CHAPTER 10, PART 2
SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION PROTECTION

1 BACKGROUND

The United States Department of Agriculture houses and processes all types of sensitive data, including information relating to the privacy of US citizens, payroll and financial transactions, proprietary information and life/mission critical data. It is essential that this information be properly handled, stored and protected from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction. The Information Categories Chart in Table 1 gives some examples of different types of Sensitive But Unclassified (SBU) information that is the focus of this section. SBU information also includes Sensitive Security Information (SSI). However the SBU category contains information that is not security related but is still sensitive in terms of its risk of exposure.

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. Table 2 defines Levels of Concern for sensitive information.

USDA and agency corporate networks are at risk because sensitive information is relayed across telecommunications service provider networks where the information can be easily intercepted en route. Key areas of risk to USDA sensitive information include, but are not limited to:

Spoofing: Using the Internet Protocol and web servers to transmit information have become a standard way for the USDA to conduct E-Government initiatives, primarily using World Wide Web technology. It is relatively easy to mimic a legitimate site and fool users into believing that they are making a trusted transaction, when in reality, they are sending information to a false site.

Data alteration: Contents of data packets can be altered so as to falsify information en route. Sensitive information can be compromised, either accidentally or maliciously to provide inaccurate information.

Unauthorized Disclosure: When data packets are traversing an open network (i.e., the INTERNET) prior to being received at the destination address, a hacker can potentially intercept these packets and read them at will. Additional filtering can alert a hacker to specific data packets that look like a series of numbers (potential credit card numbers, or social security numbers), strings that contain an "@" (e-mail addresses), or "$" (cash or monetary information) or prompts for password and user identification combinations.

SBU/SSI information is also at risk because of careless handling and storage of this data. Unauthorized disclosure also occurs when SBU/SSI is handled as routine and not afforded the protection it deserves.

2 POLICY

All USDA agencies and staff offices will identify and provide adequate security protection for Sensitive But Unclassified (SBU)/Sensitive Security Information (SSI). Further, SBU/SSI information will be encrypted in accordance with Cyber Security and NIST guidance concerning approved encryption standards and digital signatures to prevent disclosure of sensitive information to internal and external users. Each agency and staff office will provide a report to Cyber Security annually that identifies all SBU/SSI systems/information.

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 exceptions.

3 PROCEDURES

The following procedures apply to the processing, handling and storage of SBU/SSI data:

(1) All agencies and staff offices will analyze their information to determine levels of concern for the data in accordance with OMB A-130 and NIST 800-37 requirements;

(2) All SBU/SSI information transmitted via any media will be encrypted in accordance with the Media Encryption Chart requirements outlined in Table 3;

(3) Each agency or staff office will establish and implement key recovery procedures for all SBU/SSI information which is stored in an encrypted state;

(4) SBU/SSI information with a high level of concern generally should not be discussed on telephones, pagers, cell phones or other wireless devices as they are not secure and the risk of interception of the transmission is great; using other than Secure telephonic devices to discuss SBU/SSI information shall only be allowed where the degree of risk is understood and accepted;

(5) Secure fax should be used to transmit SBU/SSI with a high level of concern;

(6) Agencies and staff offices will analyze all information available or to be published on public Web pages to ensure that SBU/SSI information is not made available except on a need-to-know basis;

(7) SBU/SSI shall be processed and stored only on systems that meet DM 3535-001, Chapter 7, Part 1, USDA's C2 Level of Trust;

(8) Agencies and staff offices will shred SBU/SSI documents of high level concern in lieu of disposing of them in the trash to prevent unauthorized disclosure;

(9) Mobil systems, computers, and Personal Electronic Devices (PED) may be used to house SBU/SSI data only when required by official duties; this information must be encrypted during storage to protect against unauthorized disclosure. When the mobil system, computer, or PED is no longer required for official business, the SBU/SSI data must be removed with software to overwrite the sensitive information in accordance with USDA regulations;

(10) Care must be taken by agencies and staff office to avoid leaving SBU/SSI information with a high level of concern readily available at workstations or on personal computer screens; SBU/SSI with a high level of concern will be stored on a floppy disk or zip drive in a locking desk drawer, file cabinet or locked office;

(11) Access to SBU/SSI will be provided to employees with a Need-To-Know; when SBU/SSI data must be shared with contractors and entities outside USDA a Non-Disclosure Agreement Form (Table 4) must be executed by the information owner or agency ISSPM prior to granting access to the data to preclude possible organizational or personal conflicts of interest in accordance with FAR Subpart 9.5;

(12) All Statements of Work (SOW) and Procurement Requests for IT services on systems that contain SBU/SSI information will contain specific security requirements to include background investigations;

(13) SBU/SSI information must be marked in a conspicuous manner with the following notice: "Sensitive But Unclassified/Sensitive Security Information – Disseminate on a Need-To-Know Basis Only" in accordance with agencies regulations; electronic messages will be marked with this notice as well; and

(14) All Freedom of Information Act (FOIA) requests for SBU/SSI will be processed in accordance with agency regulations and the Attorney General's memorandum.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Formulate and publish policy and procedures for the protection, handling and storage of SBU/SSI information;

(2) Coordinate with agencies and staff offices to ensure that all SBU/SSI information is identified;

(3) Perform regular reviews of the implementation of SBU/SSI policy within the agencies and staff offices; and

(4) Maintain an electronic database of SBU/SSI systems/information identified by agencies and staff offices;

(5) Review and, if appropriate, approve waivers to the requirements of this policy.

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) Make sure that all relevant agency personnel are acquainted with the provisions of this policy; in particular this shall include the Information Systems Security Program Manager and System/Network Administrators;

(3) Prepare formal waiver requests for systems that do not meet the requirements of this policy in conformance with the waiver section above; waivers will be signed by the Agency Head or CIO and will be forwarded to OCIO;

(4) Ensure that systems are analyzed to determine levels of concern for data and formally identify SBU/SSI information;

(5) Establish key recovery procedures for SBU/SSI information stored in encrypted form;

(6) Ensure that security awareness training is provided to focus on SBU/SSI information processing, handling and storage;

(7) Maintain SBU/SSI systems in compliance with Controlled Access Protection and Configuration Management requirements;

(8) Control the transmission of SBU/SSI information and provide encryption as required to protect sensitive information from disclosure;

(9) Ensure that all contracts for IT systems with SBU/SSI information contain security requirements and that contractors complete the necessary Confidentiality and Non-Disclosure Forms; provide access to SBU/SSI data on a need-to-know basis.

c The agency Information Systems Security Program Managers(ISSPM) will:

(1) In coordination with the agency System and Network Administrators, will ensure that all agency telecommunication and computing infrastructures comply with this policy and standards;

(2) Participate in the identification of Levels of Concern for agency information and make recommendations concerning approved encryption protocols;

(3) Assist in establishing key recovery procedures for all information stored in encrypted format;

(4) Periodically review all IT systems and information to ensure that they have been properly reviewed for SBU/SSI requirements and that protections are implemented by business owners;

(5) Conduct security awareness and training that focuses on the proper handling, storage and processing of SBU/SSI data by agency employees and contractors;

(6) Maintain copies of Confidentiality and Non-Disclosure Agreement forms for all SBU/SSI systems; and

(7) As requested, participate in the development of Waiver packages for systems not in compliance with this policy.

d Agency System/Network Administrators will:

(1) Ensure that agency systems comply with this policy and standards;

(2) Participate in establishing security controls for all SBU/SSI systems in accordance this policy, Controlled Access and Configuration Management procedures;

(3) Participate with the ISSPM in the periodic review of SBU/SSI systems and in waiver requests for systems that do not meet requirements; and

(4) Ensure that all SBU/SSI systems have been hardened, configured and scanned in accordance with Cyber Security guidance to ensure protection requirements are in place and working properly.

-END-

TABLE 1: INFORMATION CATEGORIES

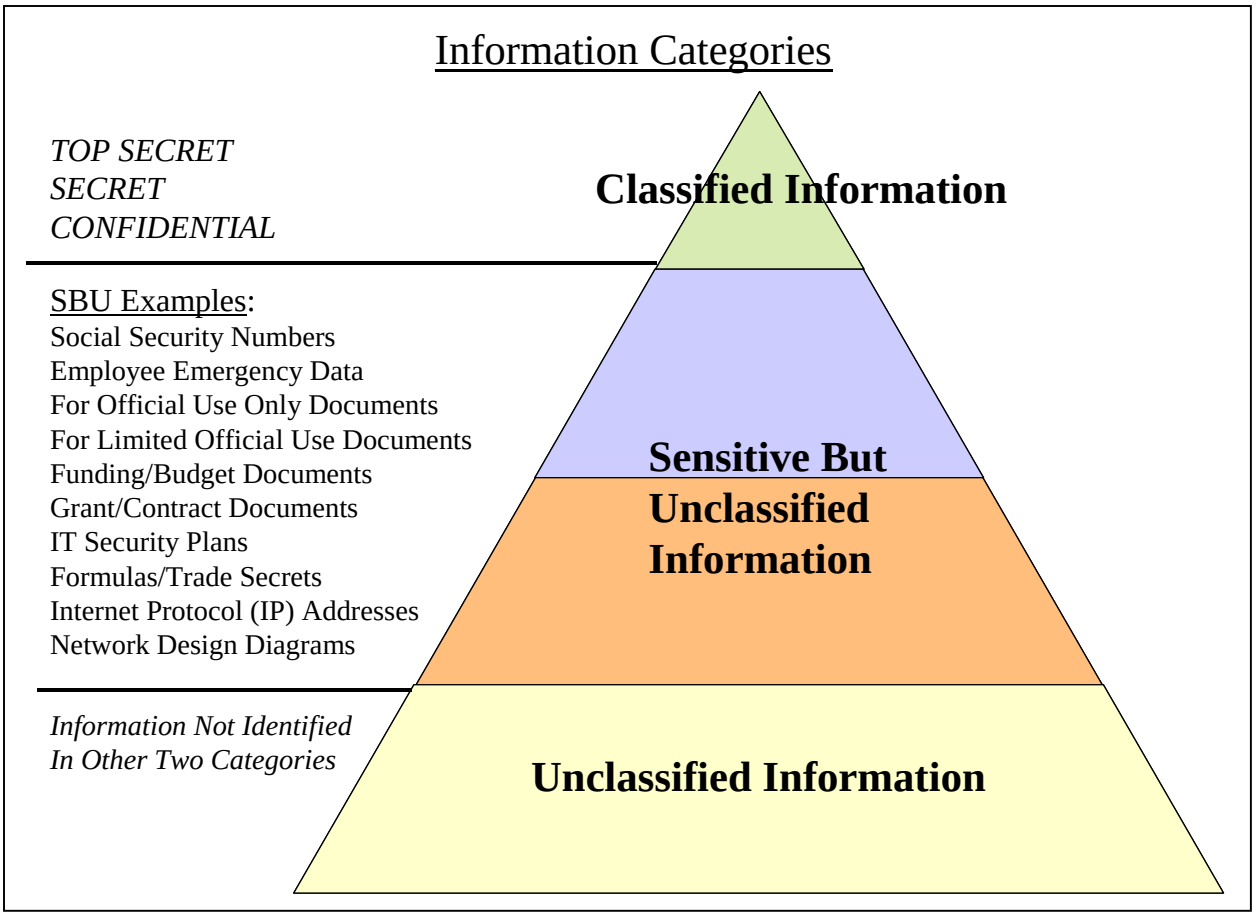

Table 2: LEVELS OF CONCERN FOR SYSTEM CRITICALITY/SENSITIVITY

	Low	Moderate	High
Confidentiality Sensitive Information (Unclassified)	Loss of confidentiality could have some negative impact on mission accomplishment.	Loss of confidentiality could degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	Loss of confidentiality could prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
Confidentiality National Security Information (Classified)	Not applicable	Not applicable	Loss of confidentiality could cause exceptionally grave damage, serious damage or damage to the national security.
Integrity	Loss of integrity could affect agency-level interests and have some negative impact on mission accomplishment.	Loss of integrity could adversely affect agency-level interests, degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	Loss of integrity could adversely affect national-level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.
Availability	Loss of availability could affect agency-level interests have some negative impact on mission accomplishment.	Loss of availability could affect agency-level interest, degrade mission accomplishment or create unsafe conditions that may result in injury or serious damage.	Loss of availability could adversely affect national -level interests, prevent mission accomplishment or create unsafe conditions that may result in loss of life or other exceptionally grave damage.

Table 3: MEDIA ENCRYPTION CHART

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**, by Agency	If transmitting SBU data in a Public Area
Satellite	**Yes**, by Agency	If transmitting SBU data within Footprint
Microwave	**Yes**, by Agency	If transmitting SBU data Node to Node
Wireless (Radio, Cell Phones)	**Yes**, by Agency	If transmitting SBU data

Table 4:
Conditional Access to USDA Sensitive but Unclassified Information Non-disclosure Agreement

I, _____, hereby consent to the terms in this Agreement in consideration of being granted conditional access to certain United States Government documents or material containing sensitive but unclassified information.

I understand and agree to the following terms and conditions:

By being granted conditional access to sensitive but unclassified information, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure in accordance with the terms of this agreement.

As used in this Agreement, sensitive but unclassified information is any information which the loss, misuse, or unauthorized access to of modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C Section 552a, 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 the national defense or foreign policy.

I am being granted conditional access contingent upon my execution of this Agreement for the sole purpose of (identify the nature of contract work or special project). This approval will permit me conditional access to certain information, (identify type(s) of information, e.g., documents, memoranda, reports, testimony, deliberations, maps, drawings, schematics, plans, assessments, etc.) and / or to attend meetings in which such information is discussed or otherwise made available to me. This agreement will not allow me access to materials to which (the United States Department of Agriculture (USDA) or USDA Agency /Office) has predetermined, in its sole discretion, are inappropriate for disclosure pursuant to this Agreement. This may include sensitive but unclassified information provided to USDA by other agencies of the United States Government.

I will never divulge any sensitive but unclassified information, which is provided to me pursuant to this Agreement to anyone, unless I have been advised in writing by (the USDA or USDA Agency / Office) that the individual is authorized to receive it. Should I desire to make use of any sensitive but unclassified information, I will do so in accordance with Paragraph 6 of this Agreement. I will submit to the USDA or USDA Agency / Office for security review, prior to the submission for publication, any book, article, column or other written work for the general publication that is based on any

knowledge I obtained during my work on (name of project) in order for the (USDA or USDA Agency / Office) to ensure that no sensitive but unclassified information is disclosed.

I hereby assign to the United States Government all royalties, remunerations, and emolument that have resulted, will result or may result from any disclosure, publication, or revelation of sensitive but unclassified information not consistent with the terms of this Agreement.

If I am permitted, at the sole discretion of (the USDA or USDA Agency / Office), to review any official documents containing sensitive but unclassified information, such review will be conducted at a secure USDA or USDA Agency / Office facility or under circumstances which have been approved by the USDA to maintain the security protection of such material. I will not be permitted to and will not make any copies of documents or parts of documents to which conditional access is granted to me. Any notes taken during the course of such access will remain at (the USDA or USDA Agency / Office), to be placed in secure storage unless it is determined by (the USDA or USDA Agency / Office) officials that the notes contain no sensitive but unclassified information. If I wish to have the notes released to me, (USDA or USDA Agency / Office) officials will review the notes for the purposes of deleting any sensitive but unclassified information to create a redacted copy of the notes. If I do not wish a review of any notes that I make, those notes will remain sealed in secure storage at the (USDA or USDA Agency / Office).

If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of sensitive but unclassified information could compromise the security of the (USDA or USDA Agency / Office).

If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to sensitive but unclassified information. This may serve as a basis for denying me conditional access to (USDA or USDA Agency / Office) information, but classified and sensitive but unclassified information in the future. If I violate the terms and conditions of this Agreement, the United States may institute a civil action for damages or any other appropriate relief. The willful disclosure of information to which I have agreed therein not to divulge may constitute a criminal offense.

Unless and until I am provided a written release by (the USDA or USDA Agency / Office) from this Agreement or any portions of it, all conditions and obligations contained in this Agreement apply both during my period of conditional access, which shall terminate at the conclusion of my work on (name of project / contract), at all times thereafter.

Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

I understand that the Unites States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.
By granting me conditional access to information I this context, the United States Government does not waive any statutory or common law evidentiary privileges or protections that it may assert in any administrative or court proceeding to protect any sensitive but unclassified information to which I have been given conditional access under the terms of this Agreement.

These restrictions are consistent with and do not supersede, conflict with or other wise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Protection Act of 1982 (50 U.S.C.421 et seq.)(governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798 and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statues are incorporated into this Agreement and are controlling.

My execution of this Agreement shall not nullify or effect in any manner any other secrecy or nondisclosure Agreement which I have executed or may execute with the United States Government.

I make this Agreement in good faith, without any mental reservation or purpose of evasion.

_____ _____

Name Date

This Agreement was accepted by the undersigned on behalf or the (USDA or USDA Agency / Office) as a prior condition of conditional access to sensitive but unclassified information required for the completion of official duties on (Project of Contract Name / number).

_____ _____

Authorized Government Official of USDA (or USDA Agency / Office) Date