CHAPTER 7 – PART 1
USDA's C2 LEVEL OF TRUST

1 BACKGROUND

USDA has traditionally depended upon diverse and rapidly changing commercially available IT resources to support its business practices and deliver services to the public. Often those resources have been implemented without consideration or implementation of minimum secure access controls and therefore, leaves sensitive information vulnerable to exploitation. USDA is establishing the minimum secure access control settings by defining its version of a Controlled Access Protection (C2) policy. This secure access control will be utilized until such time as the Common Criteria (CC) settings are available. Class C2 when implemented according to this policy by USDA agencies/staff office and contractors will meet the minimum security requirements necessary to implement, maintain, and enforce the level of trust required for sensitive data.

The Computer Security Act of 1987 (P.L. 100-235) was enacted to create "a means for establishing minimum acceptable security practices" for federal unclassified computer systems. The Act also emphasizes that federal information requires protection against unauthorized modification or destruction, as well as unauthorized disclosure. To distinguish systems covered by P.L. 100-235 from those used to process national security information, the law uses the term "sensitive". Confusion over this term may have led some agencies to focus their limited computer security resources on determining which systems would be labeled "sensitive". Information "owners" should use a risk based approach to determine what harm may result if a system is inadequately protected. The intent of the Computer Security Act is to assure <u>adequate protection of all federal IT systems</u>. NIST believes, as does CS, that all unclassified agency information requires some degree of protection to provide confidentiality, integrity or availability. Therefore each agency must determine the appropriate level of protection required for their systems. Sensitive information includes Privacy Act information, information exempt from release under the Freedom of Information Act (FOIA), procurement information that has not been released to the public and documents with handling restrictions such as Limited Official Use Only (LOUO) and For Official

Use Only (FOUO). All agencies will evaluate the degree of data sensitivity based on confidentiality, integrity and availability.

Information is one critical resource that enables organizations to succeed in their mission. Additionally, individuals have a reasonable expectation that their personal information contained in agency IT products or systems remain private, be available to them as needed, and not be subject to unauthorized modification. IT products or systems should perform their functions while exercising proper control of the information to ensure it is protected against hazards such as unwanted or unwarranted dissemination, alteration, or loss. Adequate IT security needs to be in place to prevent/mitigate these hazards.

When using standard or default installation parameters, many operating systems are considered insecure. However, most of the companies that develop and market operating systems have documented the necessary parameter settings to achieve the C2 security level. C2 is a standard that is applied to operating system software to provide a required minimum level of security. This standard is the highest government rating for business computing products and requires that the system have discretionary resource protection and auditing capability. CS is implementing the first two parts of C2 Controlled Access Protection, specifically security policy and accountability, as defined below and a need-to-know requirement. These five parts, as modified, comprise USDA's C2 Level of Trust.

The National Computer Security Center issued the first DOD Trusted Computer System Evaluation Criteria (TCSEC), commonly referred to as the "Orange Book" in August 1983. It was reissued in December 1985 as a DOD Standard (DOD 5200.28-STD). The TCSEC Standard serves the following purposes:

- Provides product manufacturers with a standard of security features to build into their products;
- Provides DOD components with a metric to evaluate how much trust can be placed in an automated information system for secure processing of classified or other sensitive data; and
- Provides a basis for specifying security requirements in acquisition specifications.

More information on TCSEC can be found at http://www.radium.ncsc.mil/tpep/library/tcsec/index.html. The TCSEC standard has been superseded by the Common Criteria (CC).

This policy is issued with the understanding that the CC will eventually replace the USDA C2 Level of Trust implemented by this directive. This issue will be reviewed on an annual basis to determine when CC will be implemented. NSA and NIST developed CC, in cooperation with the National Information Assurance Partnership (NIAP), as a security evaluation scheme that enables vendors of IT systems to provide C2 equivalent protection capabilities and is an international standard. When the CC is fully implemented and vendors offer comprehensive product lines that fully meet the standards this material will be modified. The CC represents the outcome of a series of efforts to develop criteria for evaluation of IT security that is broadly useful both nationally and internationally. CC is based on the TCSEC but is more flexible and adaptable to the evolving nature of IT security in general. More information can be found on CC at http://csrc.nist.gov/cc/ or http://www.commoncriteria.org.

Currently, acceptable CC settings are not available for this standard. In the interim, all USDA servers and mainframes and mainframes will be hardened to the USDA C2 Level of Trust until CC settings are formulated and published. The National Policy on Controlled Access Protection dated 7/17/87 directs all Federal agencies to provide automated Controlled Access Protection (C2 level) for all sensitive or classified information processed or maintained by automated information systems (AIS), when all users do not have the same authorization to use the sensitive information. All authorized accesses shall be implemented, executed and completed by authentication in the form of passwords, personal identification numbers (PINs), tokens (Smartcards or dongels), biometrics or private keys. This policy also expands the principle of C2 (need to know) control.

2 POLICY

It is USDA policy that agencies/mission areas implement USDA's C2 Level of Trust on all servers and mainframes storing, processing or maintaining mission critical or sensitive information. Any server or mainframe involved with the management, retention or transmission of sensitive data or information shall be hardened to establish a “need to know” environment and have the functional equivalent of USDA’s C2 Level of Trust or the Common Criteria Evaluation Assurance Level EAL3.

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. The request shall include:

a Business case detailing the reasons C2 hardening can not be accomplished and a cogent justification for continuing to operate a sensitive server in an unsecured environment.

b Details explaining how the confidentiality, integrity and availability of the sensitive information will be preserved;

c Any associated costs for an alternative approach funded by the proposing agency;

d Any negotiations required with other entities for implementation and/or support undertaken by the proposing agency will be outlined. This will remain separate from any agreements regarding the confidentiality, integrity and availability of the sensitive information;

e Assurances that any alternatives implemented will not adversely affect the costs, security, maintenance or operations of existing solutions implemented by other Departmental entities; and

f A schedule and tasks to be undertaken to render the server compliant.

CS reserves the right to conduct periodic reviews of all USDA sensitive information servers and mainframes. These servers and mainframes must be adjusted, as necessary, to conform to the Integrated USDA Enterprise Architecture and security standards.

3 PROCEDURES

a <u>There are five principles of USDA's Level of Trust Platform. They are: Identification and Authentication, Need to Know, Discretionary Access Control, Object Reuse, and Audit Trails</u>.

(1) <u>Identification And Authentication</u>. Identification and Authentication is the <u>first requirement</u> of USDA's C2 level of Trust. All authorizations to access and use IT resources will be granted based on official business need. Accesses will be authorized by the agency business owner responsible for managing and controlling the IT resources and will be reviewed periodically for accuracy. After authorization, system access can be loaded by non-government personnel. Each access, whether a USERID or process, will be identified to an individual and will not be shared.

A USDA mandatory minimum password length <u>of 6 - 8 alphanumeric characters</u> will be established. To comply with USDA's C2 Level of Trust, passwords for all general users of systems, applications or processes shall be <u>changed every</u> <u>60 days.</u> Passwords issued to privileged users (system administrators, system managers, auditors and engineers) will be <u>changed every 30 days</u>. All passwords will be encrypted and dictionary words shall not be used for passwords. As a routine courtesy, the users may be notified by the system in advance that their password will expire. Logons/passwords shall not be automated through use of functions keys, scripts, or other methods where logons/passwords may be stored on systems. Passwords can be established by agencies for specific groups that do not follow general user requirements. However, the authority to establish the group, the password standards, duration and assurances of proper security controls in place to protect the system must be documented in a formal waiver to OCIO. In no case, will password groups be established before an approved waiver is in place.

Whenever access is to be gained by remote methods, passwords shall be supplemented with personal identification numbers (PINs), tokens (USB port or software), smart cards or some other trusted authentication device/procedure. Systems shall not allow reuse of a previously used password until after 5 other different passwords have been used.

(2) Need-To-Know. Need-to-Know is the second requirement of USDA's C2 Level of Trust. All accesses shall be limited to only the resources that a user needs to complete or facilitate official duties. Need-to-know shall be determined by the executive or manager deemed to be the system owner of the asset and that individual will authorize access. Need-to-know may be modified based on temporary assignments or projects with modifications requested or initiated by the project manager or supervisor and the approval of the system owner.

(3) Discretionary Access Control. Discretionary Access Control (DAC) is the third requirement for USDA's C2 compliance. DAC is an access policy in which the system owner restricts access to system objects such as files, directories, devices, databases, and programs, based on the identity of the users and/or groups to which they belong. "Discretionary" means that the owner of the information or system controls access permissions to those resources. The DAC mechanism shall, either by explicit user (owner) action or documented default, provide that objects are protected from unauthorized access. The access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing permission(s) to access sensitive information shall be granted only by the assigned system owner. The documentation and implementation of Discretionary Access Control (DAC) is necessary to maintain USDA's

C2 Level of Trust. DAC implementation requires not only "need-to-know", but also the practice of "least privilege". Separated employees/contractors shall have their access removed immediately prior to their departure. System owners will periodically review access controls and reconcile any discrepancies between system users and their access by adding, removing or changing employees/contractors, as required.

In addition to Need-to-know, USDA's C2 requires implementation of least privilege. Least privilege is defined by NIST as: "the security objective of granting users only those accesses required to perform their duties". Least privilege may mean that some employees have significant access while other employees with the same need-to-know have less access. The most restrictive set of privileges is granted to a user to perform authorized tasks. For example, an ISSPM may receive the same access to the same system alerts or security patches (need-to-know) as the system administrator. However, the ISSPM does not have the capability to install the patches (least privilege).

DAC can include the construction of access control lists or modification of system/object parameters. Access Control Lists (ACLs) shall be documented by the system owner/administrator and updated each time there is a change in an object's accessibility or when accesses are no longer needed. ACLs shall be deleted when no longer needed.

Another important element in access control is separation of duties. This refers to dividing roles and responsibilities so that a single individual cannot subvert a critical system. DACs will be implemented in compliance with separation of duties.

(4) Object Reuse. The fourth requirement of USDA C2 is Object Reuse. Object Reuse is capability and assurance that storage object/device (memory, disk, tape, cartridge/cassette, and CD-ROM) storing sensitive data has been rendered inaccessible before

it is used for other purposes. C2 security requires operating systems to clear memory locations before using those locations to process another function. For example, data stored in memory must be unavailable before that memory location can be reused. If the security system's OBJECT REUSE function is not activated then a waiver must be obtained from the OCIO. All data storage devices shall be rendered unreadable by degaussing, overwriting (5-7 times with random 1's and 0's) or complete physical destruction prior to disposal.

(5) Audit Trails. The fifth requirement for C2 compliance is that the system must have valid audit trail capabilities. An audit trail is a series of records of computer events, about an operating system, application, or user activities. A computer system may have several audit trails, each devoted to a particular type of activity. Auditing is a review and analysis of management, operational, and technical controls. It is considered valid if the records of detailed transactions provide: who completed the transaction, what did the transaction accomplish or attempt, where did the transaction take place and when did it occur. In other words it satisfies the questions, who, what, when, where and becomes a matter of permanent record. Audit trail reviews should be conducted every 30 days or more frequently depending on the transaction volume of the system.

Audit trails maintain a record of activity both by the system/ application processes and track user activity on the systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, security performance problems, and flaws in applications. Immediate action should be taken to report all security violations in accordance with DM 3505-001, Chapter 1, Incident Response Procedures and to correct security vulnerabilities and application flaws. Archived audit logs will be maintained for a minimum of three years and kept as a separate backup for easy retrieval when needed.

The operating system must provide an audit trail for system users, time/date of logon or logoff, and the workstation/IP address used. The operating system must allow read-only access to the audit log. The audit log should indicate usage of communication ports within the system.

b The Common Criteria specify a series of Evaluation Assurance Levels (EAL) for evaluated products. The higher the EAL, the higher level of confidence that a product provides security functionality which is performed correctly, effectively and in accordance with expectations. At a minimum, the server or mainframe operating system must be configured in accordance with the five principles of :

identification/authentication, need to know, discretionary access controls, object reuse, and audit trails and must be resistant to unauthorized access or modifications. As a general best practice, test and development servers and mainframes will be separate from production servers and mainframes whenever feasible to limit Systems/Applications Developer (S/AD) access to other areas of the server. All servers and mainframes will undergo a certification and accreditation process prior to being employed in a production environment.

The functional equivalence of C2 is established by setting operating system parameters to vendor established C2 values. This policy is intended for the operating system and related software. Any deviations from a C2 configuration should be noted in the server/mainframes configuration control manual with an explanation for the deviation that is signed by the Designated Accrediting Authority (DAA). In the situation where an operating system has not been C2 certified, agencies will use the vendor's "Trusted Facility Manual" or the equivalent document to obtain the correct operating system settings. Each agency will be certify that their Web servers comply with these C2 requirements annually. All other servers and mainframes are to be certified every three (3) years or when a major change occurs.

Security patches, service packs, software upgrades, and updates to the server/mainframe operating system shall be installed within a reasonable time as defined in CS Guidance Regarding Patch Management and System Updates. The timing for installation of the updates should be determined by the nature of the risk that the patch/update corrects and the vendor's record of reliability in releasing stable patches/updates. These packages should not be deployed until tested and a roll back/recovery plan has been established. Agency personnel responsible for implementing and maintaining C2 and CC will be trained annually on these requirements.

c The term Sensitive Information as defined in the Computer Security Act of 1987, Public Law 100-235, January 8, 1988, Section 20, sub section (d), sub paragraph (4) is, "Sensitive Information means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), 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 national defense or foreign policy." In NIST handbook 800-12, Sensitive Information is defined utilizing the same definition found in the Computer Security Act of 1987.

Each agency must determine the sensitivity of the information entrusted to them. Information is considered sensitive if one of more of the following conditions are met:

(1) Causes the Agency embarrassment or loss of credibility;

(2) Makes the Agency or its employees subject to a suit or any legal action;

(3) Adversely affects the reliability of the Agency's product; or

(4) Adversely affects the Agency's work capability.

d Protective mechanisms that must be evaluated for sensitive systems are:

(1) Confidentiality – A requirement that private or sensitive information not be disclosed to unauthorized individuals.

(2) Integrity – Assuring that Information is timely, accurate, complete, and consistent. The information must be protected from errors or unauthorized modification.

(3) Availability – A requirement that measures a systems ability to meet user service needs. It is intended to provide assurance to users that one can access a system when needed.

Agencies need to have mechanisms in place to ensure that these requirements are met.

e Agencies will assess the business and resource implications of securing their servers/mainframes with sensitive information. If information is to be shared with another agency or activity, the information "source" agency will designate the sensitivity and how the data must be handled in terms of sharing and need-to-know. A plan that establishes timeframes and deadlines for securing servers and mainframes with sensitive information will be provided to CS within 90 days from the issuance of this policy. Servers and mainframes that cannot be secured will require a waiver.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Establish security standards for USDA servers and mainframes that handle sensitive data or information;

(2) Review agency business and resource impact plan submissions and implementation schedules and collaborate with agencies, as required, to determine the most cost effective and efficient method to provide short and long term security protection;

(3) Review agency/mission area waiver packages and provide a timely response to the all exception requests;

(4) Conduct periodic evaluations to ensure agency compliance with this policy;

(5) Maintain a database of all C2 Compliant and approved Non-Compliant servers and mainframes; and

(6) Update this policy when the Common Criteria (CC) settings become readily available.

b <u>Agency Chief Information Officers will:</u>

(1) Ensure that the five requirements of USDA's C2 Level of Trust are implemented and maintained for all agency servers and mainframes that store, process or house critical or sensitive information;

(2) Assure that all agency IT personnel involved in implementing or maintaining C2/CC standards have the appropriate personnel security minimum background investigation/clearances and separation of duties is invoked (separate tasks by roles);

(3) Ensure agency Server Administrators (SA), staff offices responsible for server administration and Information Systems Security Program Managers (ISSPM) are trained to implement and maintain servers and mainframes at a functional C2/CC level and fully understand the ongoing responsibilities to preserve that level of server security (C2/CC training will be approved by CS);

(4) Ensure that each SA maintains an electronic file of all servers and mainframes hardened to USDA's C2 level of Trust by server designation, physical location of the server, and their settings;

(5) Ensure that servers and mainframes processing Non-trivial agency information have some level of security protection;

(6) Assure that System/Application Developers (S/AD) are aware of their responsibility to include USDA's C2 Level of Trust security for all new systems/applications which process, store or transmit sensitive information;

(7) Assess the implications of securing agency servers and mainframes and develop an agency plan to achieve compliance with this policy to include timeframes <u>within 90 days</u>. The plan will include a written certification that the intent of this policy has been met by the agency, explain any deviations and document alternate approaches. The certification for Web servers will be updated annually; the certification for all other servers and mainframes will be updated every 3 years or when a major change occurs;

(8) Prepare a detailed waiver package for those servers and mainframes not in compliance with this policy <u>within 90 days</u> from issuance of this directive;

(9) In compliance with OMB Circular A-130 assure that all system "owners" determine the protection requirements for each agency owned system. Further, they must <u>assign in writing</u> the responsibility for security to an individual trained in the technology used in the system including the <u>management of security controls</u>;

c <u>Agency Information Systems Security Program Managers (ISSPM) or designate will:</u>

(1) Coordinate the implementation of USDA's C2 Level of Trust with System Administrators (SA) and System/Application Developers (S/AD) for all agency servers and mainframes processing sensitive or mission critical data;

(2) Maintain an electronic file containing Server Designation, physical location, current security settings, server configuration, active services, applications, and all non-compliant server information (Note: this can be a copy of the SA files);

(3) In coordination with the SA, ensure that all system/application patches, service paks, software upgrades and updates are performed within a reasonable time after release and that a written

record is maintained by the SA when these updates are performed;

(4) In coordination with the S/AD and owner, ensure that all new systems or applications developed include the appropriate level of security protection level based on sensitivity of data/probable risk and that the systems/applications are tested and certified prior to being placed into production;

(5) Ensure that SAs provide an adequate level of security protection for servers and mainframes, which process agency unclassified information;

(6) Participate in the development of a plan to assess the business and resource implications of securing servers and mainframes, as required;

(7) In coordination with the SA and the IT Staff assist in the preparation of waiver packages for all non-compliant servers and mainframes;

(8) Conduct periodic reviews of servers and mainframes to ensure that USDA's C2 Level of Trust is maintained and implemented on new and existing servers and mainframes;

(9) In conjunction with the SA, perform audits of servers and mainframes containing sensitive information every 30 days or more frequently depending on system transaction volume; and

(10) Review the system audit results for unusual behavior patterns or other security violations, security performance problems or system flaws and take remedial action to correct these issues.

d <u>Agency System Administrators, System/Application Developers, IT Staff responsible for administration of systems will:</u>

(1) In coordination with the ISSPM, <u>harden</u> all servers and mainframes that manage, retain or transmit sensitive

information in accordance with USDA's C2 Level of Trust;

(2) Prepare/update an electronic file of information on C2 servers and mainframes to include: Server designation, physical location, current security settings, server configuration, active services, applications, and non-compliant server information;

(3) Install system patches, service paks, software upgrades and updates with a reasonable amount of time after release (this depends on the vendor's record of releasing stable patches);

(4) Maintain an electronic record of all patches, service paks, software upgrades and updates installed to include: System/application name, date of patch, service pak, software upgrade or update, version installed, SA name and signature;

(5) In coordination with the Business Owner and ISSPM, install the appropriate security protection for all agency classified and unclassified information;

(6) Participate, as required, in the development of an agency plan to address business and resource impact of C2 hardening;

(7) Prepare, if required, a detailed waiver package for all non-compliant servers and mainframes;

(8) Maintain an electronic log of any security changes made to C2 servers and mainframes by other individuals to include type of change, date and individual authorizing change; and

(9) In conjunction with the ISSPM, perform audits of servers and mainframes containing sensitive information every 30 days or more frequently depending on system transaction volume and assist with any remedial actions required to ensure the system remains C2 compliant.

- END -