SECURITY PROTECTION
TABLE OF CONTENTS
3530-000

3530-005
Part 5 – Security Encryption Standards

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

DEPARTMENTAL MANUAL	NUMBER: 3530-000
SUBJECT: Security Protection	DATE: February 17, 2005
	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 for Information Technology (IT) assets within USDA. Security Protection includes the use of Gateways, Firewalls, Intrusion Detection Systems, Public Key Infrastructure (PKI) Technology, IBM/IBM Compatibles Mainframe Security Standards, Identification and 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.

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).

Part 4, Firewalls Technical Security Standards discusses the secure Information Technology standards for our Firewalls within USDA. This

policy is designed to assist agencies/mission areas in implementing secure connections from the Internet to all USDA networks, including Intranets and Extranets.

Part 5, This Departmental Manual Chapter sets forth the departmental policy, minimum standards and approved protection techniques to safeguard Sensitive But Unclassified information (SBU), also referred to as Sensitive Security Information (SSI), which is stored or transmitted electronically throughout USDA and external telecommunication networks. In addition, these standards and protections apply to external stakeholders using telecommunication and connection methods approved by USDA.

2 CANCELLATION

This Departmental Manual will be in effect until superseded. This chapter/part replaces DN-3140-6.

3 REFERENCES

DM 3593-002, Appendix B, CS Legal and Regulatory References.

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. This manual pertains to the storage and transmission of information over both wired and wireless medium, which radiates or transits beyond a facility boundary or is otherwise not directly under the control of the department or departmental agencies communications Point of Presence (POP).

5 ABBREVIATIONS

ACID	- Access Identification
AIS	- Automated Information System
APF	- Authorized Program Facility
CA	- Certificate Authority
CA-ACF-2	- Computer Associates Access Control Facility
CCB	- Configuration Control Board
CICS	- Customer Information Control System
CIO	- Chief Information Officer
COOP	- Continuity of Operation Plan
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
DMZ	- De-militarized Zone
IBM	- International Business Machines
ICMP	- Internet Control Message Protocol
IDS	- Intrusion Detection System
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
PDD	- Presidential Decision Directive
PKI	- Public Key Infrastructure
RA	- Registration Authority
RACF	- Resource Access Control Facility
RAID DASD	- Redundant Array of Inexpensive Disks DASD
SA	- System Administrator
SBU	- Sensitive But Unclassified
SE	- System Engineer/Developer
SSA	- System Security Administrator
SSL	- Secure Socket Layer
SVC	- Operating System Service Calls
TCP	- Transmission Control Protocol
TCP/IP	- Transmission Control Protocol/Internet Protocol

TSO	- Time Sharing Option
USDA	- United States Department of Agriculture
VM	- Virtual Memory
VPN	- Virtual Private Network
VSAM	- Virtual Storage Access Method
VTAM	- Virtual Telecommunications Access Method