U.S. Department of Agriculture
Washington, D.C. 20250

DEPARTMENTAL REGULATION	Number: 3140-001
SUBJECT: USDA Information Systems Security Policy	DATE: May 15, 1996
	OPI: Policy Analysis and Coordination Center, Information Resources Management

1 PURPOSE

This regulation establishes policies to ensure comprehensive protections are in place to safeguard all information technology resources. PACC-IRM, and USDA managers must ensure that protections are in place to protect against accidental or deliberate, unauthorized alteration, destruction, delay, theft, access, use or damage to systems, data, applications, equipment, and telecommunications. This regulation also defines USDA's information and telecommunications security missions, goals, scope, and responsibilities.

2 CANCELLATION

This regulation cancels DR 3140-1, "USDA ADP Security Policy," dated July 19, 1984.

3 SCOPE

This regulation applies to all USDA organizational elements and their employees, other Federal agencies, State agencies, contractors, and sub-contractors who are involved in development of systems, obtaining, transmitting, using, and processing USDA information, data, on behalf of USDA. This regulation also applies to USDA computers operated on behalf of the USDA by State and local government or other private organizations to accomplish a USDA function. Finally, it includes anyone involved in the design, development, acquisition, installation, operation, maintenance and use of USDA ADP, telecommunications, LANs, and WANs.

4 BACKGROUND

The Computer Security Act of 1987, (Public Law 100-235) and OMB Circular No. A-130, Appendix III, dated February 8, 1996, "Security of Federal Automated Information Resources" require all Federal agencies (Departments) to plan for the security of all sensitive information systems throughout their life cycle.

OMB Circular No. A-130, Appendix III establishes a minimum set of controls to be included in Federal AIS security programs; and assigns Federal agencies the responsibilities for security of automated information. It also links agency automated information system security programs and agency management control systems established in accordance with

OMB Circular No. A-123, "Management Accountability and Control." The ISSP is designed to meet the requirements of Federal Laws and guidance. It also ensure the availability of telecommunications, ADP resources, and Word processing (WP) services, and to provide adequate physical protection to all IT resources.

All responsible officials must assume that controls are placed and administered where they are most effective. Local procedures must be developed, documented, implemented, and monitored to ensure reasonable and effective management of both traditional and new technology.

5 POLICY

All USDA entities shall organize, implement, and maintain an information systems security program that ensures adequate security of all USDA information. It applies to all USDA agencies, programs, teams, organizations, contractors, consultants, appointees, employees of USDA funded councils, associations, State, local as well as other government agencies, and committees that use, process, manage USDA information or meet the requirements of the definition of "operator of Federal computer system (The Computer Security Act of 1987)."

The USDA Agency ADP Security Officer title is changed to ISSPM. This title is directly in line with titles used by NIST to address the Federal Information Systems Security community. The new title reflects the expanded role of the ADP Security Officer, a role which no longer focusses on the ADP environment only.

Security must be addressed in the System life-cycle (Planning Phase). It must be applied where it can be the most effective and with the least cost to the agencies. Ensure most cost effective and reasonable security approaches by including the ISSPM in the early stages of planning and technical reviews.

Establishment of security controls in all general support systems are hereby required in accordance with OMB Circular No. A-130, Appendix III.

6 PUBLIC LAWS, FEDERAL GUIDANCE, AND DEPARTMENTAL REGULATION

The following public laws and Federal guidance are applicable to the USDA ISSP:

a External

(1) OMB Circular No. A-130, "Management of Federal Information Resources," revised February 8, 1996;

(2) OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," dated July 9, 1990;

(3) OMB Circular No. A-123, "Management Accountability and Control" dated June 29, 1995

(4) OMB Circular No. A-127, "Financial Management Systems," dated July 30, 1993;

(5) Public Law 97-255, "Federal Manager's Financial Integrity Act of 1982;"

(6) Public Law 93-502, "Freedom of Information Act of 1980;"

(7) Public Law 93-579, "Privacy Act of 1974;"

(8) Public Law 99-474, "Computer Fraud and Abuse Act;"

(9) Public Law 100-235, "The Computer Security Act of 1987," dated January 8, 1988;

(10) Executive Order 10450, "Security Requirements for Government Employment;"

(11) Copyright Act of 1980;

(12) Public Law 104-13, "The Paperwork Reduction Act of 1995;"

(13) National Information Infrastructure (NII) The Federal Role, June 5, 1995; and

(14) "Information Technology Management Reform Act of 1996."

b USDA Internal Regulations

(1) DR 3140-2, "USDA Internet Security Policy," dated March 7, 1995; and

(2) DR 3300-1, "Telecommunications, Section 4, Appendix I," dated March 20, 1996.

7 ABBREVIATIONS

AIS Automated Information Systems

ADP Automated Data Processing

ART Acquisition Review Team

DISSPM Departmental Information System Security Program Manager

DOS Disk Operating System

FOISM Field Office Information Security Managers

GAO General Accounting Office

IRM Information Resources Management

ISPO Information Service Processing Organization

IS Information System

ISSPM Information Systems Security Program Manager

ISSP Information System Security Program

IT Information Technology

LAN Local Area Network

NIST National Institute of Standards and Technology

NSA National Security Agency

OIG Office of the Inspector General

OMB Office of Management and Budget

PACC-IRM Policy Analysis and Coordination Center

Information Resources Management

SIRMO Senior IRM Official

TCP/IP Transmission Control Protocol/Internet Protocol

WAN Wide Area Network

WP Word Processing

USDA United States Department of Agriculture

8 DEFINITIONS

a Access to Information. Refers to providing the public, upon their request, access to government information to which they are entitled under appropriate law.

b Adequate Security. Security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification, of information. This includes ensuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

c Application. The use of information resources (information and information technology) to satisfy a specific set of user requirements.

d Confidentiality. The assurance that only properly authorized persons can view particular information. This refers to the treatment of data; confidentiality is achieved when specific information is not available or transmitted beyond those with an authorized need-to-know. A requirement that private or confidential information not be disclosed to unauthorized individuals.

e Critical Information. Information necessary for the continued operation of any USDA agency or organization, its automated information resources and services. This information may not be sensitive. However, the loss, denial, or modification of such information may cause grave damage to the operation of the organization. For example: the determination and prioritization of the critical information is necessary for emergency preparedness and disaster recovery. Critical information may be transmitted via E-Mail, without being encrypted. It's audience can be strictly controlled.

f Discretionary Access. The automated restricting of accesses to files, programs, protocols, resources, and information based on each user's need-to-know and least privilege requirement. Discretionary Access uses either built in system security capabilities or "third party" security enhancement products.

g Dissemination of Information. Refers to distributing government information to the public, whether through printed documents, or electronic or other media. "Dissemination of information" does not include intra-agency use of information, interagency sharing of information, or responding to requests for "access to information."

h Firewalls. It is a security policy and technology that define the services and access to be permitted, and an implementation of that policy in terms of a network configuration, one or more host systems and routers, and other security measures such as advanced authentication in place of static passwords. The main purpose of a firewall system is to restrict access to or from a protected network (i.e., a site). It implements a network access policy by forcing connections to pass through the firewall, where they can be examined and evaluated.

i General Support System. An interconnected set of information resources under the same direct management control, sharing common functionality. A general support system normally includes hardware, software, information, data, applications, and people. For example: a local area network (LAN), or a system can include smart terminals that support a branch office, an Agency-wide backbone, a communications network, a departmental data processing center, including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

j Granularity. The relative fineness or courseness by which a mechanism such as access controls can be adjusted to implement discretionary access requirements.

k Information. Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized data bases, paper, microfilm, or magnetic tape.

l Information Resources Management (IRM). The planning, budgeting, organizing, directing, training, and control associated with government information. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and technology.

m Information Security. The protection of information resources and technology from intentional or accidental unauthorized destruction, alteration, disclosure, denial, or delay.

n Information System (IS). The organized collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

o Information Technology. The hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal Government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others. It includes automatic data processing equipment as that term is defined in Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949. Automatic data processing and telecommunications activities related to certain critical national security missions, as defined in 44 U.S.C. 3502(2) and 10 U.S.C. 2315, are excluded.

p Information Technology Facility. An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology.

q Least privilege. Refers to the information systems security objective and requirement of granting users only those accesses they need to perform their official duties. It requires that users be granted the lowest level of computer/system access that is consistent with job authority. Increases in privileges shall be requested and granted by written communications.

r Major Application. An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, unauthorized access to, or modification of the information in the application. Note: All Federal information requires some level of protection. Certain applications, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by redundant systems in which they operate.

s Major Information System. Information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources.

t Mandatory Access Controls. Consist of those access controls mandated in documented policies, procedures, system protocols, and systems parameters which serve as the mandatory minimum standards for all users regardless of their discretionary access requirements. The required protection functions and assurances that must be bound together to create a protection profile. For example: All users shall be required to have a unique, authorized userid and password assigned to them by the ISSPM before they can access the system.

u Need-to-Know. The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a person's duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient.

v Non-Discretionary Access Controls. Policies, procedures, practices, instructions or system options that are implemented or activated to counter periodic, nonrecurring or unique threats, such as Trojan horses, viruses, logic bombs, or improperly tested software. Non-Discretionary access controls are determined by ISSPMs and cannot be changed or deleted by unprivileged users, systems administrators or privileged users. Unprivileged users may utilize very limited discretionary administrative controls over these controls. These controls serve to enhance and strengthen Mandatory and Discretionary controls.

w Position Sensitivity. The determination by the organizations's management with the Support and consultation of the ISSPM of the potential for each position accessing the information system resource to cause great harm. System managers/administrators and privileged users shall require a higher level of sensitivity than a system operator. Systems which do not have separation of duties between system administrators/managers and IS ISSPMs require the highest position sensitivity.

x Preauthentication. A protocol or process for proving that a user knows her/his password before access to a system with a password is allowed. Preauthentication can be completed by the use of pin numbers, smart cards, biometrics or tokens.

y Privileged User. A user of a computer who is authorized to bypass normal access control mechanisms, usually to be able to perform system management functions. Policies shall clearly state limits to privileges and separation of duties.

z Reverse Intent. Is the name given to a common hacker technique offlipflopping a piece of security knowledge to identify a potential weaknesses. It is also the development and adoption of Information Systems Security policies, which by their wording, unintentionally and inadvertently reveal system vulnerabilities and capabilities that can be exploited by attackers. For example: a policy, which states: "System administrators shall not leave modems attached to the server in 'auto answer' or 'auto response' condition after normal working hours, during weekends and holidays" indicates to an attacker that the network has modems and is vulnerable to attack.

aa Separation of Duties. Refers to dividing roles and responsibilities so that a single individual cannot subvert a system or critical process. For example, ISSPMs shall perform security functions on systems, whole systems managers perform systems management functions. It is a form of checks and balances.

bb Sensitive Information. Any information, the loss, misuse, unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy) Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

cc Threat. Something in the system environment which, if paired with a corresponding vulnerability, could cause a harmful event to occur. The means through which the evidenced ability or intent of a threat agent to adversely affect an ADP system, facility, or operation may be manifested. The four basic threats are: (1) Denial of Service, (2) Unauthorized Use, (3) Unauthorized Manipulation, and (4) Unauthorized Disclosure of Information.

9 GOALS

The goals of the USDA ISSP:

a Identify, protect and secure critical and sensitive USDA information, systems, applications, and data;

b Ensure that managers at all levels and entities provide adequate security for information resources and automated information systems (AIS) supporting their missions;

c Ensure annual information systems security awareness training and that employees and contractors at all levels of USDA are provided with sufficient guidance to discharge their responsibilities relating to AIS security;

d Ensure individual accountability for use of all automated information resources and AIS;

e Ensure audit ability and availability of all AIS;

f Ensure that all USDA ISSPMs have comprehensive and current information systems security training;

g Allocate sufficient resources to manage Information Systems Security needs in all USDA organizations, including Field Offices;

h Empower ISSPMs throughout USDA to have the authority equivalent to their responsibilities;

i Establish minimum mandatory information systems security standards that are applicable to all USDA and USDA funded organizations;

j Establish authority and guidelines for enforcement; and

k Provide authorization for disciplinary actions for Information Systems Security Non-compliance.

10 RESPONSIBILITIES

Information systems security responsibilities and accountability shall be explicit. The primary responsibility for security relating to all information technology resources is that of the end-user. The responsibilities and accountability of owners, providers, and users of computer systems and other parties concerned with the security of information systems shall be documented. The assignment of responsibilities may be internal to a USDA organization or may extend across organizational boundaries. (Source: An Introduction to Computer Security: The NIST Handbook).

a The Director of PACC-IRM will ensure that USDA:

(1) Is in compliance with all Public Laws relating to Information Systems Security, ethics, privacy and communications;

(2) Has defined and authorized the USDA Information Systems Security Program;

(3) Has staffed and budgeted the USDA Information Systems Security Program with resources commensurate with its responsibilities;

(4) Empower ISSPM to lead and assist USDA organizations in Information Systems Security Program development;

(5) Ensure thorough reviews of USDA organizations' ISSP that USDA agencies are in compliance with Federal and Departmental regulations;

(6) Ensure enough Deputy ISSPMs sufficient to meet the needs of the ISSP, critically and sensitivity of data; and

(7) Acknowledge that the ISSP is an integral part of the USDA administration.

b The Departmental ISSPM will:

(1) Manage the Departmental ISSP throughout the USDA, consistent with this policy document, and other Federal policies issued to protect AIS within USDA;

(2) Monitor and report on compliance and guidance with Departmental and Federal security policies to PACC-IRM Management, OIG, OMB, GAO, NIST, and any other oversight agency requesting information and serve as principal information systems security consultant to USDA senior management;

(3) Develop, coordinate, and maintain information systems security policies, procedures, and guidelines for the protection of all information resources within the Department;

(4) Represent USDA to other Federal Government organizations and specialized groups on information systems security activities;

(5) Establish criteria for computer security awareness training and ensuring a training program is implemented to meet the requirements of the Computer Security Act of 1987; and

(6) Assist Agency ISSPM in developing and improving their ISSP.

c The Director of the Office of Operations will:

(1) Assure close cooperation between her/his operational security elements and PACC-IRM Information Systems Security Policy personnel;

(2) Ensure the development and implementation of physical security policies, practices and guidance that accounts for the increasing dependency on information technology in all USDA offices and locations;

(3) Direct compliance with all Government and USDA policies and regulations for all information technology operational units; and

(4) Provide advice and suggestions to PACC-IRM, which shall improve the USDA ISSP;

d The Director, Human Resources Management (HRM) will:

(1) Be aware of and consider the criticality, privacy, confidentiality and sensitivity of information under her/his domain which is processed, transmitted and stored using information technology;

(2) Provide guidance and direction to PACC-IRM in the development of Information Systems Security guidelines and policies, which serve, support and protect the mission of HRM;

(3) Develop job descriptions for personnel, which include requirements for the protection of critical, confidential, privacy or sensitive information as performance elements;

(4) Develop job description standards for all USDA entities which are uniform and consistent with the requirements to protect critical, confidential, privacy and sensitive information.

(5) Administer a personnel security program that identifies, categorizes and defines personnel security requirements for USDA entities, requires appropriate background investigations/security clearances for employees and contractors alike;

(6) Ensure that DM 3440-1 is updated regularly to reflect changing environment in which Classified Information is processed;

(7) Advise the USDA ISSPM of any personnel regulation changes that can affect the ISSP; and

(8) Designate an HRM ISSPM.

e The Director of the Office of Civil Rights Enforcement will:

(1) Assure that the USDA ISSPM is aware of all requirements to protect and secure Civil Rights Enforcement & Adjudication information in order to prepare and develop specific ISSP policies;

(2) Assure coordination of and compliance with all procurement actions with information systems security requirements;

(3) Lead a Technology Management program which includes the ISSP; and

(4) Designate an ISSPM with responsibility for OO.

f Director, Administrative Management Services will:

(1) Cooperate and collaborate with the PACC-IRM ISSPM to ensure coordination of administrative duties with ISSP requirements;

(2) Designate a DAMS ISSPM; and

(3) Develop and maintain inventory of all Information Technology within the scope of DAMS authority and responsibility.

g Agency Administrators will:

(1) Ensure that information systems security policies and procedures are in place to support this policy and the ISSPM;

(2) Ensure that the ISSP function is properly staffed and resources allocated to allow effective implementation and continuance of a comprehensive and proactive Agency ISSP;

(3) Ensure that the ISSPM is a permanent member of the Agency parallel review process and serves on the ARTs;

(4) Ensure that the ISSPM is a permanent member of all Agency application development, telecommunications, and IRM life-cycle management planning processes;

(5) Ensure that all field and headquarters offices are covered under the responsibilities of the ISSPM;

(6) Ensure assignments of personnel who will be designated as Deputy ISSPMs and persons who will have security as their collateral duties;

(7) Ensure that security of information technologies in field locations has priority as an assignment of the security managers;

(8) Ensure that ISSPMs are assigned to a level within the organization that can independently report to the appropriate program and/or departmental officials. The ISSPM must be able to apply security across the entire agency's programs. It may be necessary to place them in the Deputy Administrators' or Administrators' offices rather than assign them to the agency SIRMO;

(9) Ensure that training opportunities are provided to the ISSPM and security staff in he security field;

(10) Provide for the integrity, availability and confidentiality of information that is critical to USDA to meet its missions;

(11) Protect and secure all USDA information resources;

(12) Ensure that managers provide appropriate security of all information resources supporting their functional activities;

(13) Ensure individual accountability for data, information, all IT resources, to which individuals have access;

(14) Ensure auditability of all AIS;

(15) Ensure that employees are provided sufficient guidance for the discharge of responsibilities regarding information systems security;

(16) Establish guidelines for information systems security enforcement;

(17) Ensure individuals have the least amount of access necessary to accomplish authorized activities;

(18) Ensure that Agency annual Information System Security Plans are developed in accordance with PACC-IRM guidelines and OMB Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contains Sensitive Information." These plans are due to PACC-IRM on April 14, of each year; OMB Circular A-130, Appendix III supersedes OMB Bulletin 90-08 and expands the cover of security plans from Bulletin 90-08 to include rules of individual behavior as well as technical security;

(19) Ensure that each annual information systems security plan contains an agency status report which is comprehensive and documents all aspects of their Information Systems Security Program;

(20) Ensure security is included in all stages of systems life cycle as defined in DM 3140-1, "Management of the Information Systems Security Program;"

(21) Ensure each USDA General Support System shall have assigned to it an individual knowledgeable in all the system's features and capabilitilies, including understanding and implementing all security options or parameters necessary to protect the information and provide auditability; and

(22) Ensure that each major application is assigned a management official knowledgeable in the nature of the information and process supported by the application including management, personnel, operational, and technical controls used to protect it.

h System Security Manager General Support System will:

(1) Cooperate and collaborate with the organizational ISSPM in planning, developing, implementing and documenting security;

(2) Provide access to the ISSPM in compliance with the Separation of Duties principle;

(3) Not exceed her/his Need-To-Know authority;

(4) Support auditing and accountability;

(5) Report violations of policy and security vulnerabilities;

(6) Advocate and support the organization's information systems security program;

(7) Keep the Agency's ISSPM informed on all security matters relating to that general support system; and Additional control features for general support ystem are identified in OMB Circular No. A-130, Appendix III, page 35, under "Controls for General Support Systems."

i System Security Manager Major Applications will:

(1) Assure that effective security products and techniques are appropriately used in the application, and shall be contacted when a security incident occurs concerning the application; and

(2) Work with the Agency's ISSPM and keep the Agency's ISSPM informed on all security matters relating to the major application; and Additional control features for major applications are identified in OMB Circular No. A-130, Appendix III, page 37, under "Controls for Major Applications."

j Senior IRM Officials (SIRMO) will:

(1) Develop and maintain a comprehensive and effective ISSP that ensures compliance with established Federal mandates and Departmental policies; and

(2) Exercise responsibility for the ISSP through the activities of the ISSPM.

k Directors, Associate Directors, Division Chiefs, and other Managers throughout USDA will

(1) Have the primary responsibility for the security of data supporting their functions;

(2) Implement established security policies within their areas of responsibility;

(3) Identify Agency sensitive systems and develop security plans for those systems;

(4) Develop, maintain, and test contingency and disaster recovery plans;

(5) Participate in Agency security risk analyses;

(6) Appoint and train security representatives, ISSPM'S, LAN security officers, and facility/installation security officers;

(7) Promote information systems security awareness and the ethical use of information resources; and

(8) Issue appropriate instructions needed to implement provisions of computer security policies and standards established in Agency directives, Departmental Regulations, and Federal laws.

l USDA Agency ISSPMs Additional ISSPM responsibilities which relate to specific areas of security may be found in DM 3140-2, "Duties and Responsibilities of the Information Systems Security Program Manager." Agency ISSPMs will:

(1) Manage the information systems security programs throughout their agencies including field offices;

(2) Provide overall leadership and direction for the Agency ISSP, by planning and developing agency specific information system security policies, and procedures;

(3) Report agency compliance with Departmental and Federal security policies and guidance to Agency management, PACC-IRM management, OIG, OMB, GAO, NIST, and any oversight agencies requesting information;

(4) Develop, coordinate and maintain information system security policies, procedures, and guidelines for the protection of Agency information resources;

(5) Develop and implement a comprehensive risk management program which ensures that security risks are identified and evaluated; and appropriate counter measures are implemented; This includes the development of information system security plans, contingency plans, certification and accreditation of sensitive systems, and physical security to include access control;

(6) Serve as principal information systems security specialist to Agency senior management, contracting officers, field office information systems security managers, and users;

(7) Represent the Agency at other Federal Government organizations and specialized groups on ISS activities;

(8) Develop and conduct computer security awareness training for security personnel, employees, and contractors to meet the training program requirements of the Computer Security Act of 1987;

(9) Serves as a member of the ART, and reviews proposed procurement requests to ensure adequate security and safety provisions;

(10) Participate in internal or external reviews, conduct inspections for compliance with policies and procedures, and monitor measures to correct deficiencies identified in audits or inspections;

(11) Develop the Agency annual Information System Security Plan, in accordance with PACC-IRM guidelines and OMB Bulletin 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contains Sensitive Information." Submission is due April 14, of each year;

(12) Investigate and report all suspected and actual computer security breaches that may indicate a computer security incident, violation or

attempt to gain unauthorized access to computers, information systems or data, and resident on Agency information resources;

(13) Participate as a permanent member of all agency application development, telecommunications, and IRM life-cycle management planning processes; and

(14) Identify, protect and secure critical and sensitive USDA information, systems, applications, and data.

m ADP Facility ISSPMs will:

(1) Perform the primary duties of the ISSPM as defined in DM 3140-2, "Duties and Responsibilities of the Information Security Program Manager;" and

(2) Take on a heightened level of physical security to protect the physical environment of the facility.

n ADP Facility Managers will:

(1) Designate an individual as the Facility ISSPM for the facility when it meets the criteria specified in DM 3140-1;

(2) Maintain adequate security measures required to protect the Agency data that are maintained or processed at the facility;

(3) Develop and update ADP security and contingency plans;

(4) Develop and implement procedures to back up user programs and data; and

(5) Ensure that procedures are in place and tested for disaster recovery.

o Field Office Information Security Managers will:

(1) Provide adequate security for those in single location space or those FOISM that share offices space;

(2) Provide the same level of security protection that is required of the Agency ISSPM in the protection of the Agency information;

(3) Provide physical security protections from intruders or persons unauthorized to have access to the Agency resources;

(4) Establish an Agency approved security policy, contingency plan and disaster recovery plan that all persons working at the location are aware of and adhere to;

(5) Implement established security policies within their areas of responsibility;

(6) Identify Agency sensitive systems and assist in the development of security plans for those systems;

(7) Test contingency and disaster recovery plans for their field location;

(8) Participate as required by their Agency in developing risk analyses;

(9) Promote information systems security awareness and the ethical use of information resources within their field office; and

(10) Issue appropriate instructions needed in their field location to implement provisions of computer security policies and standards established in Agency directives, Departmental Regulations, and Federal laws.

p Users, Contractors and Sub-contractors will:

(1) Comply with all security requirements pertaining to the information resources they use;

(2) Refrain from using trivial and obvious passwords;

(3) Ensure that passwords are held in strict confidence and properly safeguarded from unauthorized access and use;

(4) Employ available and approved safeguards to protect the confidentiality, integrity and availability of data, applications, and information resources;

(5) Comply with all licensed software agreements; and

(6) Report any suspected security incidents observed to the ISSPM and your immediate supervisor.

11 STAFFING

The USDA shall have a full-time ISSPM located in PACC-IRM. PACC-IRM shall staff the program office, as necessary, to ensure national and USDA computer security requirements can be met. Agencies shall have a ISSPM position which may be filled with a collateral-duty ISSPM. Agencies shall determine whether the position will be full-time or part time. Each agency shall determine the size of any security support staff, but must ensure personnel resources for security are adequate to meet national and USDA computer security requirements.

12 TRAINING

The USDA and Agencies ISSPMs shall ensure that information systems security requirements, procedures, and practices are included in computer security training materials. Each new employee will receive an orientation outlining their security responsibilities. Thereafter, the program managers shall ensure training is provided to their employees on a regular basis.

All USDA agencies must make security awareness and training mandatory for all employees that use, operate, supervise, or manage computer systems or use output from computer systems. Each USDA employee that uses computers or output from computers must be:

a Provided awareness of their security responsibilities;

b Provided periodic security training (minimum once a year) in how to fulfil the responsibilities of security; and

c Informed of requirements as stated in OMB Circular A-130 relating to awareness and training.

13 SYSTEM USAGE

USDA employees, consultants, contractors, and sub- contractors working for USDA shall:

a Not attempt to gain access to systems, applications, or data for which they have not been authorized;

b Not assist others in attempting to gain unauthorized access to systems, applications, or data;

c Not knowingly destroy or modify data without permission, nor introduce malicious software (viruses or worms) or infected files;

d Not make illegal copies of software; and

e Not use USDA computer systems for personal use or gain.

14 VIRUS PROTECTION

The ISSPM will ensure that anti-virus software is installed and used to check microcomputer systems, LAN servers, new software packages, and diskettes for viruses before use.

15 SYSTEM WARNING MESSAGE

All USDA host computer systems capable of being accessed by communications connections, including local area networks and stand-a-lone systems, after completion of system booting procedures, must display a warning message at login. This message at a minimum must address the following, "The user has accessed a United States Government computer which requires prior authorization to access. Any person or computer assisted access is deemed to be unauthorized and can result in fines or imprisonment."

16 INTERNET ACCESS

USDA systems will employ robust authentication measures for dial in and Internet access. Use of a firewall or router when the system uses TCP/IP to prevent intrusions is a centralized and convenient method of protecting USDA systems and networks. The use

of passwords alone is not an adequate method of protecting systems that are connected to the Internet. This policy is not intended to deny access to public data. Rather, it is intended to protect data that has not been identified for public disclosure.

PACC-IRM has responsibility for determining the adequacy of security measures in place in systems used as gateways to the Internet. All such systems will be regularly reviewed by the Agency ISSPM for vulnerabilities from known threats. It is the responsibility of USDA agencies and staff offices that have or plan a gateway to the Internet to fund, implement, and maintain the prescribed protective features.

All USDA agencies and staff offices using the Internet must follow the guidance in DR 3140-2, "USDA Internet Security Policy," and DR 3300-1, "Telecommunications."

17 SYSTEM SAFEGUARDS

In accordance with OMB Circular No. A-130, Appendix III, each general support system and major application will have developed a security plan consistent with guidance issued by NIST as a MINIMUM. The current guidance is published in OMB Bulletin 90-08. PACC-IRM requires as a part of the OMB Bulletin 90-08 submission an annual IRM Security Program Status Report. The following topics are to be addressed in the status report part of the security plan submission:

a Accomplishments

b Security awareness program

c Reviews

d Disaster recovery

e Improvements to agency security

f Number of sensitive systems

g Number of systems recertified during the year

h Telecommunications

i Protection for Local Area Network

j Agency security policy development

k Description of audits performed

l List of any audits conducted by outside agencies which included aspects of computer security

THE SUBMISSION OF THE SECURITY PLAN SHALL BE DUE ON THE 14th OF APRIL EACH YEAR.

18 REPORTING SECURITY BREACHES

Report security breaches to the address listed below:

PACC-IRM

Departmental ISSPM

Room 427-W Jamie L. Whitten Federal Building

14th & Independence Ave. SW

Washington, D.C. 20250

Internet: WGant@.USDA.gov

Email: SIESNET: WGANT

Phone: 202-720-4301 FAX: 202-690-0574

All reports will be forwarded to the Office of The Inspector General.

19 COMPLIANCE

All users of information and AIS, including contractors working for USDA, are responsible for complying with this information systems security policy as well as procedures and practices developed in support of this policy. Any contractor handling sensitive USDA data is subject to the security requirements specified in this Departmental Regulation.

Anyone suspecting misuse or attempted misuse of USDA information systems resources are responsible for reporting such activity to their management officials and to the ISSPM.

20 NON-COMPLIANCE

Violations of standards, procedures, or practices in support of this policy will be brought to the attention of management officials for appropriate action which will result in disciplinary action, that could include termination of employment.

Signed By:

HOLLACE L. TWINING

END