IM-93-1 ADP System Security Requirements and Review Process - Federal Guidelines

Office of Information Systems Management

U.S. Department of Health and Human Services
Administration for Children and Families
Washington, D.C. 20447

Information Memorandum #: OISM-IM-93-1 ***Date: October 1, 1992***

TO: **State Public Assistance, Child Support Enforcement and Medicaid Agencies and other interested parties.**

Subject: ADP System Security Requirements and Review Process - Federal Guidelines

Related References: 45 CFR Part 95, Subpart F, Section 95.621

Purpose: In order to assist States in meeting the security requirements of 45 CFR Part 95, DHHS is attaching a guidance document which provides a description of what we consider appropriate for a State to address in its written security summary of findings and determination of compliance with Part 95 requirements. This information is intended as guidance and is not to be used as an outline or checklist. Each State's security program is unique, possessing features necessitated by singular data processing environments.

Background: State public assistance agencies are responsible for the security of all developmental or operational Federally funded automatic data processing (ADP) systems. These systems are subject to the provisions of 45 CFR Part 95, Subpart F.

On February 7, 1990, the Department of Health and Human Services (DHHS) published final rules at 45 CFR Part 95, Subpart F and the Department of Agriculture, Food and Nutrition Service (FNS), published final rules at 7 CFR Part 277 in the *Federal Register*. See 55 FR 4364. These regulations became effective on May 8, 1990, and included new provisions for establishing minimum standard requirements for the security of systems used to administer programs covered under these rules.

<u>State Responsibility to Establish ADP Security Program</u>

Under 45 CFR 95.621 each State is responsible for the security of all ADP projects under development and all operational systems used by State and local governments to administer programs covered under 45 CFR Part 95, Subpart F. This regulation requires that State agencies shall (1) determine the appropriate ADP security requirements based on recognized industry standards or standards governing security of Federal ADP systems and information

processing; (2) implement appropriate security requirements; (3) establish asecurity plan and, as appropriate, policies and procedures to address the areas of ADP security at 95.621(f)(2)(ii); (4) establish and maintain a program for conducting periodic risk analyses; and (5) conduct a biennial ADP system security review of installations involved in the administration of DHHS programs which, at a minimum, includes an evaluation of physical and data security operating procedures, and personnel practices. This requirement applies to all ADP systems used by State and local governments to administer programs covered under 45 CFR Part 95, Subpart F.

On January 10, 1991, the former Family Support Administration (FSA) and the Food and Nutrition Service (FNS) jointly issued Action Transmittal FSA-AT-91-2. That Action Transmittal established that biennial reviews for existing systems must be completed and reported to DHHS and FNS by October 1, 1992 and every two years thereafter.

State Responsibility to Conduct Biennial ADP System Security Review

The biennial reviews for existing systems must be completed and reported to DHHS and FNS by October 1, 1992 and every two years thereafter. For new ADP applications, reviews must be conducted upon implementation and every two years thereafter. After completing the required biennial ADP system security review, Heads of State agencies must provide a written summary of findings and a determination of compliance with the Part 95 ADP security requirements. In their reports to DHHS and FNS, States must include written summaries of their ADP security programs and action plans with the scheduled dates of milestones which, when the appropriate safeguards are properly implemented, will protect against identified threats. States also must certify compliance of their ADP Security Program in the following areas:

A. Physical security of ADP resources;

B. Equipment security to protect equipment from theft and unauthorized use;

C. Software and data security;

D. Telecommunications security;

E. Personnel security;

F. Contingency plans to meet critical processing needs in the event of short or long-term interruption of service;

G. Emergency preparedness; and

H. Designation of an Agency ADP Security Manager.

Funding for ADP security will generally be available at the regular administrative cost for operating State and local systems to administer programs covered under 45 CFR Part 95, Subpart F. As an exception,

however, the statutes authorizing enhanced funding, sections 454(16)(c) and 402(a)(30) of the Social Security Act, specifically reference security as a requirement of the State. For example, these requirements are addressed within the review and approval of a FAMIS APD and enhanced funding will be provided for those automated procedures related to the security of this system.

Information Sources

Additional information on computer systems security can be obtained from sources such as the Computer Security Institute, Datapro Research Corporation, and the Information Systems Officers Association. Additionally, the National Institute of Standards and Technology (NIST) "Publications List 91" list may prove helpful. A copy of this list is attached to FSA-AT-91-2 dated January 10, 1991. It provides instructions for ordering specific publications from the U.S. Government Printing Office and the National Technical Information Service.

Instructions: DHHS has already received some submissions and requests for clarification from States. It is the intent of this Information Memorandum to respond to requests from States for technical assistance in order to meet ADP systems security requirements. We have attached a guidance document that you may find useful when conducting reviews and preparing written summaries.

As this is the first time that State and local government entities have reported biennial reviews in accordance with this new regulation, we anticipate that the reports to HHS will be varied and informative. HHS welcomes any and all comments from State and local governments concerning this Information Memorandum and its attachment.

Mail Plans
To: Mr. Mark E. Ragan, Director
Office of State Systems
Administration for Children and Families, DHHS
Washington, D.C. 20447

Telephone
Inquiries To: Administration for Children and Families
(202) 401-6960

_____

Assistant Secretary
for Children and Families

Attachment

State ADP Security Components
45 CFR Part 95, Subpart F, Section 95.621

I. Objective of ADP Biennial Security Requirements

Under 45 CFR 95.621 each State is responsible for the security of all ADP projects under development and all operational systems involved in the administration of DHHS programs. This regulation requires that State agencies shall (1) determine the appropriate ADP security requirements based on recognized industry standards or standards governing security of Federal ADP systems and information processing; (2) implement appropriate security requirements; (3) establish a security plan and, as appropriate, policies and procedures to address the areas of ADP security specified at 95.621(f)(2)(ii); (4) establish and maintain a program for conducting periodic risk analyses; and (5) conduct a biennial ADP system security review of installations involved in the administration of DHHS programs which, at a minimum, includes an evaluation of physical and data security operating procedures, and personnel practices. These requirements apply to all ADP systems used by State and local governments to administer programs covered under 45 CFR part 95, subpart F.

State agencies are to complete the required biennial ADP System Security Review before October 1, 1992 for existing systems. Heads of State agencies are required to provide DHHS the following information no later than October 1, 1992: (1) a summary of the State's findings during the biennial review; (2) a determination of compliance with the State's ADP security requirements; (3) a description of the State's ADP security program; (4) an action plan with scheduled due dates of milestones which when completed will correct any security weaknesses; and (5) certification of State compliance with those areas cited in 95.621(f)(2)(ii). Certification of compliance must be made by the head of the State agency.

II. Summary of State's findings during the biennial review

A Summary of Findings during the biennial review gives the types and levels of protection necessary for equipment, data, information, applications, and facilities to meet the requirements of the State's ADP systems security policy. These are the minimum requirements necessary for the State to maintain an acceptable level of security. States usually include a summary list of vulnerabilities. The following areas of vulnerability may be addressed:

-- Opportunity for entering erroneous or falsified input data
-- Opportunity for unauthorized access
-- Ineffective administrative controls
-- Ineffective application program controls and back-up capability

Such summaries usually discuss all instances where a biennial review shows non-compliance with security requirements. These State findings are used to determine compliance with the State's ADP systems security requirements.

State ADP Security
Components
45 CFR Part 95, Subpart F, Section 95.621

III. Determination of Compliance with the State's ADP security requirements

A Determination of Compliance with the State's ADP security requirements uses the Summary of Findings to develop the protective measures and controls that are needed to meet the security requirements for the State. These are usually called security safeguards and may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices. A Determination of Compliance usually addresses all areas where a Summary review shows non-compliance with security requirements.

IV. Description of State's ADP security program

This provides an overview of the security of all ADP projects under development and operational systems involved in the administration of DHHS programs. It usually identifies the process used to determine the appropriate ADP security requirements, citing recognized industry standards or standards governing security of Federal ADP systems and information processing, used as a basis for this determination. It describes an overall security program which assures a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the system(s). Accordingly: (1) each operational system involved in the administration of DHHS programs must have the appropriate technical, personnel, administrative, environmental, and telecommunications safeguards; (2) each system's security should be cost-effective; and (3) each system, which supports critical functions, would have to have a contingency or disaster recovery plan to provide continuity of operations. The State's description summarizes ADP security requirements and how they are met. Some typical areas may be:

A. Physical security of ADP resources

Physical security safeguards apply in administrative, physical, and technical areas which involve the administration of DHHS programs. They can be achieved through the use of locks, guards, administrative controls, and measures to protect against damage from intentional acts, accidents, fires, and environmental hazards such as floods, hurricanes, and earthquakes. Minimum security safeguards reflecting minimum security requirements are usually planned and/or implemented based on the results of a risk analysis.

There are various components of State facilities which may require protection. For example:

-- Computer room

-- Data control and conversation area
-- Programmer's area
-- Terminal/remote job entry (RJE) room
-- Communications equipment area
-- Data file storage area
-- Forms storage area
-- Supplies storage area
-- Maintenance/workshop area
-- Support equipment area (including cooling towers and water supply)
-- Telephone closet
-- Power supply area (including transformer vaults and power panels)
-- General office area (where sensitive data is handled)

1. Access Control

Physical and administrative controls to prevent unauthorized entry into operations, data storage, library, and other support areas are access controls. The following areas are examples of access control:

-- Physical controls
-- Administrative controls
-- Protection of sensitive materials
-- Fire safety

2. Operating Systems Control

These are the operating system features that guarantee systems integrity and prevent unauthorized use of sensitive system interfaces. They may include operating system control of access to data files and software programs stored in the facility, recording and displaying non-routine activity that may indicate a security violation, safeguards to protect operational status and subsequent re-start integrity during and after shutdown.

B. Equipment security to protect equipment from theft and unauthorized use

These are the physical protection concerns the State addresses in order to prevent or minimize equipment loss or damage due to theft, sabotage, civil disturbance, natural disaster or other threats. Critical areas, such as cost of replacement, security precautions in place (e.g., locked area, patrolled by guard), fire protection, theft, vandalism, and other types of potential damage or loss are usually discussed here.

C. Software and data security

These types of control processes ensure that appropriate administrative, physical, and technical safeguards are incorporated into all applications and significant modifications.

D. Telecommunications security

This is how the State provides effective and appropriate protection for the DHHS program data when they are transmitted by data communications equipment. Typical areas of telecommunications security are:

1. The State's process for establishing and implementing required and appropriate procedures, controls, and security safeguards for the data communications network.

2. An overview of its contingency plan for use in the event of major disruptions to the communication of highly sensitive data or highly critical data communications capabilities is helpful.

E. Personnel security

Personnel security policies are usually in place which cover all individuals participating in system design, operation, and maintenance, or having access to data from systems involved in the administration of DHHS programs. One important aspect of personnel security is the State's security awareness and training activity.

F. Contingency plan to meet critical processing needs in the event of short or long-term interruption of service.

Every facility and outlying office/remote site (including Wide Area Networks and Local Area Networks) which process applications that are critical to the performance of the State's mission in support of DHHS programs should have a contingency plan. Contingency planning usually includes:

-- Identification of critical applications
-- Maximum permissible outage (i.e., disruption of service, use, or access) for each application
-- Regular backup of critical applications, data, operating software, and databases
-- Alternate operating procedures, as appropriate
-- Regular contingency plan testing
-- Update of the contingency plan based on test results

G. Emergency preparedness.

This is advance planning which clearly identifies circumstances that require an emergency response, who to contact, where to contact them, and when they should be contacted. The goal of emergency preparedness is to minimize or prevent interference with systems involved in the administration of DHHS programs. Requirements for different facilities will vary, and may be addressed by identifying, in general terms, what is being protected and what emergency situation it is being protected from.

H. Designation of an Agency ADP Security Manager.

This identifies the State ADP Security Manager and usually includes major duties/responsibilities.

I. Periodic Risk Analyses

Each State is required to develop a comprehensive risk management program. The State risk management program may be summarized as it pertains to the administration of DHHS programs. Risk management programs usually entail many risk analyses and may provide for additional reviews which are required whenever a system, facility, or network undergoes a significant modification.

V. Action plan with scheduled dates of milestones which when completed will correct any security weaknesses

This is a schedule for implementing selected safeguards, giving key milestone dates, when available. Such schedules usually describe the State's plan for monitoring the scheduled implementation of safeguards, and the process used to review and approve all implementation plans for accuracy and adequacy.

VI. Certify State compliance with 95.621(f)(2)

Heads of State agencies must determine that the security program is in compliance with the security requirements identified as a result of implementing this regulation. Such determination must include written certification of compliance with those areas cited in 95.621(f)(2).

State ADP Security
Components
45 CFR Part 95, Subpart F, Section 95.621

Definition of DHHS Security Terms

access control

The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access. (See page 7.)

action plan

A written plan of activities which a State will initiate to correct security weaknesses identified during its biennial review. (See pages 2, 5 and 10.)

ADP security

ADP or computer security refers to the combination of physical, administrative, and technical measures applied to protect automated information system assets from loss, destruction, misuse, alteration, or unauthorized disclosure or access. (See pages 1, 2 and 5.)

ADP security manager

The person responsible to the State agency head for ensuring that security is provided for and implemented throughout the life cycle of an automated information system from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal. (See pages 3 and 10.)

ADP security program

The laws, rules, procedures and practices that regulate how ADP systems are managed and protected in order to meet a State's security requirements. (See pages 1, 2, 5 and 6.)

These definitions are drawn from official documents of the United States Government departments and agencies. The intent of these definitions is to clarify ADP security terms which arise during a State's biennial security review.

State ADP Security
Components
45 CFR Part 95, Subpart F, Section 95.621

Definition of DHHS Security Terms

biennial ADP system security review

A thorough examination of a State's ADP systems conducted every 2-years for the purpose of determining a State's compliance with ADP security requirements. (See pages 2 and 5.)

certification of compliance

The comprehensive evaluation of the technical and nontechnical security features of an automated information system and other safeguards, made in support of the biennial review process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements. (See pages 5 and 10.)

computer system

Any equipment or interconnected system or subsystems of equipment used in automatic acquisition, storage manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; and includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. (See page 3.)

contingency plan

A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation, after a reasonable period of time. (See pages 3 and 9.)

contingency planning

Contingency planning refers to the development, testing, and maintenance of plans for emergency response, backup operations, and disaster recovery at an automated information system facility where data and information are processed. The purpose of contingency planning is to maximize data availability. (See page 9.)

data availability

The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user. (See page 13.)

State ADP Security
Components
45 CFR Part 95, Subpart F, Section 95.621

Definition of DHHS Security Terms

data file

A data file is a compilation of DHHS program related information which shares specified descriptive characteristics. A data file is created, collected, processed, transmitted, disseminated, used, stored, and disposed of by application systems. The protection of DHHS program data files is the cornerstone of the DHHS ADP security requirements. (See pages 7 and 8.)

data security

The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. Also known as data integrity. (See pages 2, 3, 5 and 8.)

determination of compliance

The result of evaluating a State's findings to determine that its security standards governing DHHS information systems are adequate and whether the security program meets minimal security requirements. (See pages 2, 3, 5 and 6.)

milestone

A planned event at a point in time. (See pages 2, 5 and 10.)

personnel security

Personnel security refers to a program that determines the sensitivity of positions and screens individuals who participate in the design, operation, or maintenance of automated information systems or who have access to such systems. (See pages 3, 6 and 9.)

physical security

Physical security refers to the combination of devices that bar, detect, monitor, restrict, or otherwise control access to sensitive areas. Physical security also refers to the measures to protect a facility that houses automated information system assets and its contents from damage by accident, malicious intent, fire, loss of utilities, environmental hazards, and unauthorized access. (See pages 2 and 7.)

Definition of DHHS Security Terms

requirement

A prerequisite needed to achieve an objective or goal. (See pages 1, 2, 3, 5, 6, 7, 9 and 10.)

risk

The probability that a particular threat will exploit a particular vulnerability of the system. (See pages 6 and 10.)

risk analysis

The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards based on State security objectives. Risk analysis is a part of risk management. Synonymous with risk assessment. (See page 7.)

risk management

Risk management is a process for minimizing losses through the periodic assessment of potential hazards and the systematic application of corrective measures. (See page 10.)

safeguard

A protection which is proportional to the amount of loss and probability of loss. Safeguards should not be used if no threat exists. (See pages 2, 6, 7, 8 and 10.)

security requirement

The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy. (See pages 1, 2, 5, 6, 7 and 10.)

software security

General purpose (executive, utility or software development tools) and applications programs or routines that protect data handled by a system. (See page 6.)

standard

A recognized level of security based on similar applications applied to systems used in industry or the Federal Government. (See page 1, 5, 6, and 13.)

Definition of DHHS Security Terms

telecommunications security

Measures taken to deny unauthorized persons information from telecommunications programs, and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material and information. (See pages 3 and 8.)

threat

Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. (See pages 2, 8 and 14.)

vulnerability

A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy. (See pages 5 and 14.)