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

MAY 20 2002

Information Technology

DoDEA Administrative
Instruction 6700.8

DEPARTMENT OF DEFENSE EDUCATION ACTIVITY COMPUTER AUDIT TRAILS

References: (a) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988
(b) Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510, "Department of Defense Global Information Grid Information Assurance," June 16, 2001

1. PURPOSE

This Administrative Instruction (AI) establishes policy, assigns responsibility, and prescribes procedures under references (a) and (b) for establishing and maintaining computer audit trails.

2. APPLICABILITY AND SCOPE

The provisions of this AI apply to the Department of Defense Education Activity (DoDEA) Headquarters and all locations under the cognizance of its components, the Department of Defense Dependents Schools (DoDDS), and the Department of Defense Domestic Dependent Elementary and Secondary Schools (DDESS)/ Cuba.

3. DEFINITIONS

3.1 Audit: The examination of records or accounts.

3.2 Audit Trail: The examination of records that track an individual's access to computers and files, or their attempts to modify, bypass, or negate safeguards controlled by the system.

4. POLICIES AND PROCEDURES

4.1 It is the policy of the DoDEA that safeguards shall be in place to ensure that each person gaining legal or illegal access to a DoDEA computer system is held accountable for their actions on the system.

4.2 It is also the policy of DoDEA to collect and retain audit data to support forensics relating to misuse, penetration reconstruction, or other investigations.

4.3 The audit trail records shall be of sufficient detail to reconstruct events to determine the cause or magnitude of compromise or damage, if a security violation or malfunction should occur. Audit trails will document the following:

- The identity of each person's account and device accessing the system.
- The date and time of the access.
- All successful and unsuccessful attempts by a user to:
  - Access a system
  - Access a file
  - Add or remove hardware or software
- User activity sufficient to ensure that the user actions are controlled and open to scrutiny.
- Activities that might modify, bypass, or negate safeguards controlled by the system.
- Security-relevant actions associated with periods of processing or the changing of security levels or categories of information.

4.4 Audit trail records will not be filed by name or personal identifier.

5. RESPONSIBILITIES

5.1 The DoDEA Headquarters' Chief Information Officer; Director, DoDDS-Europe; Director, DoDDS-Pacific, and Director, DDESS/Cuba shall ensure that appropriate procedures are in place to record and maintain audit trails to document DoDEA automated information systems use.

5.2 Designated Approval Authorities (DAAs) shall ensure periodic reviews of at least every 6 months to be made of audit trails associated with AIS(s) over which the DAA has cognizance.

5.3 System administrators shall

5.3.1 Collect, retain, and ensure the integrity of the audit trail data.

5.3.2 Develop a formalized plan detailing the process, by which they will create, maintain, and store comprehensive audit trails.

5.3.3 Submit this plan to the local DAA within 60 days of this issuance and the process will be reviewed at least annually.

5.3.4 Retain audit trail data in an approved storage container for a period of not less than one full calendar year.

5.4 General Counsel, DoDEA will advise the DAA or designee, upon request, when an audit begins to focus on an individual and an investigation is opened on an individuals use of IT equipment.

6. EFFECTIVE DATE

This policy memorandum is effective immediately.

Joseph D. Tafoya
Director