of the glass. The ability to open the window should be rendered inoperable by either permanently sealing it or installing a locking mechanism on the inside during non-working hours, the windows shall be closed and securely fastened to preclude surreptitious entry Other Comments:			
3	Windows are equipped with blinds, drapes, or similar covering to prevent observation. Other Comments:			
E	**Other Openings**			
1	There are vents, ducts, pipes, registers, sewers, or similar openings penetrating the rooms' perimeter wall, ceiling or floor that are in excess of 96 square inches. (If NO, go to Section F.) Other Comments:			
2 a. b. c.	Vents, ducts, pipes, registers, sewers, or similar openings in excess of 96 square inches are secured by: 18 gauge expanded metal, Wire mesh securely fastened from the inside, or Rigid metal bars extending across the width with a maximum space of 6 inches between bars. Other Comments:			

No.	Description	Yes	No	N/A
F	**Intrusion Detection System (IDS)**			
1	The room is equipped with a UL-approved Intrusion Detection Alarm System (IDS). If there is no IDS, TOP SECRET Open Storage WILL NOT BE APPROVED. SECRET Open Storage may be approved without an IDS if Section H (Guard Services) is complied with, or the room is occupied 24 hours a day, 7 days a week by a cleared employee(s), and, the room is protected by security in-depth consisting of a minimum of two external layers of perimeter security through which personnel must pass and through which access is controlled to reach the open storage area. Other Comments:			
2	As a minimum, the IDS consists of balanced magnetic switches on all door openings, and motion detectors that provide sufficient coverage of the internal room space. Other Comments:			
3	The IDS is monitored by an authorized central monitoring station 24 hours a day, 7 days a week. Identify IDS monitoring activity: Other Comments:			
4	On-site response to unannounced alarms does not exceed 30 minutes for rooms storing SECRET materials and 5 (or 15 minutes if approved by the approval authority) for rooms storing TOP SECRET materials. Other Comments:			
G	**Acoustical Protection**			
1	For areas where classified discussions will take place, conversational tone from inside the room is unintelligible from outside the room. Where public address or other amplification systems are in use, ensure a sound attenuation test is conducted with equipment in the **ON** position. Pay particular attention to vents, ducts, and other openings that may carry sound to areas outside of the room. Other Comments:			

No.	Description	Yes	No	N/A
H	**Guard Services**			
1	The location housing the room is subject to continuous, 24 hour a day, 7 day a week protection by cleared guard personnel. Other Comments:			
2	Cleared guard or duty personnel inspect the room perimeter at least once every 4 hours. Other Comments:			
I	**Standard Operating Procedures (SOP)**			
	An SOP has been developed to provide procedures for security of the area. (Include a copy of the SOP when submitting this survey.) Other Comments:			

Other comments affecting the security of the proposed Open Storage Area that should be considered in the approval process:

NOTE: In some instances, the existence of an IDS system may substitute for structural deficiencies. For example, the need for supplemental protective barriers for vents, ducts, pipes, and other openings in excess of 96 square inches may not be required depending on the actual size of the opening and IDS coverage. Fully explain any such circumstances to include size of openings and degree of IDS coverage.

ATTACHMENT B

STANDARD OPERATING PROCEDURES
OPEN STORAGE OF CLASSIFIED NATIONAL SECURITY INFORMATION

1. Purpose. This Standard Operating Procedure (SOP) provides guidance on the security measures that will be implemented and adhered to for the operation and maintenance of the DHS designated Classified National Security Information (NSI) Open Storage Area identified in paragraph 4, below.

2. Applicability. This SOP applies to all personnel working in or around the designated Open Storage Area.

3. General.

   a. All persons authorized unescorted access to the designated area will read and be familiar with the requirements of this SOP.

   b. An Open Storage Area is established when the volume or bulk of classified materials, or the functions associated with the processing of classified information, make the use of security containers impractical. The area designated for open storage serves as the container for the storage of classified materials and security measures must be in place and maintained in order to ensure the integrity of the materials stored therein.

   c. The local Security Official will be contacted prior to any modifications being made to the structure or security devices that were in place at the time open storage was approved.

   d. Under no circumstances will the level of classified materials *openly* stored in the area exceed the level of open storage authorized per paragraph 4, below.

   e. A copy of the Open Storage Approval Memorandum and the Open Storage Survey Report will be maintained as attachments to this SOP.

4. Identifying Data.

Program Office Responsible for Area	(Self Explanatory)
Position/Title of Responsible Official	(Enter the position and or title of the person designated as a point of contact for the designated area)
Room Number(s) of Designated Area	(Enter the specific room number(s) of the area designated for open storage)
Address	(Enter the full address of the facility that houses the open storage area)
Highest Level of OPEN Storage Authorized	(Circle One) CONFIDENTIAL SECRET TOP SECRET

5. Procedures.

a. Security Controls.

(1) Key locks, cipher locks, and card readers are supplemental access control devices only and do not provide sufficient security for an unattended open storage area. Therefore, whenever the designated area is unattended, all locking devices (built-in dial type combination lock, key/cipher lock, electric strike, electric knob, magnetic lock) will be in the locked position. The dial on the combination lock will be spun at least four times to ensure the combination is cleared. **The area will never be left open or unlocked when not occupied by an authorized person.**

(2) The combination for the built-in, dial-type, combination lock is classified at the same level as the highest classification of materials stored therein. It will not be provided to any person that does not have the appropriate security clearance and need-to-know. The combination will be recorded on a Standard Form 700, *Security Container Information*, and appropriately stored by the local Security Official.

(3) At a minimum, the combination to the built-in dial type combination lock will be changed every two years, or immediately when the lock is first placed in service; when someone having knowledge of the combination terminates employment or is reassigned; if it is suspected that the combination was compromised; or if the area is found unattended and unlocked. Contact the local Security Official for information on changing combinations.

(4) The combination to a cipher lock and/or keys to a key lock will be handled as sensitive information/materials and provided only to persons with a need-to-know.

(5) The combination to a cipher lock or the key lock will be changed/re-keyed as determined by the local Security Official or responsible official.

(6) When a card reader is used for supplemental access control, the reader will be programmed with its own distinct access level. Only persons who are authorized access to the area will have their key cards programmed to access the area.

(7) (Add guidance on restrictions on the introduction and/or use of personal electronic devices (PED's) and other audio/video recording devices within the open storage area).

b. Intrusion Detection Systems (IDS). (If applicable)

(As IDS designs, specifications, and reporting procedures vary widely the procedures for its operation will be prepared locally. Procedures should include as a minimum; Opening (disarming the IDS); Closing (arming the IDS); Alarm Response; IDS Maintenance; IDS Operations Checks; and procedures during a power outage.)

c. Access Control.

(1) Only persons who have been granted a security clearance equal to or higher than the level of classified material stored in the facility, and who have a need-to-know, will be authorized unescorted access to the area.

(2) Persons who do not have a security clearance equal to or higher than the level of classified material stored, and/or do not have a need-to-know, will not be allowed unescorted access to the area. Should the need arise to allow such visitors access to the area, the area will first be sanitized by a cleared person to ensure that no classified information is exposed or could otherwise be subjected to compromise. The visitor will then be escorted by a cleared person and will remain under visual escort for the duration of the visit.

(3) When uncleared visitors are escorted into the area, the escort will announce to all persons working in the area that a visitor is present. In larger areas, if a strobe light is installed as a means for announcing visitors, it will be activated.

d. End-of-Day Security Checks.

(1) At the end of each duty day the area will be checked to ensure that it is secure. The Standard Form 701, *Activity Security Checklist*, will be used to record the end-of-day check.

(2) The end-of-day check will be conducted by a cleared person designated by the responsible official identified in paragraph 4 of this SOP.

(3) The end-of-day check will consist of physically spinning the dial of the built-in combination lock at least four times in one direction. The supplemental access control device, i.e., key lock, cipher lock, card reader, will then be unlocked and the checker will physically tug on the door to make sure the dial-type combination lock is locked. The checker will also ensure that the IDS (if applicable) is armed.

(4) Any discrepancies noted in the end-of-day check will be reported to the responsible official and/or the local security official.

e. Emergency Procedures.

(1) In the event an emergency arises that causes the immediate evacuation of the area, every reasonable effort will be made to properly secure the area prior to departure. However, personal safety will not be jeopardized in order to secure the area.

(2) Should immediate evacuation prohibit the area from being properly secured then, upon termination of the emergency, a reasonable effort will be made to verify that the integrity of the materials stored therein has not been compromised. This will include a visual inspection of the stored materials to determine if any items may be missing or tampered with. In addition, the combination to the built-in dial type combination lock will be changed.

6. Any situation that is observed that affects the security integrity of the designated area, or the materials stored therein, will be reported immediately to *(name or position/title of responsible official and phone number)* and/or *(name and phone number of the local security official).*

7. Any questions regarding this SOP should be referred to (*name or position/title of responsible official and phone number*).

U.S. Department of Homeland Security
Washington, D.C. 20528

Homeland Security
Office of Security

(Use organizational element's letterhead where appropriate)

MEMORANDUM FOR (Insert Addressee Information)

FROM: ***(Insert Approval Authority's Information)***

SUBJECT: Open Storage of Classified Information

DATE: ***(Insert Date)***

This memorandum serves as approval for the open storage of classified information, not to exceed the ***(CONFIDENTIAL, SECRET, or TOP SECRET)*** level, within ***(Insert physical address and room number of area being approved)***. This approval is based on the Open Storage Survey and Report conducted and prepared by ***(Insert name of security specialist who completed the survey)*** and the Open Storage Area Standard Operating Procedures submitted by ***(Insert organizational element information)***.

This open storage approval is limited to information technology systems connectivity only. All media, i.e., discs, documents, etc., that contain classified information will be secured in an appropriate security container whenever the room is unattended and at the end of each duty day. ***(Remove this paragraph if area is being approved for all classified material)***

This open storage approval applies to all systems and media (i.e. discs, documents, etc.) that contain classified information. ***(Remove this paragraph if area is being approved for information technology systems only)***

Any modifications to the structure or procedures on which this approval was based shall be coordinated through the approval authority prior to implementation.

A copy of this approval memo, the Open Storage Survey Report, and the Standard Operating Procedures shall be maintained within the approved room. If you have any questions please contact me at ***(Insert contact information)***.