



DEPARTMENT OF DEFENSE
EDUCATION ACTIVITY
4040 NORTH FAIRFAX DRIVE
ARLINGTON, VIRGINIA 22203-1635

MAR 27 2001

LOGISTICS

DoDEA REGULATION 4700.2

DEPARTMENT OF DEFENSE EDUCATION ACTIVITY
INTERNAL PHYSICAL SECURITY

- References: (a) DS Regulation 4700.2, "Department of Defense Dependents Schools Internal Physical Security," November 1993 (hereby canceled)
(b) DoDEA Regulation 4800.1, "Department of Defense Education Activity Safety Program," March 6, 2001
(c) DoD 1342.6-M, "Administrative and Logistic Responsibilities for DoD Dependents Schools," August 1995
(d) DoDEA Regulation 4700.1, Department of Defense Education Activity "Antiterrorism/Force Protection Program," July 6, 2000

1. REISSUANCE AND PURPOSE

This Regulation reissues reference (a) to update policy, responsibilities, and procedures for protecting the Department of Defense Education Activity (DoDEA) staff, students, and resources from criminal acts or conditions of vulnerability which could result in loss of life, destruction or loss of Government property, and disruption of DoDEA operations. This Regulation establishes minimum internal security standards designed primarily to deter criminal acts versus hostile acts of political turbulence or terrorism. This Regulation authorizes the publication of related pamphlets, manuals, or other media to assist in safeguarding the DoDEA personnel and resources.

2. POLICY

It is the DoDEA policy that all reasonable steps shall be taken to protect the DoDEA staff, students, and Government property by ensuring a secure environment at the DoDEA facilities and activities. All DoDEA employees should take appropriate action to correct conditions contributing to a poor security environment for DoDEA staff, students, and resources.

3. APPLICABILITY

The provisions of this Regulation apply to all DoDEA personnel responsible for, or concerned with, the protection of students, staff and resources from conditions which could result

in personal injury or death, property loss or destruction, or disruption of DoDEA operations. This Regulation applies to both the Department of Defense Dependents Schools and the Department of Defense Domestic Dependent Elementary and Secondary Schools.

4. RESPONSIBILITIES

4.1. The Director, DoDEA shall:

4.1.1. Ensure the implementation of internal physical security controls and procedures within the DoDEA.

4.1.2. Designate the DoDEA Security Programs Manager with oversight for the development, application, program assistance/reviews, and accountability outcomes for DoDEA policies, procedures, and standards pertaining to internal physical security.

4.1.3. Provide assistance to all schools and offices to achieve compliance with the provisions of this Regulation and other applicable **DoD** security directives.

4.2. The Deputy Directors shall:

4.2.1. Safeguard and protect the DoDEA students, personnel, visitors, and resources within their area of responsibility.

4.2.2. Designate the Area Safety and Security Officer to serve as the area point of contact for all physical security controls and procedures.

4.2.3. Implement internal physical security measures and procedures designed to minimize susceptibility to loss, destruction, or theft of Government-owned or leased property within their area of responsibility,

4.3. The Area Safety and Security Officer shall:

4.3.1. Manage the internal physical security program for their area of responsibility.

4.3.2. Monitor the serious incident reporting system and provide program assistance and guidance in problem resolution to districts and schools, as necessary.

4.3.3. Review internal physical security program implementation and compliance within the respective area (with spot checks at schools and/or districts), This-review includes coordination with CINCs and major service commands that transcend school district lines.

4.3.4. Provide assistance and guidance to District Safety and Security Officers to ensure program integrity and standards.

4.3.5. Coordinate with host nation and U.S. military command authorities to ensure both normal or increased law enforcement and security assistance as needed within the area.

4.4. District Superintendents shall:

4.4.1. Safeguard and protect the DoDEA students, personnel, visitors, and resources within the district.

4.4.2. Appoint the District Safety and Security Officer as the district point of contact for all internal physical security controls and procedures.

4.4.3. Implement internal physical security measures and procedures designed to minimize susceptibility to loss, destruction, or theft of Government-owned or leased property within their area of responsibility.

4.4.4. Report serious incidents. Monitor any further developments until all action is accomplished.

4.5. District Safety and Security Officers shall:

4.5.1. Provide guidance, assistance, and system oversight to Superintendents and Principals to ensure serious incidents are reported accurately and timely. Monitor incident data for trend analysis and management reporting within the district.

4.5.2. Visit each school annually to evaluate physical security controls and procedures. Analyze security deficiencies within the district and facilitate their correction or make recommendations for appropriate corrective actions.

4.5.3. Develop and/or administer security education programs for personnel within the district.

4.5.4. Maintain liaison with the Military Community security offices responsible for physical security inspection assistance.

4.5.5. Assist school administrators to develop internal security plans and procedures for internal physical security within the specific facilities.

4.5.6. Review security controls and procedures to ensure program implementation and compliance. This review should be combined with the safety program evaluation.

4.5.7. Coordinate with installation security officials to ensure that school security plans and procedures are coordinated with installation officials and that school and transportation operations are included in installation plans.

4.6. Principals shall:

4.6.1. Implement security controls and procedures to safeguard and protect the DoDEA students, personnel, visitors, and resources at the school level.

4.6.2. Develop internal school security controls and procedures using guidance from this Regulation and enclosures. Develop school specific emergency procedures using Personnel Emergency Alerting System (intercom) standard signals and/or voice notifications covering (but not limited to) fire evacuation, bomb threat evacuation, and lockdown procedures. Coordinate these emergency procedures with supporting host military installation or community security officials. Exercise fire evacuation procedures in accordance with DoDEA Regulation 4800.1, reference (b) and Life Safety Code requirements. Exercise bomb threat evacuation and lockdown procedures annually, in coordination with supporting community security officials.

4.6.3. Work cooperatively with host installation or community security officials, district or area administrators, school staff, and students to promote a security conscious attitude in all phases of the school's operation.

4.6.4. Schedule physical security inspections of school facilities by host installation or community security officials in accordance with DoD 1342.6-M, reference (c), and applicable Interservice Support Agreements. Physical security inspections should be conducted in concert with safety, bio-environmental, 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.

4.6.5. Maintain documentation on any corrective action needed as a result of facility inspections and the status of corrections. This documentation should be coordinated with the District Safety and Security Officer.

4.6.6. Ensure that staff receive training and applicable security awareness briefings on internal security procedures and the current state of local terrorist threat conditions and countermeasures in place for the school and local area. Students should receive security awareness training consistent with their ages, training materials provided, and the local threat.

4.6.7. Report serious incidents in accordance with Enclosure 6, "Serious Incident Reporting," and monitor and report any further developments until all action is accomplished.

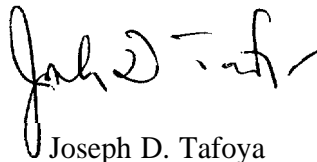
4.7. Teaching staff shall:

4.7.1. Become familiar with applicable school security controls, plans, and procedures developed for the security of staff, students, and resources.

4.7.2. Exercise applicable school security plans and procedures as directed by the Principal.

5. EFFECTIVE DATE

This Regulation is effective immediately.



Joseph D. Tafoya
Director

DISTRIBUTION: X

Enclosures – 7

E1. Definitions

E2. Physical Security Planning

E3. Key and Lock Control

E4. Visitor and Access Control

E5. Funds Control

E6. Serious Incident Reporting

E7. Forms

EI. ENCLOSURE 1

DEFINITIONS

- E1. Arson. The willful and malicious setting fire to or burning of any structure or property.
- E2. Assault with a Deadly Weapon. The use of a firearm, deadly weapon, or other instrument or by any other means of force likely to produce great bodily injury.
- E3. Battery. The willful and unlawful use of force or violence upon another person.
- E4. Bomb Threat. Any time there is a possibility that a bomb exists. Notification may be communicated in writing and/or verbally (may be telephonically).
- E5. Burglary. Any entry with the intent to commit a theft, even though force may not have been used to gain entry.
- E6. 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.
- E7. 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.
- E8. 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.
- E9. Destructive Devices. Any projectile containing any explosive or incendiary material or any chemical substance; bomb; facsimile bomb; breakable container which contains a flammable liquid with a wick or similar device capable of being ignited; and any sealed device containing any chemically reactive substances.
- E10. Drug/Alcohol Offenses. Incidents involving the possession, use, sale, or furnishing of any drug, alcohol, or intoxicating substance, as well as drug paraphernalia, that is prohibited by law.

E1 1. Explosive Devices. Any substance, or combination of substances, the primary common purpose of which is detonation or rapid combustion.

E12. Extortion. Threat of force or wrongful use of fear to take the property **from** another person without his or her consent.

E13. Firearm. A weapon consisting of a tube that shoots a projectile at high velocity, especially a pistol, rifle, or shotgun, using an explosive charge as a propellant.

E14. Force Protection. Security program developed to protect Service members, civilian employees, family members, facilities and equipment, in all locations and situations, accomplished through the planned and integrated application of combating terrorism, physical security, operations security, personal protective services supported by intelligence, counterintelligence, and other security programs.

E15. Graffiti. Any form of unauthorized painting, writing, or inscription on another's property regardless of the content or nature of the material used in the commission of the act.

E16. Homicide. The unlawful killing of a person by another person.

E17. Loitering. To linger or to idle about without lawful business for being present.

E18. Master/Sub-Master Key. A key or keys that will operate a number of different locks, each of which is different.

E19. Other Users. Any individual or organization outside of the DoDEA that is authorized to use the DoDEA facilities.

E20. "Other" Weapon. Includes knives with blades over 3 inches long or with lock-in-place blades of any length, but do not include typical Swiss Army type knives, small folding pocket knives, or pen knives with blades less than 3 inches long; BB, or pellet guns; a realistic looking "replica" firearm.

E21. Personnel Emergency Alerting System. A mechanical or electronic notification system physically installed in every building and room housing staff or students, designed to provide positive signal and/or voice notification of an emergency nature to all staff and students. This emergency alerting system is generally associated with an intercom system.

E22. 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.

E23. Pilferable Items. Material having a ready resale value, civilian utility or personal application and, therefore, susceptible to theft.

E24. Repository. A secure container or metal key box for the controlled storage of keys and locks used within the Key and Lock Control System.

E25. Robbery. Taking the property in possession of another, from his or her person or immediate presence, and against his or her will, accompanied by force or fear.

E26. Safe. A General Services Administration approved security container equipped with a re-locking device.

E27. Sex Offenses. Incidents including sexual battery, rape, statutory rape, sodomy, lewd and lascivious conduct, oral copulation, and child molestation.

E28. Tabletop Exercise. An exercise of plans or procedures by gathering representatives of all key participants to a planned scenario. These participants review exercise plans and procedures, discuss varying scenarios and plan accordingly to address practical alternatives.

E28. 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.

E29. 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.

E30. Theft. Taking, leading, driving, or carrying away of property belonging to another with the intent to deprive the rightful owner of its use.

E31. Threats of Extreme Violence. Written, verbal, internal, and/or external threats by students or others that are of a violent nature.

E32. Trespassing. Entry without registering with the site or program administrator. Remaining after being asked to leave, or returning after being asked to leave.

E33. Vandalism. The malicious defacing, damaging, or destroying of facilities, equipment, or material.

E34. Vault. A strongly built chamber for preserving items of ~~considerable~~**worth** or value.

E35. Visitor. **Any** individual, military or civilian, not assigned to or employed within a school or activity to which access is requested.

E2. ENCLOSURE 2

PHYSICAL SECURITY PLANNING PROCEDURES

E2.1. INTERNAL EMERGENCY SECURITY PLANNING

DoDEA operates schools worldwide, in varying and ever changing threat environments. Internal physical security plans and procedures are designed primarily to deter criminal acts of **theft**, destruction, and violence. However, these plans and procedures complement the **antiterrorism** planning and **countermeasures** found in DoDEA Regulation 4700.1, reference (d). Basic to the formulation of internal security controls is the determination of what is to be protected and the degree of protection to be accorded. This is a very site specific process in which the security interest and security measures of an activity are affected by the changing environment in which they operate.

E2.2. PLANNING CONSIDERATIONS

E2.2.1. All schools should have an internal communication system capable of transmitting signals and voice notifications throughout campus locations housing students and staff. This system is usually an intercom and alarm type system and is known in security terminology as a Personnel Emergency Alerting System (PEAS). Site specific internal security plans and procedures using emergency notification through PEAS should address, at a minimum, the following areas:

E2.2.1.1. Emergency fire evacuation. Establish specific notification signals, evacuation routes, holding areas, and contingency plans for student/staff needs, etc.

E2.2.1.2. Emergency bomb threat evacuation. Establish specific notification signals, evacuation routes, holding areas, and contingency plans for student/staff needs, etc. Note: Holding areas for bomb threat evacuations should not be adjacent to parked vehicles. It is much easier to hide a bomb in a vehicle and then place a bomb threat call to trigger an evacuation to the vehicle than it is to hand carry a bomb into the building.

E2.2.1.3. Emergency **lockdown** procedures. Establish specific notification signals and/or verbal codes to indicate the nature and possible location of any hostile or violent emergency affecting the school. Emergencies that may trigger a **lockdown** situation may come from outside or inside the school. **Lockdown** scenarios may include violent outside criminal activity where authorities want to prevent a criminal from taking refuge in the school; a deranged

or violently distraught adult threatening staff or students at the entrance or inside the school; or an equally deranged or violently distraught student in the school. In an emergency lockdown, the following areas should be considered in planning effective procedures:

E2.2.1.3.1. All students must be cleared **from** hallways and directed into internal rooms.

E2.2.1.3.2. Bathrooms and utility type rooms should be cleared of students and locked, if possible, by staff members.

E2.2.1.3.3. Classes/persons caught outside, such as Gym, recess, or other activities, should either re-enter the school, take available cover, or evacuate to a safer area depending on the nature and location of the threat.

E2.2.1.3.4. All internal rooms should have locks that can be key activated **from** inside the room by the classroom teacher or assigned staff member.

E2.2.1.2.5. Internal room doors that have windows should have **draw-**down shades on the inside that can be pulled down to restrict viewing during a lockdown.

E2.2.1.3.6. Teachers are encouraged to continue teaching or engage interactively with students to prevent undue speculation or panic.

E2.2.1.3.7. Students should be kept away from doors and windows and should take available cover on the floor if gunshots or explosions are heard.

E2.2.1.3.8. Students should not be allowed to leave the classroom, or other rooms locked down in an emergency, for any reason – bathroom break or otherwise – except as directed by the main administrative office, which will act as a control center, or by emergency response personnel.

E2.2.1.3.9. To avoid the spread of panic, and to avoid spreading or picking up erroneous information on the crisis, no use of radios, television, or cellular phones should be permitted.

E2.2.1.3.10. Establish an “all clear” signal accompanied by a verbal confirmation code.

E2.2.1.3.11. Coordinate lockdown plans with local security officials and perform a joint **tabletop** exercise and then a practical exercise with staff and local security officials annually.

E2.2.1.4. Natural disasters and other emergency notifications. Plan for natural disasters associated with your location, such as tornadoes or earthquakes which may have little or no warning. Natural disaster plans should be coordinated with the local military Disaster Preparedness Office, which will also coordinate for mass casualties. Also coordinate with local command officials to determine if any military emergency notifications should be planned for emergency school procedures. Examples of this may be notifications of pending flood, hurricane, typhoon or other natural disaster. The local military command may have other emergency warning or attack signals, such as chemical/biological warning signals which may indicate an industrial chemical accident, chemical/biological attack, or other threat against the installation, etc.

E2.3. INTERNAL SECURITY CONTROLS AND PROCEDURES

E2.3.1. In addition to the previously listed emergency procedures, physical security controls and procedures shall be established, or followed in accordance with this Regulation, for the following areas:

E2.3.1.1. Key and lock control. (See Enclosure E3 for further guidance).

E2.3.1.2. Visitor and access control. (See Enclosure E4 for further guidance).

E2.3.1.3. Funds control. (See Enclosure E5 for further guidance).

E2.3.1.4. Serious incident reporting. (See Enclosure E6 for further guidance).

These emergency plans and procedures and internal security controls and procedures listed in Enclosure E2 shall constitute the minimum required internal physical security guidance. This guidance shall be provided to staff for familiarization and exercise where applicable.

E3. ENCLOSURE 3

KEY AND LOCK CONTROL

E3.1. KEY AND LOCK CONTROL

E3.1.1. A key and lock control system encompassing all locks and keys used to secure U.S. Government property will be established for all the DoDEA activities. In designing the system, planners must be cognizant of the fact that locks are only delay devices. 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 schools, facilities, and offices. This control system is essential for the proper protection of facilities, and the equipment and material contained therein.

E3.1.2. Keys to administrative offices, classrooms, storage areas, desks, storage lockers, etc., should be included in the internal security key and lock control system.

E3.1.3. The DoDEA 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.

E3.1.4. The office manager or school principal is ultimately responsible for all key and lock controls for each respective activity. However, a staff member may be designated in writing as key control officer (may also be known as the key custodian) responsible for the daily operation of the key and lock control system. 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.

E3.1.5. 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 key control officer and a key repository.

NOTE: Equivalent key and lock control systems (such as modified automated or hardcopy systems) other than outlined here are authorized but must be individually approved for use by the District Safety and Security Officer. Equivalent control systems must meet the intent and control afforded by the controls outlined in this Regulation. Mechanical card access systems using magnetic coding has also proven to be very durable, manageable, and cost effective at the school

level as the need for rekeying is drastically reduced or eliminated. However, product availability and maintenance support varies from area to area, so research should be conducted prior to commitment to nontraditional locking systems.

E3.1.6. The District Safety and Security Officer shall review the key and lock control system and will accomplish the following:

E3.1.6.1. Advise the principal and the key control officer on all matters relating to lock and key control systems.

E3.1.6.2. Inspect the implemented systems during scheduled school visits. Evaluate any key and lock control systems other than those provided here for adequacy. NOTE: Automated control systems must be password controlled, routinely backed up to controlled disks, and may not be resident on networked drives.

E3.1.6.3. Ensure that external locking devices are checked during non-duty hours by installation security personnel and that a contact person is identified to receive reports of violations, tampering, or illegal entry.

E3.1.7. DS Form 4701, Key Repository Index, or its equivalent, will be maintained for each repository within the key and lock system. The index will be kept inside the repository, or under equivalent safeguards, and will be used as a basis for inventories of keys controlled from the repository.

E3.1.8. Distribution of master and sub-master keys must be strictly controlled. A useful guide in determining this distribution is to issue master and sub-master keys only to those persons that would be routinely expected to respond during non-duty hours for emergency access to multiple offices or school areas. After this careful and considered distribution of keys, all keys within the key and lock system must be accounted for at all times. This will be accomplished as follows:

E3.1.8.1. 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.

E3.1.8.2. DS Form 4702, Key Repository Accountability Record, or its equivalent, will be used to maintain accountability of each repository and the keys contained therein.

E3.1.8.2.1 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, or its equivalent. This individual will then complete the DS Form 4702, or its equivalent,

leaving the block titled “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 titled “PRINTED NAME AND SIGNATURE OF INDIVIDUAL ASSUMING RESPONSIBILITY” will be left blank and the “REMARKS” block will be annotated “CLOSING INVENTORY.”

E3.1.8.2.2 Discrepancies detected during repository inventories will be annotated in the “REMARKS” block of the DS Form 4702, or its equivalent, and will be reported immediately to the school key control officer.

E3.1.8.3. DS Form 4703, Key Control Register, or its equivalent, will be used by the key control officer to record the issue and turn-in of keys. A separate, up to date, DS Form 4703, or its equivalent 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.

E3.1.9. 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 470 1, or its equivalent.

E3.1.10. All keys and padlocks within the key and lock control system, to include keys issued for personal retention, will be inventoried by serial number annually. 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.

E3.1.11. Padlocks in use within the key and lock control system will be rotated once every 12 months.

E3.1.12. 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 DoDEA 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-DoDEA 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.

E3.2. 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, tiling 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 shall be prepared which shows the following information:

E3.2.1. Location of key repositories.

E3.2.2. Keys (by building, area, or cabinet number) to be turned in to each repository.

E3.2.3. Method of marking or tagging keys for identification.

E3.2.4. Method of control of issue and receipt of keys, and identification of personnel authorized possession of keys.

E3.2.5. Action required if keys are lost, stolen, or misplaced.

E3.2.6. Frequency and method of lock rotation.

E3.2.7. Assignment of responsibilities by job or position title.

E3.2.8. Emergency type keys, which would be readily available to the installation security officer, district security coordinator, or area service center security officer.

E3.2.9. Other controls deemed necessary to facilitate the effectiveness of this particular key and lock control system.

E4. ENCLOSURE 4

VISITOR AND ACCESS CONTROL

E4.1. PERSONNEL IDENTIFICATION AND CONTROL

A positive personnel identification and control system must be established and maintained in order to prevent unauthorized entry to offices or schools. Non-DoDEA activities or “other users” that are given the privilege of using the DoDEA facilities after normal hours must be held responsible for limiting access to authorized persons. These non-DoDEA activities must have the school principal’s approval for after hours access in accordance with DoD 1342.6-M, 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 used 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:

E4.1.1. Initially determining who has a valid requirement to be in the school area or DoDEA facility.

E4.1.2. Limiting uncontrolled access to those persons who have that valid requirement.

E4.1.3. Establishing procedures for positive identification of persons seeking access to offices or schools.

E4.1.4. Prominently displaying signs to notify visitors that visitor control procedures are in effect, to direct visitors through the administrative office for visitor control, and to establish the basis for trespassing (or equivalent) charges if control procedures are circumvented and charges are deemed necessary.

E4.2. VISITOR IDENTIFICATION AND CONTROL

E4.2.1. The control of visitors is required for physical security, precaution against pilferage, student and employee protection, and prevention of vandalism. However, visitors can

not be adequately controlled if the school administrative office or administrative personnel are not positioned to provide oversight of the main school entrance. Therefore, the positioning of administrative offices for oversight of the main school entranceway should be a priority for security funding. Visitors can generally be grouped into the following categories:

E4.2.1.1. Persons with whom every DoDEA activity must deal in connection with the conduct of its business; e.g., contractors, authorized servicing vendors, parents, and military or civilian officials.

E4.2.1.2. Individuals or groups who desire to visit a DoDEA 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.

E4.2.1.3. 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.

E4.2.1.4. Guided tour visits to selected portions of installations in the interest of public relations.

E4.2.2. Arrangements for the identification and control of visitors should include the following:

E4.2.2.1. Positive methods to establish the authority for visitor access, as well as any limitations relative to access.

E4.2.2.2. 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.

E4.2.2.3. 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.

E4.2.2.4. Issuance of a visitor badge to all adult visitors.- The badge should be worn on the outer clothing above waist level.

E4.2.2.5. A control system to ensure that visitor identification cards or badges are recovered when the visit is concluded.

E4.2.2.6. As a minimum, visitor identification badges should be logged and accountable and include:

E4.2.2.6.1. Unique badge color so it can be easily recognized from a distance.

E4.2.2.6.2. Name and address of the DoDEA school or facility being visited. This will facilitate return if a lost badge is recovered.

E4.2.2.6.3. A badge control number and the word "VISITOR."

E4.2.2.6.4. 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 personal escorts and adequate visitor parking.)

E5. ENCLOSURE 5

FUNDS CONTROL

E5.1. APPLICABILITY

The standards and procedures in this section apply to all appropriated, non-appropriated (e.g., school activity funds), and other U.S. Government funds, negotiable instruments (bonds, credit cards, traveler's checks, checkbooks, etc.) and objects classified as having an intrinsic value requiring additional protection. Objects such as wallets, snapshots, keys, letters, etc., will not be accepted for safekeeping. Funds and negotiable instrument shall not be stored in the same security containers as classified material.

E5.2. NON-APPROPRIATED FUNDS

A non-appropriated fund instrumentality, 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 DoDEA facility will be guided by the regulations of their respective agencies, but will not exceed the overnight funds storage limitations imposed for the DoDEA facilities.

E5.3. FUNDS STORAGE LIMITATIONS DURING NONOPERATING HOURS.

E5.3.1. 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 in negotiable instruments be stored overnight.

E5.3.1.1. Accumulations of funds or negotiable instruments of less than \$7,500 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.

E5.3.1.2. Accumulations of funds or negotiable instruments above \$7,500, but less than \$15,000 must be stored in a General Services Administration (GSA) approved security container manufactured to Federal Specifications AA-F-357, AA-F-358, AA-F363B, and AA-F-15 18. 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).

E5.4. FUND STORAGE CONTAINERS

E5.4.1. 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."

E5.4.2. 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.

E5.4.3. Funds containers 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.

E5.4.4. 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 non-operating hours, the immediate area of the container must be lighted.

E5.5. COMBINATION SECURITY FOR VAULTS AND SAFES

E5.5.1. 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 cannot be observed by others. Consult host installation security officials for combination storage procedures if outside storage of the school's security container combinations are desired by administration or required locally.

E6. ENCLOSURE 6

SERIOUS INCIDENT REPORTING

E6.1. SERIOUS INCIDENT REPORTS (SIR)

E6.1.1. Reportable serious incidents should consist primarily of alleged or suspected crimes versus lesser school misconduct or prohibited items issues. Lesser misconduct type disciplinary issues should be reported through student information management systems such as Win School or equivalent systems.

E6.1.2. When serious incidents occur involving suspected crimes, as listed below, a telephonic notification requesting assistance and/or reporting the incident shall be made to the applicable law enforcement authorities.

E6.1.3. These time-sensitive serious incidents, involving suspected crimes, negative media/community attention, or other sensitive incidents should generate an immediate initial notification up-channel to higher management. For these initial, rapid internal notifications, an e-mail text message describing the initial incident, with the information available, should be immediately forwarded, as a minimum, to the Safety and Security Office at the District, Deputy Director, and DoDEA HQ levels to provide rapid higher management notifications.

E6.1.4. As a follow-up to these time-sensitive e-mail notifications and for reports that are not time sensitive, a “DoDEA Serious Incident Report (SIR),” DoDEA Form 4705 (enclosure 7), will be completed (normally at the school level), attached to an e-mail message, and forwarded to the District Safety and Security Office. This SIR should be forwarded by the school as soon as details are available to complete the report format, usually within 5 working days of the incident occurrence. District Safety and Security Officers should review the DoDEA Form 4705 for accuracy and log or retain a copy for district trend analysis prior to forwarding the finished report to the Deputy Director’s Safety and Security Office. The Deputy Director’s Safety and Security Office should review the DoDEA Form 4705 and log or retain a copy for area trend analysis before forwarding the report to the DoDEA Safety and Security Office for statistical management.

E6.1.5. The following reporting categories and incidents will encompass the majority of DoDEA serious incident reports:

E6.1.5.1. Drug/Alcohol Offenses.

E6.1.5.1.1. Use of Drugs/Alcohol.

E6.1.5.1.2. Possession of Drugs.

E6.1.5.1.3. Possession of Alcohol.

E6.1.5.1.4. Possession of Drug Paraphernalia.

E6.1.5.1.5. Possession of Drugs/Alcohol for Sale.

E6.1.5.1.6. Sale and/or Furnishing of Drugs/Alcohol.

E6.1.5.2. Crimes Against Persons.

E6.1.5.2.1. Battery.

E6.1.5.2.2. Assault with a Deadly Weapon.

E6.1.5.2.3. Homicide.

E6.1.5.2.4. Robbery/Extortion.

E6.1.5.2.5. Sex Offenses.

E6.1.5.3. Crimes Against Property.

E6.1.5.3.1. Personal Property Theft (over \$100 loss).

E6.1.5.3.2. Government Accountable Property Theft (generally, property identified with bar-coded property tags).

E6.1.5.3.3. Vandalism (over \$500 loss).

E6.1.5.3.4. Graffiti (over \$500 loss).

E6.1.5.3.5. Arson.

E6.1.5.3.6. Burglary.

E6.1.5.4. Security Threats (affecting the school, staff, students, or operations).

E6.1.5.4.1. Bomb Threat.

E6.1.5.4.2. Force Protection.

E6.1.5.4.3. Threats of Extreme Violence.

E6.1.5.5. "Other" Incidents.

E6.1.5.5.1. Destructive/Explosive Devices.

E6.1.5.5.2. Loitering/Trespassing.

E6.1.5.5.3. Possession of an Actual Firearm.

E6.1.5.5.4. Possession of "Other" Weapon. NOTE: Definitions of weapons are uniformly determined by jurisdictional Service Component Directives. Whenever a question arises as to whether a device is legally classified as a weapon, the supporting Command law enforcement authority interpretation will prevail. Knives with blades less than 3 inches long are school prohibited items and should be reported via student information management systems for disciplinary statistics.

E6.1.5.5.5. Other. Any incident which the reporting official feels may be considered to be serious or sensitive enough to warrant a detailed report for the record to be forwarded to the respective district, Deputy Director, and DoDEA management personnel. This would include incidents which may not fit comfortably within the categories listed above, but which may develop into incidents of negative media attention or other issues felt by the reporting official to warrant a report for the record.

E7. ENCLOSURE 7

FORMS

E7.1. Associated Internal Physical Security Program forms are listed below:

E7.1.1. DoDEA FORM 4701, KEY REPOSITORY INDEX
(Attached and developed in MS Word format)

E7.1.2. DoDEA FORM 4702, KEY REPOSITORY ACCOUNTABILITY RECORD
(Attached and developed in MS Word format)

E7.1.3. DoDEA FORM 4703, KEY CONTROL REGISTER
(Attached and developed in MS Word format)

E7.1.4. DoDEA FORM 4704, VISITOR REGISTER
(Attached and developed in MS Word format)

E7.1.5. DoDEA FORM 4705, DoDEA SERIOUS INCIDENT REPORT
(Attached and developed in MS Word format)

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

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 MM/DD/YY	TIME HH:MM	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	

KEY CONTROL REGISTER				REPOSITORY NUMBER	LOCATION OF REPOSITORY				
ISSUE DATE MM/DD/YY		TIME HH:MM	SERIAL NUMBER OF KEY(S)	TOTAL NUMBER OF KEYS	PRINTED NAME AND SIGNATURE OF INDIVIDUAL RECEIVING KEY(S)	SIGNATURE OF INDIVIDUAL ISSUING KEY(S)	RETURN DATE MM/DD/YY	TIME HH:MM	PRINTED NAME AND SIGNATURE OF INDIVIDUAL RECEIVING KEY(S)

VISITORS REGISTER

DATE MM/DD/YY	TIME-IN HH:MM	VISITOR	BADGE NO.	PERSON/PLACE VISITING	AUTHENTICATING OFFICIAL	TIME-OUT HH:MM

DoDEA SERIOUS INCIDENT REPORT

AREA:	DISTRICT:	SCHOOL NAME:
DATE OF INCIDENT:		TIME OF INCIDENT:
INCIDENT OCCURRED: <input type="checkbox"/> ON SCHOOL GROUNDS <input type="checkbox"/> OFF SCHOOL GROUNDS (Enroute to or from school or while at a school sponsored activity)		

TYPE OF INCIDENT
(Refer to DR 4700.2, Enclosure 1, Definitions)

DRUG/ALCOHOL OFFENSES <input type="checkbox"/> Use of Drugs/Alcohol <input type="checkbox"/> Possession of Drugs <input type="checkbox"/> Possession of Alcohol <input type="checkbox"/> Possession of Drug Paraphernalia <input type="checkbox"/> Possession of Drugs/Alcohol for Sale <input type="checkbox"/> Sale and/or Furnishing of Drugs/Alcohol <input type="checkbox"/> "Other" Drug/Alcohol Offenses	CRIMES AGAINST PERSONS <input type="checkbox"/> Battery <input type="checkbox"/> Assault with a Deadly Weapon <input type="checkbox"/> Homicide <input type="checkbox"/> Robbery/Extortion <input type="checkbox"/> Sex Offenses <input type="checkbox"/> "Other" Crimes Against Persons
---	---

CRIMES AGAINST PROPERTY <input type="checkbox"/> Personal Property Theft (over \$100 loss) <input type="checkbox"/> Govt. Accountable Property Theft (generally, bar-coded property) <input type="checkbox"/> Vandalism (over \$500 loss) <input type="checkbox"/> Graffiti (over \$500 loss) <input type="checkbox"/> Arson <input type="checkbox"/> Burglary <input type="checkbox"/> "Other" Crimes Against Property	SECURITY THREATS (Affecting School, Staff, Students, or Operations) <input type="checkbox"/> Bomb Threat <input type="checkbox"/> Force Protection Issues (i.e., suspected surveillance or other suspicious or actual activity constituting a threat or potential threat to students, staff, or operations) <input type="checkbox"/> Threats of Extreme Violence (i.e., written, verbal, internal or external, by students or others) <input type="checkbox"/> "Other" Security Threats
---	--

OTHER INCIDENTS

Destructive/Explosive Devices
 Loitering/Trespassing
 Possession of an Actual Firearm

Possession of "Other" Weapon (i.e., report knife with 3 inch blade or lock-in-place blade/razor of any length, BB/Pellet guns or realistic "replica" guns, nun-chucks, clubs, and other items possessed or used to inflict bodily **harm**. Whenever a **question arises** as to whether a device is a legally classified "weapon," the supporting Command/host law enforcement authority interpretation will prevail.

Other (Use this area to record those incidents which do not fit comfortably within the categories listed above, but which may develop into incidents of negative media attention or other issues felt by the reporting **official** to warrant a report for the record.

PARTICIPANTS (List name as last, first, MI)	GENDER (M/F)	AGE	GRADE	STATUS (Subject/Victim/Witness)

NOTIFICATIONS: Police District Area DoDEA HQ
 Police Responded? Yes No Police Investigating? Yes No
 Notifications made/coordinated by: _____

DESCRIBE IN DETAIL WHAT OCCURRED. STATE WHO, WHAT, WHEN, WHERE, & HOW. EXTENT OF ANY MONETARY LOSS, DETAILS OF ANY WEAPON, ETC.

FOR OFFICIAL USE ONLY
(When filled in)