



DEPARTMENT OF DEFENSE
OFFICE OF DEPENDENTS EDUCATION
4040 NORTH FAIRFAX DRIVE
ARLINGTON, VA 22203-1635



LOGISTICS

DS REGULATION 4700.2
November 1993

DEPARTMENT OF DEFENSE DEPENDENTS SCHOOLS
INTERNAL PHYSICAL SECURITY

- References :
- (a) DS Regulation 4700.2, "Department of Defense Dependents Schools Internal Physical Security, " August 27, 1985 (hereby cancelled)
 - (b) DS Regulation 4800.1, "Department of Defense Dependents Schools Safety Program, " September 1993
 - (c) DoD 1342.6-M-1, "Administrative and Logistic Responsibilities for DoD Dependents Schools, " October 1978

A. REISSUANCE AND PURPOSE

This regulation reissues reference (a) to update policy, responsibilities, and procedures for protecting the Department of Defense Dependents Schools (DoDDS) personnel, students, and resources from acts or conditions which could result in loss of life, destruction or loss of Government property, and disruption of the DoDDS activities in overseas areas.

B. APPLICABILITY AND SCOPE

The provisions of this regulation apply to all the DoDDS personnel responsible for, or concerned with, protecting the DoDDS personnel, students, and resources from conditions which could result in personal injury or death, property loss or destruction, or disruption of DoDDS activities. This regulation establishes minimum security standards and procedures and authorizes the publication of pamphlets, manuals, or other media to assist in safeguarding the DoDDS personnel and resources.

c. DEFINITIONS

Terms and phrases used in this regulation are defined in enclosure 1.

D. POLICY

It is the DoDDS policy that all reasonable steps shall be taken to protect the DoDDS staff, students, and Government property by ensuring a secure environment at the DoDDS facilities and activities.

E. RESPONSIBILITIES

1. The Director, DoDDS, is responsible for:

a. The internal physical security program within the DoDDS .

b. The appointment of a security advisor with oversight for the development and application of the DoDDS policies, procedures, and standards pertaining to internal physical security.

c. Assistance to regional offices to achieve compliance with the provisions of this regulation and other applicable DoD security directives.

2. Regional Directors are responsible for:

a. Safeguarding and protecting the DoDDS students, personnel, visitors and resources within the region.

b. Appointing a regional security officer.

c. Implementing internal physical security measures and procedures designed to minimize susceptibility to loss, destruction, or theft of Government-owned or leased property within the region.

3. Regional security officers are responsible for:

a. Managing the internal physical security program for the region.

b. Providing assistance to district security coordinators to correct school security discrepancies forwarded to regional level for resolution. Maintaining records on waivers or exceptions to security standards and following up on corrective actions or changing situations that may negate or downgrade the discrepancy.

c. Visiting each school, in coordination with district security coordinators, at least every third year to evaluate the internal physical security program. This visit should be combined with the safety program evaluation.

d. Coordinating with host nation and U.S. military authorities to ensure both normal or increased law enforcement and security assistance as needed.

e. Reporting serious incidents in accordance with Enclosure 7., "Serious Incident Reporting". Monitoring and reporting any further developments until all action is accomplished.

4. District Superintendents are responsible for:

a. Safeguarding the DoDDS students, personnel, visitors, and resources within the district.

b. Appointing a security coordinator.

c. Administering the internal physical security program within the district.

5. District security coordinators are responsible for:

a. Analyzing security deficiencies at the DoDDS facilities within the district and facilitating their correction or making recommendations for appropriate corrective actions.

b. Developing and/or administering security education programs for personnel within the district.

c. Maintaining liaison with the Military Community security offices responsible for physical security inspection assistance.

d. Assisting school administrators to develop physical security plans, if necessary, or standard operating procedures for internal physical security within the specific facilities.

6. School principals are responsible for:

a. Safeguarding the DoDDS students, personnel, visitors, and resources at the school level. A subordinate school administrator may be appointed to serve as point of contact for security coordination.

b. Developing an individual physical security plan or standard operating procedure specific to their school. See enclosure 3 to determine which schools must develop a complete security plan or only internal security procedures. (One copy of each physical security plan or standard operating procedure will

be provided to the District Superintendent, Regional Director, and the Office of Dependents Education (ODE) , Transportation, Safety & Security Branch) .

c. Implementing the internal security program standards and procedures at the local level.

d. Working cooperatively with host installation or community security officials, district or regional administrators, school personnel and students to promote a security conscious attitude in all phases of the school's operation.

e. Coordinating semiannual physical security inspections of school facilities by host installation or community security officials. One of these semiannual inspections should be conducted in concert with safety, bioenvironmental, and fire marshal officials for a coordinated and balanced appraisal of security and safety. The preferred time for this inspection is prior to the beginning of the new school year.

f. Maintaining documentation on any corrective action needed and the status of corrections. This documentation must be coordinated with the cognizant district security coordinator or regional security officer. Maintain a copy of any waiver or exception to security standards granted to the individual school.

g. Ensuring that the school faculty and staff receive training and security awareness briefings on internal security procedures and current state of terrorist threat conditions and countermeasures in place for the area. Students should receive security awareness training consistent with their ages, information and resources available, and the local threat.

F. WAIVERS AND EXCEPTIONS

Procedures for requesting waivers or exceptions to standards are outlined in enclosure 2.

G. INTERNAL PHYSICAL SECURITY PLANNING PROCEDURE~

Procedures for internal physical security planning are outlined in enclosure 3.

H. KEY AND LOCK CONTROL

Procedures for key and lock control are outlined in enclosure 4.

I. IDENTIFICATION AND CONTROL MEASURES

Identification and control measures are outlined in enclosure 5.

J. STORAGE OF FUNDS

Procedures for storing cash or negotiable/accountable items are outlined in enclosure 6.

K. SERIOUS

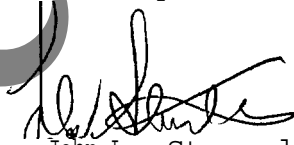
Procedures for evaluating and reporting serious incidents are outlined in enclosure 7.

L. FORMS

Forms described in this regulation and the enclosures are shown in enclosure 8.

M. EFFECTIVE DATE

This regulation is effective 30 days after date of publication. One copy of all implementing instructions will be provided to the District Superintendent, Regional Director, and ODE, ATTN: Chief, Transportation, Safety & Security Branch within 60 days of issuance.



John L. Stremple
Director

DISTRIBUTION: X, Y, Z, Q(WWPAC)

Enclosures - 8

1. Definitions
2. Waivers and Exceptions
3. Physical Security Planning Procedures
4. Key and Lock Control Procedures
5. Identification and Control Measures
6. Storage of Funds
7. Serious Incident Reporting
8. Forms

DEFINITIONS

1. Classified Information. Information or material that is (a) owned by, produced for or by, or under the control of the U.S. Government; (b) determined under Executive Order 12356 or any predecessor's order to require protection against unauthorized disclosure; and (c) is so designated.
2. compensatory Measure. An alternate physical security measure employed to provide a degree of security equivalent to or exceeding that provided by the physical security measure or procedure required by this regulation. See also Waiver and Exception.
3. controlled Area. A designated area that contains resources which, while not vital to National Security, require special security measures for protection from theft or damage because of high value, vulnerability to pilferage, or because loss would create a major disruption of activities.
4. Exception. Permanent relief from specific requirements imposed by this regulation. Requests for exceptions will be based on an individual determination that unique circumstances at a given school or installation are such that conformance to established standards is impossible, highly impractical, unnecessary due to measures exceeding those prescribed, or otherwise not in the best interest of the U.S. Government.
5. Other Users. Any individual or organization outside of the DoDDS that is authorized to use the DoDDS facilities.
6. Physical Security. That part of security concerned with physical measures designed to safeguard personnel, prevent unauthorized access to equipment, facilities, material, and documents, and to safeguard the aforementioned against damage and theft.
7. Pilferable Items. Material having a ready resale value, civilian utility or personal application and, therefore, susceptible to theft.
8. Repository. A secure container or metal key box for the controlled storage of keys and locks used within the Key and Lock Control System.
9. Safe. A General Services Administration approved security container weighing 750 pounds or more equipped with a re-locking device.

10. Terrorist Incident. A distinct criminal act committed, or threat of such an act to be committed, against individuals or property to coerce or intimidate governments or societies, generally to achieve political, religious, or ideological objectives.

11. Terrorist Threat condition. A Department of Defense standardization of recommended responsive measures to terrorist threats against U.S. personnel and facilities. Also called THREATCONS , this system facilitates interservice coordination and support for antiterrorism activities.

12. Vandalism. The willful damage or destruction of facilities, equipment, or material.

13. Vault. A strongly built chamber for preserving items of considerable worth or value.

14. Visitor. Any individual, military or civilian, not assigned to or employed within a school or activity to which access is requested.

15. Waiver. Temporary relief from specific standards imposed by this regulation pending accomplishment of actions or programs which will conform to established standards. The time limits of the waiver will be specified by the approving authority.

WAIVERS AND EXCEPTIONS

Requests for temporary waivers or permanent exceptions to specific portions of this regulation will be submitted through the district superintendent to the regional office for evaluation and concurrence. The regional office may disapprove the request or, if concurred, the request for waiver or exception will be signed by the Regional Director or Deputy Director and forwarded to ODE, ATTN: Chief, Transportation, Safety & Security Branch, for final approval.

A. WAIVERS

Waiver requests will be considered if all reasonable efforts to correct a deficiency fail and the situation must be carried into the following fiscal year for scheduled correction. A request for waiver will include:

a. A statement of the problem or deficiency that creates standards below those cited in this regulation or by host installation security officials as a result of their inspections.

b. Reasons why the school cannot comply with the requirements of this or host installation security regulations. Include an explanation of the plan, program, or schedule that will meet the prescribed security requirements.

c. The estimated date by which the deficient condition(s) will be corrected.

B. EXCEPTIONS

Permanent exceptions to this regulation will be considered if unique circumstances at a given location are such that conformance to established standards are impossible, highly impractical, unnecessary due to compensatory measures exceeding those prescribed, or otherwise not in the best interests of the U.S. Government. Requests for permanent exceptions to this regulation must include:

a. A statement of the problem or deficiency that creates standards below those cited by this or host installation security regulations.

b. Measures in effect to compensate for noncompliance with required standards of protection.

c. Reasons why the activity cannot comply with the requirements of this or host installation security regulations. Include any statements from host installation or community officials explaining why support to correct or measures to compensate for the deficiency can not be provided, if applicable. Include information as to the cost associated with correcting the deficiency if it may be a factor in determining if an exception is appropriate.

The ODE Transportation, Safety & Security Branch will be notified in writing whenever an approved waiver or exception is no longer required. Permanent exceptions will be reviewed annually, prior to the beginning of the new school year, to determine if circumstances have changed to allow the correction of a deficiency that was granted status as an exception to this regulation.

Cancelled

PHYSICAL SECURITY PLANNING PROCEDURES

A. INTERNAL PHYSICAL SECURITY PLANNING

The internal security program is the sum total of all planning and analysis arranged in a logical sequence that provides for planning, coordination, and review of courses of action devised for the protection of the DoDDS personnel and resources. Basic to the formulation of a security program is the determination of what is to be protected and the degree of protection to be accorded. It is a continuing process in which the security interest and security measures of an activity undergo constant scrutiny and evaluation. Security planning must be based on the operating requirements of an installation or activity.

B. PLANNING CONSIDERATIONS

1. To determine the type and extent of internal protection required at an activity, prime consideration will be given to operational requirements. The following action should be taken in the order indicated:

a. Define and thoroughly analyze the areas to be protected including the nature and configuration of the school and installation. This will include the number of personnel involved, monetary and/or strategic value of material located therein, and other salient and limiting features which impact on security.

b. Assess the relative criticality and vulnerability of the installation and school(s) .

(1) Estimate effect of internal security measures on efficiency and operations for each measure.

(2) Estimate costs of security material and equipment to be installed, as well as availability of funds to provide adequate protection for all areas and activities.

(3) Identify the best security measures for the desired degree of security, efficiency, and cost effectiveness.

c. Evaluate potential damage and/or loss.

d. Identify alternate measures or techniques to eliminate deficiencies.

2. Each regional office, district office, and school must continually evaluate its position in the light of the above assessments and devise internal security measures consistent with the operating environment. When evaluating the degree and type of internal physical security required, it must be remembered that vulnerability and susceptibility may vary from time to time.

c. MINIMUM STANDARDS OF SECURITY

1. The security standards prescribed by this regulation and by the existing host installation security directives shall be used to develop a security program for each DoDDS activity.

2. Physical location or support deficiencies that may affect your DoDDS activity and require special attention to devise minimum security standards include the following:

a. Indication that the presence or mission of the military installation on which the DoDDS school is located or associated with, may attract significant hostility from elements of the host nation population or other disaffected group or individual. Care should be taken to avoid any speculation or record of elements of information that may be classified as National Security Information or politically sensitive in nature when making this assessment.

b. Indications that perimeter security is inadequate.

c. Indications that fences and/or lights are needed.

d. Disclosure that controls and checks of persons entering and leaving the installation are inadequate, thereby affecting school security.

e. Indications that communications, plans, and procedures to support installation security are inadequate, not exercised/tested periodically, or slow in response.

f. Evidence that unlawful or unauthorized activity is being practiced on the installation, or in the vicinity of or within the DoDDS activity. For example, a high crime rate that may include theft, illegal drugs, or black marketeering.

3. Internal physical security standards should be established for the following:

a. Indoctrination of personnel in the internal control procedures and the need for vigilance to prevent financial loss or loss of material resources.

b. Receipt, management, and disposition of equipment and supplies.

c. The maintenance and accuracy of accountable property inventories.

d. Receiving, holding, or storing legal tender currency or negotiable instruments.

e. Structural security criteria of school facilities.

f. Security guard personnel and the effectiveness and enforcement of their orders.

g. Communications.

h. Criteria for installation of intrusion detection systems and cost evaluation.

D. PHYSICAL SECURITY PLAN

1. Physical Security Plan. The DoDDS activities which are not located on U.S. Government installations and/or can not be incorporated in the host activity's physical security plan must develop a comprehensive physical security plan of their own. These plans should be coordinated through and developed with the assistance of the designated district security coordinator. Any interservice support agreements or assurances of host nation security and law enforcement support should be documented in this plan. The host installation or foreign base security official should be requested to provide a recommended security plan or assist security planning for schools located in off-base leased buildings.

2. Standard Procedures. The DoDDS activities that are tenants on U.S. Government installations having a physical security plan that includes physical security protection for tenant activities need not prepare a separate physical security plan. The DoDDS activities in this category will publish standard operating procedures (SOP's) which outline internal physical security procedures for their organization. Such SOP's will supplement the host installation's physical security plans. SOP's will be updated and submitted for review in the same manner as physical security plans.

KEY AND LOCK CONTROL PROCEDURES

A. KEY AND LOCK CONTROL

1. A regional key and lock control system encompassing all locks and keys used to secure U.S. Government property will be established for all the DoDDS activities. In designing the system, planners must be cognizant of the fact that locks are delay devices only. Their adequacy and effectiveness are only as good as the controls placed over the keys or combinations to open them. A key control system supplements other security measures used to control access to school facilities and offices. It is essential for the proper protection of facilities, and the equipment and material contained therein.

2. Keys to administrative offices, classrooms, storage areas, desks, lockers, etc., should be included in the internal security key and lock system.

3. The DoDDS activities that are tenants on U.S. Government installations or tenants in Government-owned or privately owned buildings will comply with the provisions of this section to the maximum extent possible, commensurate with the existing lease arrangements, security support agreements, and/or memoranda of understanding.

4. A key control officer will be designated in writing by the school principal or the head of an activity. The designee will be responsible for the overall supervision of the key and lock control program, the supply of locks and how they are stored, the issuance and handling of keys, records maintenance, investigation of lost keys, and maintenance and operation of key repositories .

5. Depending upon the size of the school or activity, a key and lock control system may consist of a single system or a number of subsystems. Each system and subsystem will have a designated custodian and a key repository.

6. The regional security officer and district security coordinator will monitor and enforce the key control system and will accomplish the following:

a. Advise the principal, key control officer, and key custodians on all matters relating to lock and key control systems.

b. Inspect the implemented systems during scheduled visits to each school.

c. Ensure that external locking devices are checked during nonduty hours by installation security personnel and that a contact person is identified to receive reports of violations, tampering, or illegal entry.

d. Review the local education program pertaining to key and lock control for adequacy.

7. DS Form 4701, Key Repository Index, will be maintained for each repository within the key and lock system. The index will be kept inside the repository to which it pertains and will be used as a basis for inventories of keys controlled from the repository.

8. All keys within the key and lock system must be accounted for at all times. This will be accomplished as follows:

a. The key repository will be located in a secure room, preferably the principal's or assistant principal's office, out of sight of casual visitors and not accessible to staff.

b. DS Form 4702, Key Repository Accountability Record, will be used to maintain accountability of each repository and the keys contained therein.

(1) If an individual signs out the repository key from the key control officer, an inventory of keys contained therein will be accomplished, using DS Form 4702. This individual will then complete the DS Form 4702, leaving the block entitled "SIGNATURE OF INDIVIDUAL RELIEVED OF RESPONSIBILITY" blank. The "REMARKS" block will be annotated, "Opening Inventory. " On return of the repository key, the procedure will be reversed. The block entitled "PRINTED NAME AND SIGNATURE OF INDIVIDUAL ASSUMING RESPONSIBILITY" will be left blank and the "REMARKS" block will be annotated "CLOSING INVENTORY. "

(2) Discrepancies detected during repository inventories will be annotated in the "REMARKS" block of the DS Form 4702, and will be reported immediately to the school key control officer.

c. DS Form 4703, Key Control Register, will be used by repository custodians to record the issue and turn-in of keys. A separate, up to date, DS Form 4703 will be locked inside the repository to which it pertains. All keys removed from, or returned to, the repository will be recorded on both copies of the Key Control Register.

9. Keys normally issued and used as a group will be affixed together, as a set, on metal rings. Each ring will include a metal or plastic tag stamped or imprinted with a ring identification code. Rings may be signed out by the identification code. However, the serial numbers of each key on the ring must be identified in the Key Repository Index, DS Form 4701.

10. All keys and padlocks within the key and lock control system, to include keys issued for personal retention, will be inventoried by serial number at least once every 6 months. A record of the inventory will be maintained by the key control officer until completion of the next scheduled inventory. Individuals or groups issued keys should be advised that government keys may not be duplicated.

11. Padlocks in use within the key and lock control system will be rotated at least once every 12 months.

12. Under no circumstances will a lock be left hanging open on a hasp, staple, hook, or other device. In all cases, locks will be relocked to the locking device immediately after opening, and the key will be removed. This action prevents surreptitious substitution of locks. Keys should not be issued to personnel employed by organizations other than the DoDDS for personal retention except in extenuating circumstances and under a memorandum of understanding delineating responsibilities for care of the U.S. Government property and facilities. Under no circumstances should non-DoDDS personnel be issued keys to controlled areas; e.g., computer rooms, media storage, principal's office, etc. Custodial service personnel should clean controlled areas prior to departure of the principal or responsible school/activity personnel.

B. KEY CONTROL ANNEX. Since each school or facility will have conditions and requirements peculiar to its activity, key control systems will vary. Before establishing a system, a survey should be conducted to determine actual requirements and to identify all classrooms, storage areas, safes, filing cabinets, etc., that require the additional protection afforded by locking devices and security of keys. When this determination is made, an annex to the physical security plan or standard operating procedures will be prepared which shows the following information:

1. Location of key repositories.
2. Keys (by building, area, or cabinet number) to be turned in to each repository.
3. Method of marking or tagging keys for identification.

4. Method of control of issue and receipt of keys, and identification of personnel authorized possession of keys.

5. Action required if keys are lost, stolen, or misplaced.

6. Frequency and method of lock rotation.

7. Assignment of responsibilities by job or position title.

8. Emergency type keys, which would be readily available to the installation security officer, district security coordinator, or regional security officer.

9. Other controls deemed necessary to facilitate the effectiveness of this particular key and lock control system.

Cancelled

IDENTIFICATION AND CONTROL MEASURES

A. PERSONNEL IDENTIFICATION AND CONTROL

A positive personnel identification and control system must be established and maintained in order to preclude unauthorized entry and facilitate authorized entry of personnel during the school or work day. Non-DoDDS activities that are given the privilege of using the DoDDS facilities after normal hours must be held responsible for limiting access to authorized persons. These non-DoDDS activities must have the school principal's approval for after hours access in accordance with reference (c) . Personal recognition, visitor identification badges, and personnel escorts are elements which contribute to the effectiveness of identification and control systems. The best control is provided when systems incorporate all of these elements. Simple, understandable, and workable identification and control measures and procedures should be utilized to achieve security "objectives without impeding efficient operations. Properly organized and administered, a personnel and movement control system provides a means not only of positively identifying those who have the right and need to enter or leave the facility, but also of detecting unauthorized personnel who attempt to gain entry. These objectives are achieved by:

- a. Initially determining who has a valid requirement to be in the school area.
- b. Limiting uncontrolled access to those persons who have that valid requirement.
- c. Establishing procedures for positive identification of persons within, and of persons authorized access into, areas.

B. VISITOR IDENTIFICATION AND CONTROL

1. The control of visitors is required for physical security, precaution against pilferage, student and employee protection, and prevention of vandalism. Visitors can generally be grouped into the following categories:

- a. Persons with whom every DoDDS activity must deal in connection with the conduct of its business; e.g. , contractors, authorized servicing vendors, parents, and military or civilian officials.
- b. Individuals or groups who desire to visit a DoDDS activity for a purpose that is not essential to, or necessarily

in furtherance of, its operations. Such visits may be desired, for example, by business, educational, technical, or scientific organizations, and individuals or groups desiring to further their particular interests.

c. Individuals or groups specifically sponsored by U.S. Government organizations such as foreign nationals visiting under school cooperation programs and similar visits by U.S. nationals. Requests for visits by foreign nationals should be processed in accordance with host installation procedures.

d. Guided tour visits to selected portions of installations in the interest of public relations.

2. Arrangements for the identification and control of visitors should include the following:

a. Positive methods to establish the authority for visitor access, as well as any limitations relative to access.

b. Positive identification of visitors by means of personal recognition, visitor permit, or other identifying credentials. The employee, supervisor, or principal should be contacted to ascertain the validity of the visit.

c. Use of DS Form 4704, "Visitors Register", which will provide a record of the identity of the visitor, the time and duration of the visit, and other pertinent control data.

d. Issuance of a visitor badge to all adult visitors. The badge should be worn on the outer clothing above waist level.

e. A control system to ensure that visitor identification cards or badges are recovered when the visit is concluded.

f. As a minimum, visitor identification badges should be logged and accountable and include:

(1) Name and address of the school being visited. This will facilitate return if a lost badge is recovered.

(2) A badge control number.

(3) Lamination or made of a durable substance to prevent easy alteration or mutilation.

(Note: A one-time visitor attendance list and group escort system may be used for large group activities instead of the normal visitor register and badge issuance system. Plans for large group activity visits should include adequate visitor parking.)

STORAGE OF FUNDS

A. APPLICABILITY

The standards and procedures in this section apply to all appropriated, nonappropriated (e.g., school activity funds), and other U.S. Government funds, negotiable instruments or accountable documents under the control of the DoDDS personnel or stored in the DoDDS facilities.

B. IMPREST FUNDS

Imprest funds will be controlled and secured in accordance with the procedures specified by the fiscal activity that issued the funds.

C. NONAPPROPRIATED FUNDS

Nonappropriated fund instrumentalities, such as the Army and Air Force Exchange Service, the Navy Resale and Support Services Office, or the Marine Corps Exchange Service, that operate facilities such as school cafeterias within a predominately DoDDS facility will be guided by the regulations of their respective agencies, but will not exceed the overnight funds storage limitations imposed for the DoDDS facilities.

D. FUNDS STORAGE LIMITATIONS DURING NONOPERATING HOURS.

1. The local finance activity will establish fund container requirements for imprest funds.

2. As a general rule, cash collections shall be deposited intact as of the close of each business day. In no case shall accumulations exceeding \$15,000.00 in negotiable instruments be stored overnight.

a. Accumulations of funds or negotiable instruments of less than \$7,500.00 may be stored overnight in a safe having a three-position dial combination lock, or a standard steel, insulated, and fire resistant file cabinet having a steel modified locking bar with a three-position dial combination lock.

b. Accumulations of funds or negotiable instruments above \$7,500.00, but less than \$15,000.00 must be stored in a General Service Administration (GSA) approved security container manufactured to Federal Specifications AA-F-357, AA-F-358, AA-F363B, and AA-F-1518. Locks for these GSA-approved security containers must meet Group 1 or 1R requirements specified in UL

Standard Number 768. This container must be placed in a designated funds storage room within the school that was approved by the host installation security officer. GSA-approved containers should have an external label indicating their approval, and an internal label which states the federal specifications it was manufactured under and the protection it affords.

(Note: Consult host installation security officials to obtain UL Standards and an evaluation of existing security containers).

E. FUND STORAGE CONTAINERS

1. Containers used to store U.S. Government or school activity funds will be certified as to their capability to protect funds. If the container does not meet GSA specifications, it must be certified by an Underwriter's Laboratory (UL) label (or foreign equivalent), as a burglar-resistant safe, and must be equipped with a "relocking device. "

2. Existing funds containers may be certified for continued use if, in the judgement of the installation security officer, they provide satisfactory protection. This certification should be reviewed each year during the annual host installation security inspection. As new or replacement containers are procured, they must meet GSA specifications for the storage desired.

3. Funds containers on casters or those that weigh less than 500 pounds and are not protected by an approved alarm system must be secured to the premises to prevent easy removal. Containers may be secured by fastening with bolts or heavy metal straps. Containers that may remain a permanent part of the structure may be embedded in concrete.

4. Position each container or container door, if possible, so that it may be seen through a window from outside the building. This facilitates after-hours security checks by host installation security personnel. During nonoperating hours, the immediate area of the container must be lighted.

F. COMBINATION SECURITY FOR VAULTS AND SAFES

1. Imprest Fund safe. The procedures will be the same as for the school activity fund safe except that in cases where the imprest fund is located some distance from the Accounting and Finance Office, the combination may be kept in the custody of the local installation commander. In the event of an emergency, the Accounting and Finance Officer or local installation commander, in the presence of a disinterested witness, is authorized to open the envelope containing the combination and then open the safe.

2. Opening Vaults and Safes. Carefully control the container combination and restrict it to the least number of persons. Change the combination annually or upon the relief, transfer, discharge, or separation of anyone who knows it or when it is compromised. When opening a vault or safe, the dial will be shielded so that the operation of the combination can not be observed by others.

Cancelled

SERIOUS INCIDENT REPORTING

When serious incidents occur, as listed below, a telephonic notification will be made to the applicable military law enforcement authorities and the DoDDS district and regional offices. In addition, a "DoDDS Serious Incident Report", DS Form 4705 (enclosure 8), will be completed and forwarded through the district and regional offices to ODE, Attention: Chief, Transportation, Safety & Security Branch, within 3 working days of the occurrence of any of the following incidents:

1. Arson or attempted arson.
2. Criminal assault and battery.
3. Bomb threat.
4. Possession or use of a weapon or prohibited item.

The definition of weapons and prohibited items are uniformly determined by jurisdictional directive. Report those incidents occurring on school grounds or off school grounds during bus transportation or at a DoDDS sponsored activity.

5. Other. This category is used for any incident considered by the school principal to be serious or sensitive enough to warrant rapid notification through district to region or ODE security and management personnel. Examples would include significant instances of drug use/dealing, gang violence, theft, vandalism, etc. , or situations, not listed, that could attract negative mass-media attention to the DoDDS.

ENCLOSURE 8 - FORMS

DS FORM 4701, KEY REPOSITORY INDEX
DS FORM 4702, KEY REPOSITORY ACCOUNTABILITY RECORD
DS FORM 4703, KEY CONTROL REGISTER
DS FORM 4704, VISITOR REGISTER
DS FORM 4705, DoDDS SERIOUS INCIDENT REPORT

Cancelled

KEY REPOSITORY INDEX		REPOSITORY NUMBER	LOCATION OF REPOSITORY
RING NUMBER	KEY SERIAL NUMBER	LOCK LOCATION (Building, Door, Cage Number, etc.)	NUMBER OF KEYS

Cancelled

KEY REPOSITORY ACCOUNTABILITY RECORD

REPOSITORY NUMBER

LOCATION OF REPOSITORY

THE UNDERSIGNED CERTIFIES THAT A JOINT INVENTORY OF THE KEYS MAINTAINED IN THIS REPOSITORY HAS BEEN CONDUCTED AND THAT ALL KEYS WERE ACCOUNTED FOR EXCEPT AS INDICATED IN REMARKS BELOW.

DATE	TIME	PRINTED NAME AND SIGNATURE OF INDIVIDUAL ASSUMING RESPONSIBILITY	SIGNATURE OF INDIVIDUAL RELIEVED OF RESPONSIBILITY	TOTAL NUMBER OF KEYS	INVENTORY STATUS (Check as Applicable)		REMARKS
					OPENING	CLOSING	

Cancelled

KEY CONTROL REGISTER

REPOSITORY NUMBER

LOCATION OF REPOSITORY

ISSUE		SERIAL NUMBER OF KEY(S)	TOTAL NUMBER OF KEYS	PRINTED NAME OF INDIVIDUAL RECEIVING KEY(S)		SIGNATURE OF INDIVIDUAL ISSUING KEY(S)	RETURN		PRINTED NAME OF INDIVIDUAL RECEIVING KEY(S)	
DATE	TIME			SIGNATURE	SIGNATURE		DATE	TIME	SIGNATURE	SIGNATURE

Cancelled

VISITORS

REGISTER

DATE	TIME-IN	VISITOR	BADGE NO.	PERSON/PIACE VISITING	AUTHENTICATING OFFICIAL	TIME-OUT

Cancelled

DoDDS SERIOUS INCIDENT REPORT

REGION/DISTRICT/SCHOOL NAME: _____

OF INCIDENT: _____

TIME OF INCIDENT: _____

INCIDENT OCCURRED:

TYPE OF INCIDENT:

ON SCHOOL GROUNDS
 OFF SCHOOL GROUNDS WHILE AT
ANY DoDDS-SPONSORED ACTIVITY
(INCLUDES BUS TRANSPORTATION)

ARSON OR ATTEMPTED ARSON
 CRIMINAL ASSAULT AND BATTERY
 BOMB THREAT
 WEAPON/PROHIBITED ITEM
 OTHER (REF. DS REG. 4700.2,
Enclosure 7)

NAME OF PARTICIPANTS

AGE

GRADE

PARTICIPANT STATUS
(SUBJECT/VICTIM/WITNESS)

NAME OF PARTICIPANTS	AGE	GRADE	PARTICIPANT STATUS (SUBJECT/VICTIM/WITNESS)
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

POLICE NOTIFIED BY: _____ DATE/TIME: _____

POLICE RESPONDED? YES- /NO_____ INVESTIGATION INITIATED? YES_ / N O _

DISTRICT NOTIFIED BY: _____ DATE/TIME: _____

REGION NOTIFIED BY: _____ DATE/TIME: _____

DESCRIBE IN DETAIL WHAT OCCURRED. STATE WHO, WHAT, WHEN, WHERE, AND HOW. LIST THE EXTENT OF ANY MONETARY LOSS AND FULLY DESCRIBE ANY WEAPON/PROHIBITED ITEM, IF APPLICABLE.

(USE REVERSE OF FORM OR ATTACH ADDITIONAL PAGES, IF NEEDED)

POLICE REPORT ATTACHED. POLICE/FINAL REPORT PENDING. NO POLICE INVOLVEMENT.
 NO FURTHER REPORTING ANTICIPATED FOR THIS INCIDENT.