CHAPTER 6 – PART 5
Encryption Security Standards

1 BACKGROUND

All USDA agencies and staff offices need to transmit Sensitive But Unclassified (SBU) over open networks. In using IT to continuously improve mission performance, the USDA is becoming more interconnected to open networks and other emergent global networks. The openness of these networks enables malicious cyber attacks against sensitive USDA assets and increases the potential risk to sensitive information. This risk is compounded through the use of the Internet and other non-secure mediums such as Wireless Local Area Network technology, Microwave, and Radio technologies. This technology includes utilizing Laptops and Personal Electronic Devices (such as cellular telephones, pagers and hand held computers) to communicate and process USDA information from any location.

Encryption methods can protect sensitive information during storage and transmission. They provide important functionality to reduce the risk of intentional and accidental compromise and alteration of data. Encryption algorithms use a mechanism called a key, which is used to render the information unreadable during transmission. While the information is encrypted it is mathematically protected against disclosure because it is cannot be read by some one who does not have a corresponding key to decrypt the information. Encryption methods serve as part of the USDA defense-in-depth strategy and provide reasonable protection of sensitive information at a comparatively low cost.

The primary factor that must be considered when determining if encryption is required is data sensitivity. Data sensitivity is a measure of the importance and nature of the information processed, stored, and transmitted by an IT system to the organization's mission and day-to-day operations. The sensitivity of information can be addressed by analyzing the system requirements for confidentiality, integrity, and availability.

2 POLICY

All USDA agencies and staff offices will use the Approved Protocols and Protection Techniques outlined in Section 3, Procedures, below. Encryption will be used in all IT systems that process and store SBU to preclude disclosure to unauthorized internal and external parties. This policy also applies to all parties that store and process SBU on behalf of USDA agencies and staff offices.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation time; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with an updated timeline for completion. CS will monitor all approved. All SBU/SSI information will be encrypted, no exceptions will be considered to this requirement.

3 PROCEDURES

This Sensitive Information Transmission Policy sets forth the following requirements:

(1) All telecommunication and network encryption systems will have an encryption plan approved by the agency Information Systems Security Program Manager (ISSPM) or Security Officer;

(2) All sensitive USDA information transmitted will be encrypted in accordance with the Media Encryption Chart requirements outlined in Table 2;

(3) Sufficient redundancy and capacity needs to be incorporated into departmental or agency mission critical and essential communication systems to prevent transmission of SBU/SSI information in clear text;

(4) SBU/SSI will be processed and store as required by DM3535-001, USDA's C2 Level of Trust;

(5) Agencies and staff offices will exercise control over keys used in any encrypted transmissions.

Approved Protocols and Protection Techniques - All protocols must deploy either the Triple DES or the Advanced Encryption Standard approved by NIST. Encryption products used to protect sensitive information will conform to the NIST Cryptographic Module Validation Program validated listing. All encryption implementations will conform to the Level 2 Security requirements as specified in FIPS-140-2 unless otherwise identified in this policy. Agencies should contact CS for key size recommendations or any specific protocol questions. These requirements aid in providing a trusted computing base for encryption services which is essential for maintaining the confidentiality, integrity and non-repudiation of the sensitive information that these systems process. The Encryption Algorithms shown below can be used to protect sensitive information:

(1) IPSEC- is a suite of authentication and encryption protocols, suitable for all types of Internet Protocol (IP) traffic and is used to create virtual private networks (VPN) which allow sensitive information to be sent securely between two end stations or networks over an un-trusted communications medium. IPSEC technology should be considered as a technology to secure Internet and other IP communications within the USDA and agency corporate networks and to connect to authorized external customers at defined locations;

(2) Secure Shell (SSH) – may be deployed solely for the remote administration of sensitive systems;

(3) Secure Sockets Layer (SSL) – the secure sockets layer specification may be deployed to provide secured access to sensitive information on Web servers. When SSL is used to protect USDA sensitive information, the latest version (currently SSLv3) should be used with 128-bit encryption;

(4) Virtual Private Networks (VPN) – should be deployed in environments where data-link layer encryption would not be a practical solution to maintain and operate. VPN technology using IPSEC encryption allows it to be implemented independent from a particular link layer communications technology (e.g., HDLC, Frame Relay, FDDI, Ethernet, Gigabit Ethernet, ATM, etc.) As such, this policy strongly encourages the use of VPN technology to secure departmental and agency sensitive communications;

(5) Data-Link (symmetrical) Encryption – may be used in environments where Virtual Private Network management would not be a reasonable encryption implementation to maintain and operate and where the use and management of VPN technology would not be warranted;

(6) Pretty Good Privacy (PGP) – may be used to protect sensitive information transmitted via e-mail using a minimum key size of 2048 bits. Public key information may be maintained on public or internal PGP key servers**;**

(7) Public Key Infrastructure (PKI) – These implementations are suitable for all environments and must follow Cyber Security DM3530-003, Public Key Infrastructure (PKI) Technology;

(8) Secure /Multipurpose Internet Mail Extension (S/MIME) – Like PGP, S/MIME is a standards-based security enhancement to secure message attachments and provides strong authentication through digital signatures, message confidentiality, integrity and non-repudiation.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Provide technical policies and standards for encryption that is to be deployed throughout the USDA's Information Technology environment;

(2) Formulate departmental encryption strategies;

(3) Promptly review for approval requests for policy exceptions and provide a response to the agency/mission area;

(4) Conduct periodic reviews to ensure compliance by USDA agencies with this policy by auditing encryption implementations; and,

(5) Periodically review and update this policy and the procedures as required.

b Agency Management and Information Technology Officials or Chief Information Officer will:

(1) Ensure the provisions of this policy are implemented in all agency/mission area IT environments;

(2) Develop and prepare an Encryption Plan in accordance with Table 1 of this document. This plan will detail encryption use for all agency networks and mobile computing systems;

(3) Make sure that all relevant agency personnel are acquainted with the provisions of this policy and procedures with a focus on the Information Systems Security Program Manager and System/Network Administrators;

(4) Make certain that all agency security plans and internal operating procedures include encryption as part of the plan's technical controls with instructions for the secure use of approved encryption protocols;

(5) Prepare formal exception requests for encryption algorithms and techniques that do not meet the requirements of this policy in conformance with the policy exception section above; exceptions will be signed by the Agency Head/CIO and will be forwarded to OCIO; and,

(6) Receive, review and coordinate a response and mitigation strategy/schedule to the Associate CIO for Cyber Security for any deviations from this policy not covered by a pre-existing waiver.

c <u>The agency Information Systems Security Program Managers(ISSPM) will:</u>

(1) In coordination with the agency SA/NA will ensure that all agency telecommunication and computing infrastructures comply with this policy and standards;

(2) Review agency Encryption Plans to ensure that they comply with the requirements of this policy;

(3) Include the requirements of this policy in agency security program and system security plans and internal operating procedures to ensure secure use of approved encryption algorithms, protocols and techniques;

(4) In conjunction with the agency SA/NA, ensure that all VPN connections are centrally managed and users of VPN systems are fully authenticated;

(5) Conduct periodic reviews of all encryption to determine compliance with protocols and standards; report any non-compliant encryption algorithms and methods to the Agency Head/CIO and monitor non-compliance remediation;

(6) Participate in the preparation of waiver packages, as required.

d Agency System/Network Administrators will:

(1) Ensure that agency encryption complies with this policy and standards;

(2) Include these standards and approved protocols in systems that address internal operating procedures for encryption;

(3) Participate in the central management of all agency VPN connections ensuring that users of VPN services are fully authenticated; the system owner of the application or network that is the provider of the sensitive information being accessed must manage each end of the VPN service;

(4) Review all agency encryption implementations to ensure that they comply with this policy; actively participate in the preparation of waiver packages, as required.

- END –

Table 1
ENCRYPTION PLAN REQUIREMENTS

In accordance with the Office of Management and Budget Guidance on Data Availability and Encryption, each implementation will include an encryption plan. Required components in the agency encryption plan include:

(a) A configuration layout, showing complete end-to-end details of the telecommunication or computer systems encryption points;

(b) The type of encryption to be used;

(c) The source of key generation and insertion for symmetrical encryption methods;

(d) The cryptographic period required; that is, the amount of time before a session key should be updated. The maximum valid age of the cryptographic period is 60 days; and

(e) The system procedures for key loading, key generation, key protection and distribution, key recovery and key destruction.

Each agency will have key recovery procedures to recover sensitive information encrypted when the information is stored electronically.

TABLE 2

Media Encryption Chart

Transmission Media	Encryption Required	Comments
Local Area Networks	**No**	If LAN is accredited
E-mail	**Yes**, by Agency	If transmitting SBU data
Tail Circuit	**Yes**, by Agency	If transmitting SBU data
Dedicated Circuits (Analog, Digital, Broadband, ATM, Frame Relay)	**Yes**, by Agency	If transmitting SBU data
WAN Circuits (Between Nodes)	**Yes**	TSO provides
USDA Backbone Network	**Yes**	TSO provides
Agency Networks	**Yes**	If transmitting SBU data
Infrared (Laptops, PDAs)	**Yes**, Agency	If transmitting SBU data in a Public Area
Satellite	**Yes**, Agency	If transmitting SBU data within Footprint
Microwave	**Yes**, Agency	If transmitting SBU data Node to Node
Wireless (Radio, Cell Phones)	**Yes**, Agency	If transmitting SBU data