PART 2006 - MANAGEMENT

Subpart Z - Information Systems Security

TABLE OF CONTENTS

o0o

PART 2006 - MANAGEMENT

Subpart Z - Information Systems Security

§ 2006.1251 Purpose.

This Instruction establishes the policy supporting program goals, and the assignment of responsibilities for the management, implementation, and operation of the Information Systems Security program. This Instruction applies to Rural Development.

§ 2006.1252 Policy.

It is the policy of Rural Development to establish and maintain an effective Information Systems Security program that complies with applicable national, and departmental Information Systems Security policies and addresses Rural Development's unique requirements for confidentiality, integrity, and availability. The Information Systems Security program will:

(a) Assure that appropriate, comprehensive and cost effective safeguards are employed to protect sensitive information resident on or communicated through Rural Development's automated information systems;

(b) Assure that the information security management and technology issues associated with the use of automated systems are properly addressed through the establishment and maintenance of an effective Information Systems Security program;

(c) Assure the measures used to safeguard sensitive information, associated electronic processing equipment, and facilities are commensurate with the importance of the information systems to the Rural Development mission, the sensitivity and criticality of the information being processed, and the risk environment. Control measures employed to manage systems security risk shall be both cost and technically effective.

§ 2006.1253 Definitions.

Automated information system. The organized automated collection, processing, transmission, and dissemination of information in accordance with defined procedures (OMB Circular A-130).

Automated information systems security . The managerial, technical, and physical safeguards used to assure the confidentiality, integrity, and availability of sensitive information processed by or transmitted through Rural Development automated information systems (Pub. L. 100-235/OMB Circular A-130).

Security Officer . The senior Rural Development official charged with the operational responsibility for implementing the Information Systems Security program.

Sensitive information . Information that required protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an Agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

§ 2006.1254 Authority .

The legal and regulatory requirements for the Rural Development Information Systems Security program include:

(a) National .

(1) Pub. L. 100-235. "The Computer Security Act of 1987."

(2) OMB Circular A-130, Appendix III.

(3) Federal Managers Financial Integrity Act of 1983 and supplementary guidance set forth in OMB Circulars A-123 and A-127.

(4) The Privacy Act of 1974.

(b) Departmental .

(1) Departmental Regulation (DR) 3140-1.

(2) Departmental Manual 3140-1.

§ 2006.1255 Background .

The increased use of distributed information systems to store, process, and communicate sensitive information throughout Rural Development has added a new dimension of complexity to the traditional security concerns confronting managers and employees. The continuing integration of computer and telecommunications technologies further complicates the information systems security problem. The significant benefits to be gained from using this technology must be accompanied by the implementation of an Information Systems Security program that enables the productive use of computer technology while reducing the associated security risks to an acceptable level.

§ 2006.1256 Applicability .

This Instruction and associated Rural Development information systems security standards and guidelines apply to all Rural Development organizational elements and to other components of the Department of Agriculture having data resident on Rural Development computer systems. They apply also to contractors providing information processing services to Rural Development. As specified in the Computer Security Act of 1987, this Instruction and its implementing procedures, standards, and guidelines apply to Federal computer systems operated on behalf of Rural Development by a state or local government or other organization to accomplish a Federal function.

§ 2006.1257 Program objectives .

The objectives of the Rural Development Information Systems Security program are to:

(a) Provide uniform policy and centralized guidance on the various aspects of information systems security;

(b) Establish and enforce requirements for the protection of personal, proprietary, and other types of sensitive information against disclosure, modification, or destruction as appropriate;

(c) Protect funds, supplies, and material from fraud, theft, misappropriation, or misuse;

(d) Maintain the continuity of Rural Development operations by preventing the occurrence or minimizing the impact of security related events that interfere with normal information processing operations;

(e) Support the goals and objectives of the Rural Development Internal Control program;

(f) Assure that appropriate security planning and risk management requirements are integrated into the Rural Development systems development process; and

(g) Provide security awareness and training to promote information systems security awareness and accountability at all levels within Rural Development.

§ 2006.1258 Responsibilities .

(a) Automation Review Council . The Automation Review Council (ARC) is comprised of senior managers in Rural Development who provide guidance and approval for the Agency's automation program. The ARC approves security policies.

(b) Chief Information Officer . The Chief Information Officer (CIO) is the senior information systems management security officer for Rural Development. In this capacity, the CIO is responsible for the development and maintenance of a comprehensive, state-of-the-art, and cost effective Information Systems Security program that will assure compliance with established national and operational responsibility for the Information Systems Security program through the activities of the Rural Development Security Officer.

(c) Security Officer . The Security Officer is responsible for planning, developing, and directing a comprehensive Information Systems Security program. The Security Officer will:

(1) Monitor and report on Rural Development compliance with national and departmental information systems security policies and standards.

(2) Establish Rural Development information systems security goals and objectives and develop management implementation plans for achieving these goals. Coordinate, as necessary, the actions of components having collateral responsibilities.

(3) Develop, coordinate, implement, interpret, and maintain security policies, procedures, and guidelines for the protection of Rural Development information systems assets.

(4) Devise and implement a comprehensive risk management program which assures that security risks are identified, considered, and mitigated through the development of cost effective security controls implemented at the application, system, network, or facility levels. The Rural Development risk management program also includes the development and maintenance of computer security plans, as well as the security certification and accreditation of sensitive applications.

(5) Conduct periodic information systems security risk assessments, security evaluations, or internal control reviews of operational Rural Development automated information systems and facilities.

(6) Provide consolidated budgetary planning and review for information systems security equipment, control software, and services.

(7) Serve as the principal information systems security consultant to Rural Development components that use, develop, or operate automated information systems.

(8) Support the goals and objectives of the Privacy Act of 1974 by establishing appropriate physical, systemic, and procedural safeguards to assure the confidentiality of personal information processed by Rural Development automated systems.

(d) Assistant Administrator for Human Resources . The Assistant Administrator for Human Resources is responsible for assuring the establishment of security designations established by the Office of Personnel Management for government employees and contractors involved in the use operation, and development of Federal automated information systems.

(e) Deputy Chief Information Officer . The Deputy Chief Information Officer is responsible for:

(1) Ensuring that the security responsibilities inherent in the management function for Rural Development national systems are met through the development and implementation of appropriate administrative, operation, and physical controls.

(2) Establishing a management control process to ensure appropriate safeguards, security requirements, and auditing mechanisms are incorporated into all new and significant modifications to existing sensitive national Rural Development computer applications.

(3) Preparing, testing, and maintaining contingency plans for the Rural Development computer applications.

(4) Ensuring that Rural Development computer applications are certified and accredited.

(5) Assisting in the implementation and support of the Rural Development security program set forth in the policies, standards, and guidelines developed by the Rural Development Security Officer.

(f) State and Regional Directors and other Rural Development Management Officials. These Directors and Officials will:

(1) Implement established Rural Development information security policies within their jurisdictions.

(2) Promote information security awareness and the ethical use of automated systems.

(3) Appoint an Information Systems Security Representative in accordance with requirements of the Information Systems Security Handbook.

(4) Ensure that security requirements are included in the specification and/or contract for the acquisition or operation of computer facilities, equipment software packages, or related services.

(5) Issue appropriate security instructions needed to implement the provisions, the security policies, and standards established in Rural Development directives.

(6) Promptly report to the Security Officer or other appropriate officials any breaches of security, events that may indicate a security violation, or attempts to gain unauthorized access to Rural Development computer systems or the data resident on these systems.

(7) Certify and accredit sensitive applications.

§ 2006.1259 Information Systems Security Handbook .

The Rural Development Information Systems Security Handbook provides more detailed standards and guidance which support the Information Systems Security program.

§ 2006.1260 Information Systems Security program elements .

The Information Systems Security program will be composed of a balanced, cost effective combination of management and staff actions, operation activities, and technological control measures. The program elements, which are detailed in the Information Systems Security Handbook, are briefly described below. The elements consist of diverse functional security areas that are integrated into a comprehensive information systems security program.

(a) Automation security policies, standards, and guidelines . The foundation of the Information Systems Security program is the development, implementation, and compliance with policies, standards, and guidelines.

(b) Assignment of security responsibilities . Managers shall ensure that responsibilities for information systems security are clearly communicated to all employees. When required by the size and importance of the computer resources and/or the sensitivity of the information processed, an Information Systems Security Representative may be formally designated to exercise security management functions on behalf of the responsible manager.

(c) Effective use of protective technology . Rural Development shall seek to fully employ available hardware, software, and communications security technology. New information technology procurements shall be reviewed to:

(1) Assure that appropriate security is integrated into systems designs; and

(2) Assure that advances in security technology are obtained for use within Rural Development.

(d) Security education and training . Education and training comprise a key element in the Information Systems Security program. Information Systems Managers, technical staff, and users shall be familiar with the established goals of the security program and be apprised of their role in making the program effective.

(e) Risk management . The Rural Development shall, to the maximum extent feasible, implement a risk management program that incorporates cost justified baseline physical and procedural controls for similar systems while allowing for local variances based upon an assessment of the information processing environment.

(f) Recurring security inspections and reviews . Rural Development information systems shall be afforded periodic security inspections and reviews as are required by national and departmental policies.

(g) Contingency planning . The increased dependence on automated information systems makes it essential that plans and procedures be prepared and maintained to:

(1) Minimize the damage and disruption caused by undesirable events; and

(2) Provide for the continued performance of essential system functions and services.

(h) Security accreditation of sensitive information applications . A formal security accreditation process shall be implemented to assure that appropriate controls have been designed into sensitive computer applications. An essential feature of this process will be the responsibility of management in the determination of control requirements and the assessment of the internal control environment for the application.

§§ 2006.1261 - 2006.1300 [Reserved]

oOo