SECURITY PROTECTION
DM-3530-000

TABLE OF CONTENTS

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL MANUAL	Number: 3530-000
SUBJECT: Security Protection	DATE: July 15, 2004
	OPI: OCIO, Cyber Security

CHAPTER 6
GENERAL INFORMATION

1 PURPOSE

This Departmental Manual chapter establishes the policy and procedures for the use of Security Protection of Information Technology (IT) assets within USDA. Security Protection includes the use of Gateways, Firewalls, C2 Controlled Access Protection, Intrusion Detection Systems, Public Key Infrastructure (PKI) Technology, IBM/IBM Compatibles Mainframe Security Standards, Identification & Authentication, Vulnerability Scans, and User Logon Identification. Each of these areas will be covered in separate parts of this chapter.

Part 1, Vulnerability Scan Procedures, defines policy and procedures for conducting vulnerability scans in USDA.

Part 2, IBM & IBM Compatible Mainframe Security Standards, establishes policy and procedures for security of International Business Machines (IBM) and IBM Compatible Mainframes within USDA.

As USDA moves closer toward implementation of the Government Paperwork Elimination Act, Electronic Signatures in Global and National Commerce Act, the Government Performance and Results Act of 1993, and the Clinger-Cohen Act of 1996, we have been re-engineering the workplace processes to more effectively satisfy business communications using computers and a paperless

environment. With technological advances come security issues related to trust, legitimate authority and handling of sensitive or confidential information. This manual chapter discusses various security technologies acceptable for use within USDA to safeguard USDA information assets. A recognized security protection method that addresses these concerns is Public Key Infrastructure (PKI).

Part 3, PKI provides an environment that speaks to agencies' business, legal, network, and security demands for trust and confidentiality in protecting sensitive communications, transactions, and storage. PKI supports the use of policies, protocols, standards and information assurance services needed to protect the transmission of electronic data through the use of digital signatures and encryption technology. The purpose of this manual is to establish policy and responsibilities for implementing a PKI within the United States Department of Agriculture (USDA).

2 CANCELLATION

This Departmental Manual chapter will be in effect until superseded.

3 REFERENCES

Public Law No. 89-487, "Freedom of Information Act";

Public Law No. 93-579, "Privacy Act of 1974";

Public Law No. 99-474, "Computer Fraud and Abuse Act";

Public Law No. 104-106, Div. E, Clinger-Cohen Act of 1996;

Public Law No. 105-277, Div. C, Title XVII "Government Paperwork Elimination Act of 1998";

Public Law No. 106-229, Electronic Signatures in Global and National Commerce Act ("E-SIGN");

Public Law 106-398, Appendix Title X, Subtitle G, "Government Information Security Reform";

OMB Circular No. A-123, "Management Accountability and Control";

OMB Circular No. A-127, "Financial Management Systems";

Office of Management and Budget Circular A-130, Appendix III;

NIST Special Publication 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication;

NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems;

NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems;

NIST Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure;

Federal Information Processing Standards Publication 140-2, Security Requirements for Cryptographic Modules;

Federal Information Processing Standards Publication 180, Secure Hash Standard;

Federal Information Processing Standards Publication 186-2, Digital Signature Standard (DSS);

DM 3500-1, USDA Computer Incident Response Procedures, Chapter 1;

DR3300-1, Telecommunications & Internet Services and Use;

CS Guidance Regarding Annual Security Plans for IT Systems and Security Programs, CS-025; and

CS Guidance Regarding C2 Controlled Access Protection, CS-013.

4 SCOPE

This manual applies to all USDA agencies, programs, teams, organizations, appointees, employees and other activities. This manual applies to all Agency Information Systems (AIS) that the USDA manages and maintains on behalf of non-USDA entities when

those systems are on the USDA domain and backbone network (i.e., not on isolated domains) and shared resources with USDA systems. For non-USDA systems managed by USDA, the system owner must stipulate in writing (in an MOU or SLA) their security rules. In addition, the owner must acknowledge and accept the risks to their systems and data if they are not secured at least up to USDA standards.

5 ABBREVIATIONS

ACID	- Access Identification
AIS	- Automated Information System
APF	- Authorized Program Facility
CA	- Certificate Authority
CA-ACF-2	- Computer Associates Access Control Facility
CICS	- Customer Information Control System
CIO	- Chief Information Officer
CP	- Certificate Policy
CPS	- Certification Practice Statement
CPU	- Central Processing Unit
CS	- Cyber Security
DAA	- Designated Accrediting Authority
DASD	- Distributed Access Storage Device
DASDVOL	- Distributed Access Storage Device Volume
IBM	- International Business Machines
IP	- Internet Protocol
IRM	- Information Resources Management
ISS	- Internet Security Systems
ISSPM	- Information Systems Security Program Manager
IT	- Information Technology
MVS	- Multi-Processing Virtual System
NIST	- National Institute of Standards and Technology
OCIO	- Office of the Chief Information Officer
OMB	- Office of Management & Budget
PKI	- Public Key Infrastructure
RA	- Registration Authority
RACF	- Resource Access Control Facility
RAID DASD	- Redundant Array of Inexpensive Disks DASD
SA	- System Administrator
SE	- System Engineer/Developer
SSA	- System Security Administrator
SVC	- Operating System Service Calls
TSO	- Time Sharing Option
VM	- Virtual Memory

VSAM - Virtual Storage Access Method
VTAM - Virtual Telecommunications Access Method
USDA - United States Department of Agriculture