

INFORMATION TECHNOLOGY SYSTEMS

TABLE OF CONTENTS

DM 3550-000

	Page
Chapter 10 – General Information	
1 Purpose	3
2 Cancellation	3
3 References	2
4 Scope	4
5 Abbreviations	4
6 Definitions	5
Part I – Security Architecture Framework (Reserved)	
3550-002	
Part 2 – Sensitive But Unclassified (SBU) Information Protection	
1 Background	1
2 Policy	2
3 Procedures	3
4 Responsibilities	5
Tables	
1 Information Categories Chart	
2 Levels of Concern for System Criticality/Sensitivity	
3 Media Encryption Chart	
4 Conditional Access to USDA Sensitive But Unclassified Information Non-Disclosure Agreement	
3550-003	
Part 3 – Portable Electronic Devices and Wireless Technology	
1 Background	1
2 Policy	2
3 Procedures	4
4 Responsibilities	5

Table

- 1 Wireless LAN Checklist
- 2 Bluetooth Checklist
- 3 PED Security Assessment Checklist
- 4 Suggested Personal Use Policy

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

DEPARTMENTAL MANUAL		Number: 3550-000
SUBJECT: Information Technology Systems	DATE: February 8,2006	
	OPI: Office of the Chief Information Officer, Cyber Security	

CHAPTER 10
GENERAL INFORMATION

1 PURPOSE

This Departmental Manual outlines requirements for a Security Architecture framework, handling and protection of Sensitive But Unclassified (SBU) or Sensitive Security Information (SSI) in these systems and security requirements for the use of Wireless Technology.

2 CANCELLATION

This Departmental Manual will be in effect until superceded.

3 REFERENCES

E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. 3531 et seq., Title III, Federal Information Security Management Act (FISMA)

Public Law 93-579, Privacy Act of 1974;

Public Law 98-502, Freedom of Information Act;

Public Law 99-474, Computer Fraud and Abuse Act;

Presidential Decision Directive 63, Policy on Critical Infrastructure Protection;

Office of Management and Budget Circular A-130, Security of

Federal Automated Information Resources, Appendix III;

NIST Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); specifies the use of Triple DES Security Requirements for Cryptographic Modules;

NIST Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules;

NIST Federal Information Processing Standard (FIPS) 180-2, Secure Hash Standard (SHS);

NIST Federal Information Processing Standard (FIPS) 186-2, Digital Signature Standard (DSS);

NIST Special Publication, 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems (2nd Public Draft);

NIST Special Publication, 800-48, Wireless Network Security;

Federal Acquisition Regulations (FAR), Subpart 9.5, Organizational and Consultant Conflicts of Interest;

DR 3440-2, Control and Protection of "Sensitive Security Information";

DM 3530-003, Chapter 6, Part 3, Use of Public Key Infrastructure (PKI) Technology;

DM 3535-001, Chapter 7, Part 1, USDA's C2 Level of Trust; and

DM 3515-002, Chapter 3, Part 2, Privacy Impact Assessments.

DN 3300-12, DN3300-012, (04/20/05) Commercial Wireless Technologies in USDA - Unclassified Security Requirements for Wireless Networks in Unlicensed Frequencies;

DN3300-013, (04/20/05) Commercial Wireless Technologies in USDA - Unclassified Security Requirements for Wireless Devices; and

Federal Information Processing Standard Publication 140-2, Security Requirements for Cryptographic Modules.

4 SCOPE

This manual applies to all USDA agencies, programs, teams, organizations, appointees, employees and other activities.

5 ABBREVIATIONS

ACL	Access Control List
AIS	Automated Information System(s)
AP	Access Point
CIO	Chief Information Officer
CRC	Cyclic Redundancy Check
CS	Cyber Security
I&A	Identification and Authentication
IP	Internet Protocol
IRM	Information Resources Management
ISP	Internet Service Provider
ISSPM	Information Systems Security Program Manager
IT	Information Technology
LAN	Local Area Network
MAC	Medium Access Control
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
PED	Personal Electronic Device
PL	Public Law
SSI	Sensitive Security Information
SBU	Sensitive But Unclassified
USDA	United States Department of Agriculture
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

6 DEFINITIONS

- a Access control - is the security service that helps ensure that LAN resources are being utilized in an authorized manner.
- b Availability - Assurance that information, services, and IT system resources are accessible to authorized users and/or system-

related processes on a timely and reliable basis and are protected from denial of service.

- c Configuration Management - A family of security controls in the management class dealing with the control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an IT system.
- d Confidentiality - Assurance that information in an IT system is not disclosed to unauthorized persons, processes or devices.
- e Controlled Access Protection - A standard that is applied to operating system software to provide a required minimum level of security. This standard rating for business computing products requires that the system have discretionary resource protection and auditing capability.
- f Decryption - The process of transforming encrypted data into plain or readable information.
- g Data Encryption Standard (DES) - A DES key consists of 64 binary digits of which 56 are randomly generated and used directly by the algorithm. (FIPS 46-3)
- h Encryption - the process of transforming readable information into cipher text.
- i Exposure - A measure of the potential risk to an IT system from both external and internal threats.
- j Identification and authentication - is the security service that helps ensure that the LAN is accessed by only authorized individuals.
- k IT System - The set of agency information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Categories of IT systems are major applications and general support systems.
- l Integrity - Assurance that information in an IT system is protected from unauthorized, unanticipated, or unintentional modification or destruction. System integrity also addresses the quality of an IT

system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

- m Levels of Concern - An expression of the criticality/sensitivity of an IT system in the areas of confidentiality, integrity, availability, and exposure, expressed qualitatively as high, moderate or low. The level of concern indicates the extent to which security controls must be applied to an IT system based on risk, threat, vulnerability, system interconnectivity considerations, and information assurance needs.
- n Medium Access Control (MAC) Address - At the lowest level, computers communicate with each other using this hardware address.
- o Need-to-Know - The necessity for access to, or knowledge or possession of, specific information required to carry out official duties.
- p Personal Digital Assistant - a handheld computer that serves as an organizer for personal information. It generally includes at least a name and address database, a To Do List and a note taker. The unit may include a small on-screen keyboard that is tapped with a pen. Data is synchronized between a user's PDA and desktop computer by cable or wireless transmission.
- q Plain text - unencrypted information or data
- r Portable Electronic Device (PED) - any electronic device that is capable of receiving, storing, or transmitting information using any format (i.e., radio, infrared, network or similar connections) without permanent connections to Federal networks. Laptops and workstations without permanent connections to a Federal network will be covered in a separate chapter/policy document.
- s Privacy Act Record -[the substance of a record i.e.,]any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the

identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

- t Sensitive Information - Information the loss, misuse, or unauthorized access to or modification of, which would adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. Systems that are not national security systems, but contain sensitive information, are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235). Some specific categories of sensitive information are protected by statute, regulation or contract, (e.g., privacy information, proprietary information, export control information, pre-publication academic information).
- u Triple DES - a key that consists of three DES keys, also referred to as a key bundle. (FIPS 46-3)
- v Virtual Private Network (VPN) - a technology by which authorized individuals (such as remote employees) can gain secure access to an organization's intranet via the Internet.
- w Wireless Technology - a transport mechanism that supports communication between mobile, portable or fixed facilities through the use of the electromagnetic spectrum without a physical connection.