Chapter 11, Part 1
CERTIFICATION AND ACCREDITATION METHODOLOGY

1 BACKGROUND

OMB Circular A-130, Appendix III and the Federal Information Security Management Act (FISMA) requires that all federal agencies institute an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency. This includes those systems provided or managed by another agency, contractor, or other source. All USDA agencies shall institute a comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting a specified set of security requirements for the system. These actions are referred to as *system certifications*. Certification supports the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. This decision is referred to as *system accreditation*.

All USDA IT systems require certification and accreditation prior to the system becoming operational. The Designated Accrediting Authority (DAA) makes formal accreditation determinations. This action supports the regulatory requirement that every USDA system must have official approval to operate.

2 POLICY

All USDA agencies and staff offices will formally certify and accredit all federal information systems in accordance with this policy and the USDA Certification and Accreditation Guide. This guide applies to all information and information systems owned, leased, operated or connected to the Department of Agriculture. Agency/system owners are responsible for ensuring that all contractors comply with the C&A requirements defined by this policy for systems they operate in support of USDA's mission. Agency CIOs act as both the entity responsible for the overall C&A process and as the Certifying Official (CO). Accordingly, agency CIOs will ensure that the

Designated Accrediting Authorities (DAA) understands the C&A process, including system risk factors, and accepts accreditation responsibilities. Further the agency CIO will ensure that the DAA does not delegate the security accreditation decision or signature authority to subordinate levels. The agency DAA will ensure that the final review and signatory authority of the CO is not delegated to subordinate levels. Other certifications tasks may be delegated at the CO's discretion.

Certified systems will undergo an independent concurrence review by the ACIO-CS prior to submission to the DAA. Concurrence reviews will be completed by the ACIO-CS within 30 days of receipt and the results will be reported to the CO in writing. All system reviews that result in significant deficiencies will be returned to the CO for corrective action and/or adjustment necessitating that the system be placed under an Interim Authority to Operate (IATO) until the deficiencies are resolved. In addition, agencies and staff offices will electronically track significant deficiencies resulting from the concurrence review. All USDA IT systems will be certified and accredited every 3 years, unless the system undergoes significant change. Significant Change is defined in the USDA C&A Guide. Systems accreditation that occurred prior to the C&A Policy release will be grandfathered under the previous accreditation guidance until its 3 -year anniversary or it undergoes significant change. Agencies will begin the C&A process for re-accreditation in a in a timely fashion to ensure that the process is completed before the system anniversary date of the last accreditation. Agencies are reminded that the Department CIO has the right to terminate operation of systems that do not undergo proper certification and accreditation or that do not meet department security requirements.

Interim Authority To Operate (IATO) Requirements – There are no exceptions to the requirements to certify and accredit all USDA systems. However, if after assessing the results of the security certification of the IT system, the CO recommends (with ACIO-CS concurrence) to the DAA and/or the DAA deems that the risk to the agency operations, assets, or resources is unacceptable, but there is an overarching mission necessity to place the IT system into operation or continue its operation, an IATO may be issued. An interim authorization provides a limited authorization to operate the IT system under specific terms and conditions and acknowledges great risk to the agency for a 6-month period. An IATO is rendered when the identified security vulnerabilities in the IT system, resulting

from deficiencies in the planned or implemented security controls, are significant but can be addressed within a 6-month time frame. IATOs can be granted by the DAA for a maximum period of 6 months. Agencies will track and report deficiencies through the Plan of Action and Milestones (POA&M) process. An extension of this period requires the approval of the Department Chief Information Officer (CIO) and will only be considered for compelling reasons. Agencies will forward approved copies of systems IATOs to the CS Certification and Accreditation Program Manager (PM) and those will be monitored and tracked to ensure that systems are progressing through the certification and accreditation process.

All deficiencies, whether significant or reportable, must be entered and tracked using the approved database system. Significant Deficiencies tracked in the POA&M database must be resolved within 60 days. Reportable Conditions must be resolved within 180 days. Agencies must present Cyber Security with verification documentation, and receive concurrence, before a deficiency can be considered resolved.

3 PROCEDURES

Each USDA agency should complete the C&A phases for certifying and accrediting their systems. These phases consist of:

a Phase I : Pre-certification
- Define Scope of C&A
- Identify Security Controls
- Conduct Privacy Impact Assessment (PIA)
- Review System Security Plan
- Review Initial Risk Assessment
- Review approved Interconnection Security Agreements
- Negotiate with participants

b Phase II : Certification and Accreditation
- Conduct ST&E
- Update the Risk Assessment
- Update the System Security Plan
- Identify and Report any Residual Risk
- Document Certification Findings/Recommendation
- Obtain ACIO-CS concurrence on the certification package
- Accreditation Decision

c Phase III : Post-accreditation

(Repeat Steps Above every 3 years or when significant system change occurs)

NIST, 800-37 permits the use of a modified version of the C&A process for systems categorized by the agency as low risk/ low impact. In order to qualify as Low Risk/Low Impact, a system must be rated as low risk/low impact in all three of the assessment categories of confidentiality, integrity and availability. These low risk/impact systems are only required to complete Phase 1, Pre-certification, which includes the security plan, risk assessment and NIST 800-26, NIST Security Self-Assessment Guide for Information Technology Systems.

Please note:
The NIST 800-26 Self Assessment Checklist or equivalent is not an acceptable substitute for a Risk Assessment. These checklists may be used as reference material to a Risk Assessment, but do not contain sufficient discussion and analysis of a system's characterization, mitigation or residual risk.

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Develop and publish policy guidance to assist agencies and staff offices in the certification and accreditation (C&A) of IT systems;

(2) Make available, if feasible, a departmental contract to provide certification and accreditation services to agencies and staff offices;

(3) Provide training on C&A to agencies and staff offices, as required;

(4) The departmental CIO has formally delegated Certifying Official (CO) authority to the agency CIOs. However, certification packages will be submitted to the ACIO-CS for an in-depth concurrence review prior to submission to the DAA

(5) Track the status of IT systems and the associated C&A actions and any approved IATOs to ensure that systems are certified and accredited within 6 months.

b Agency Chief Information Officer will:

General Process Duties

(1) Implement and manage the certification and accreditation of all agency IT systems in accordance with this policy; ensures that systems with significant deficiencies are placed under an IATO in accordance with the requirements outlined above and that they are certified and accredited in a timely manner within the six month IATO period;

(2) Ensure that a Designated Accrediting Authority (s) is appointed in writing for each agency IT system and that they fully accept the responsibility for system risk and operation;

(3) Ensure that the DAA designates an independent individual to act as the Agency CO for IT systems; ensure that the CO does not delegate final review and signature authority to subordinate individuals;

(4) Disseminate this policy to all IT professionals, security officers and business owners who will be involved in the C&A process to ensure they understand and can fulfill the roles and responsibilities in this procedure;

(5) Support and facilitate the work the Certification Teams to ensure that agency IT systems are certified and accredited; approve ST&E teams, and ensure that final C&A packages are accurate and complete;

(6) Take necessary actions to ensure that system risks are mitigated by appropriate security controls and security issues are resolved;

(7) Monitor the C&A progress of systems and provide status to Cyber Security, including those under an IATO;

(8) Ensure that all system changes are examined to determine if re-certification and re-accreditation of the system must be performed; institute appropriate C&A action as a result of this examination;

(9) Ensure that all agency IT systems are routinely certified and accredited every 3 years or when significant changes occurs in the system; and

(10) Ensure that systems that have significant deficiencies uncovered as a result of audits, concurrence reviews, IV&Vs or other authorized processes are placed under an IATO until these findings are resolved and that all corrective actions are tracked and reported to CS through the Plan of Action & Milestones (POAM) process.

Certifying Officials Duties

(1) Act as the certification agent responsible for the comprehensive evaluation of the management, operational and technical security controls within an IT system;

(2) Manage and coordinate the functions of the Certification Team;

(3) Perform the final review of the certification package, prior to mandatory ACIO-CS concurrence, and ensures the signed package is timely and accurate (final review and signature authority will not be delegated to subordinate levels);

(4) Provides recommended corrective actions to reduce or eliminate vulnerabilities in IT systems and assesses system security plans for completeness and consistency; and

(5) Makes recommendations to the DAA (Authorizing Official) for accreditation of an IT system, after obtaining concurrence of ACIO-CS.

c The agency Designated Accrediting Authority (DAA) will:

(1) Act as the Authorizing Official with the authority to approve or the operation of an IT system at an acceptable level of risk;

(2) Authorize a system to operate as accredited or under an IATO only with the concurrence of the ACIO-CS.

(3) Issue an Interim Authority to Operate (IATO), where appropriate, for an IT system based on the level of risk involved in system operation or for systems that have major deficiencies resulting from and IV&V;

(4) Deny authorization for an IT system's operation or halt a system's operation if unacceptable security risk; and

(5) Formally designate independent individuals responsibility for C&A activities in writing; the DAA shall not delegate the security accreditation decision and the signing of the associated Accreditation Decision Letter.

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

(1) Assist in the certification and accreditation of all agency IT systems;

(2) Participate in Certification Teams providing guidance, testing security controls and assisting in the preparation of the final C&A package, as required;

(3) Monitor and electronically track using Plans of Action and Milestones (POAM) the C&A progress on IT systems and report progress to agency CIO, including all systems under IATO to ensure that deficiencies are corrected in a timely manner;

(4) In conjunction with the agency Configuration Control Board (CCB), identify system changes that require re-accreditation; and

(5) Participate in the preparation of IATO packages, as required.

-END –

Appendix A

United States Department of Agriculture (USDA) Certification and Accreditation Guide

Document Configuration Control

Version	Release Date	Summary of Changes
Version 1.0	April 2003	Initial Strawman
Version 1.1	June 2003	Revised Draft
Version 1.2	June 2003	Second Revised Draft
Version 2.0	November 2003	Third Revised Draft
Version 3.0 Version 4	December 2003 March 2005	Fourth Revised Draft Fifth Revision

Table of Contents

1. INTRODUCTION

1.1. Purpose

This Certification and Accreditation Guide is intended to provide a comprehensive and uniform approach to the certification and accreditation (C&A) process. Individuals responsible for, or involved in the C&A process, will use this guide as a resource to assist them in certifying and accrediting the United States Department of Agriculture (USDA) general support systems and major applications.

A primary purpose of this guide is to support the Office of Management and Budget (OMB) Circular A-130, Appendix III requirement for agencies to "ensure that a management official authorizes in writing the use of each system/application…before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years." Agencies are also reminded that the Department CIO has the right to terminate operation of a system that does not undergo proper certification and accreditation.

Ideally, the C&A process should be integrated into the system development life cycle (SDLC) during the capital planning and investment control (CPIC) process. During development, the system security plan (SSP) should be written and the initial risk assessment completed in order to provide an assessment of the possible risks to the system. Additionally, the security-related documents listed in Appendix D of this Guide should be completed during this process.

However, many USDA legacy systems already in place have not gone through the C&A process as part of the SDLC. The requirement for system approval applies to these systems as well. If systems have not obtained official approval to operate prior to deployment, they must complete the C&A process and obtain approval to operate. New regulations state that every USDA system and application must have official approval to operate. This approval can consist of an unconditional approval (which is good for three years or until a significant change occurs). The approval can also be an Interim Authority to Operate (IATO), which is only valid for up to 6 months. An extension of this period requires the approval of the Department Chief Information Officer (CIO) and will only be considered for compelling reasons. An IATO can be granted if risks have been identified and a mitigation plan with a specific timetable for addressing those risks has been approved.

1.2 Interim Authority to Operate (IATO) Requirements

The CO may make a recommendation, with the ACIO-CS' concurrence, to the DAA to obtain an IATO if a mission critical system has an unacceptable level of risk to agency assets based on the security certification. An IATO may also be deemed necessary by the DAA if there is an overarching mission need to place a new system into operation or continue processing in an existing system. An IATO is rendered when the identified security vulnerabilities in the IT system, resulting from deficiencies in the planned or implemented security controls, are significant but can be addressed within a 6-month timeframe. An extension of this period requires the approval of the Department Chief Information Officer (CIO) and will only be considered for compelling reasons. Agencies will forward IATO Request Submissions to the ACIO-CS and those will be monitored and tracked to ensure that systems are progressing

through the certification and accreditation process. Phase 1 of the C&A Activities must be completed in order for an IATO to be approved. The IATO Request Submission is a structured approach to monitor the effectiveness of the security controls in the IT **system** during the 6-month period. Consequently, the IATO Request Submission submitted by the IT **system** owner is used by the authorizing official and CS to monitor the progress in correcting deficiencies noted during the security certification. Agencies must forward to the C&A PM a copy of the DAA letter, indicating that the specified IT system has been granted an IATO. A template of the DAA IATO letter is in Appendix F along with a template for the IATO Submission.

All deficiencies, whether significant or reportable, must be entered and tracked using the approved database system. Significant Deficiencies tracked in the POA&M database must be resolved within 60 days. Reportable Conditions must be resolved within 180 days. Agencies must present Cyber Security with verification documentation, and receive concurrence, before a deficiency can be considered resolved.

Finally, agencies should be reminded that, in accordance with OMB policy, an IT **system** is not accredited during the period of limited authorization to operate. When the security-related deficiencies have been adequately addressed, the interim authorization should be lifted and the IT **system** accredited to operate.

1.3 General Support Systems and Applications

As stated above, all systems and applications are required to be certified and accredited. The differences between General Support Systems (GSS) and Applications that are germane to the certification and accreditation of such systems focus on the extent of activities performed for each. An application "performs a clearly defined function for which there are readily identifiable security considerations and needs"[1] whereas a GSS "provides standard information security capabilities, such as boundary defense, incident detection and response, and key management, and also delivers common applications, such as office automation and electronic mail"[1]. The scope of the certification will vary depending on the type and extent of the systems. For example, a GSS, such as the USDA Wide Area Network (WAN), will require extensive testing to ensure that all system components are evaluated against the baseline security requirements. Applications that reside on a GSS that has already been certified and accredited may refer to portions of the GSS risk assessment and Security Testing & Evaluation (ST&E) activities (such as testing and document evaluation) on certain components used by those applications rather than repeating ST&E and risk assessment activities on those components.

1.4 Background

The Federal Information Security Management Act[2] (FISMA) is the most recent legal requirement mandating that Federal agencies develop a comprehensive IT security program. Laws such as FISMA, as well as requirements in OMB Circular A-130, mandate that security must be developed at both the programmatic and system levels.

---

1 NIST Special Publication 800-37

2 Public Law 107-307

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 provides guidelines for security certification and accreditation of information technology (IT) systems, as does the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP). IT systems can only be allowed to operate if they do not compromise legal or regulatory security requirements**.**

1.5 Scope

The scope of this guide includes identifying roles and responsibilities of key players, defining the C&A process, and describing the three phases that comprise the C&A process. The guide is based on OMB Circular A-130, dated November 2000, NSTISSI No. 1000, NIACAP, dated April 2000, Federal Information Processing Standards (FIPS) Publication (PUB) 102, dated September 1983, NIST SP 800-37, May 2004**,** and other applicable Department and Federal IT security laws and regulations.

1.6 Outcome

The C&A methodology outlined in this guide will provide USDA system owners and program managers with uniform guidance on how to certify and accredit their IT systems. Proper use of the C&A methodology will assure the Department that the level of security implemented and controls in place adequately protect assets given an acceptable level of residual risk. The Department will benefit from the C&A activities performed on IT systems in the following ways:

- Formal approval to operate
- Standard operating environment through utilization of baseline security requirements
- Clearly defined system boundaries
- Privacy implications reviewed (Privacy Impact Assessment/System of Records Notice)
- Documented security plans
- Defined and tested contingency plans
- Established configuration management processes
- Heightened information security awareness
- Validated security controls
- Measured levels of risk based on identified threats and vulnerabilities
- Defined security roles and responsibilities

1.7 Structure

This guide is organized into four major sections. Section 1 introduces the Department's C&A Guide. Section 2 provides an overview of the roles and responsibilities of the key parties involved in the C&A process.

Section 3 describes the C&A process, which consists of three phases comprising 12 major steps. A checklist has been included at the end of each phase. These checklists are reminders of all the actions that occur during that specific phase of the C&A process. They are designed to provide a quick reference for all participants in the process.

Section 4 contains a summary of the C&A methodology described in this Guide. Table A-1 provides a glossary of terms used in the document. Table A-2 contains a list of acronyms. Table A-3 provides a list of document references used to develop this C&A methodology. Table A-4 provides a list of required system documentation that must be maintained for each system as part of the system's certification and accreditation. Table A-5 provides a list of the USDA software application and operating system checklists that have been developed for use in the C&A process. Table A-6 provides templates for conditional and unconditional Security Evaluation Reports (SER), respectively. Table A-7 contains the evaluation criteria for various C&A documents. This table exists as a separate guide to facilitate the usefulness of the checklists since they must be completed for all systems undergoing certification and accreditation. Table A-8 contains Security Accreditation Decision Letter (Samples). Table A-9 is the form to use when submitting a request for an Interim Authority to Operate (IATO).

2 ROLES AND RESPONSIBILITIES

The following sections describe the various personnel involved in the USDA C&A process and their particular responsibilities.

2.1 Designated Accrediting Authority

The Designated Accrediting Authority (DAA) is a USDA program area executive with the authority to evaluate the mission, business case, and budgetary needs for the system in view of the security risks present in the system's operating environment. The DAA is a senior level official or executive who has the authority to formally approve the operation of an IT system at an acceptable level of risk within its environment. The DAA is the business owner of the general support system or major application being certified. By accrediting a system, the DAA assumes responsibility for the residual risks of operation of the system in a stated environment. The DAA approves security requirements documents, memoranda of agreement (MOA), memoranda of understanding (MOU), and any deviations from security policies.

If the DAA is presented with a system with unacceptable risks, but a plan for remediation, he or she may issue an Interim Authority to Operate (IATO), which will allow the system to remain in operation for 6 months. During that time, the mitigation strategies for reducing the unacceptable risks should be implemented. A regression ST&E should also be completed to ensure that the unacceptable risks are mitigated. **IATOs are only good for six months; an extension of this period requires the approval of the Department Chief Information Officer (CIO).**

In addition to having the authority to accredit systems for operation, the DAA has the authority to deny approval for systems to operate and, if the systems are already operational, the authority to halt operations if unacceptable security risks are found to exist. The right to reject residual risk present for any general support system or major application remains the right of the DAA if they are not comfortable with the level of risk presented.

In some situations where IT systems interconnect, certification and accreditation activities may involve multiple DAAs. If so, agreements detailing which security controls are expected to be on which systems must be established among the responsible DAAs and documented in the accreditation package. In these cases, it may be advantageous to agree to a lead DAA to represent the other DAAs during the C&A process. NIST SP 800-47 provides guidance on how to coordinate security for interconnecting systems. Additionally, the DAAs shall sign system Interconnection Security Agreement (s).

In the event of inter-agency or inter-department connections, the DAAs should draft and sign MOAs or MOUs that provide details on which agency or department is responsible for what areas of security.

2.2 Certifying Official (CO)

The USDA Chief Information Officer (CIO) is the Department's Certifying Official (CO). The CIO has delegated the authority to certify agency systems to each agency CIO. Thus, the CO for each agency will be the agency CIO unless a conflict of interest exits. If the agency CIO is also the DAA, the agency Administrator or Head will serve as the DAA or will appoint another senior

executive level manager to act in this capacity who is not in the CIO's chain of command. The CO will be the point of contact for the agency with regards to certification activities. The mission of the CO is to evaluate the certification package from a technical perspective, obtain the mandatory concurrence from the ACIO-CS and present a recommendation to the DAA in regards to the accreditation of the system. At the conclusion of the C&A process, the certification team will present the certification package to the CO, who will evaluate the risk to the system. At that point, the CO will make the final decision about whether or not to request concurrence from the ACIO-CS and, if concurrence is reached, recommend the DAA accredit the system and will prepare the accreditation package to present to the DAA.

2.3 Certification Team

The certification team consists of the technical personnel from the business unit responsible for conducting the certification activities. The certification team is responsible for identifying, assessing, and documenting the risks associated with operating the system, coordinating C&A activities, and consolidating the final C&A package. The team will assess the vulnerabilities in the system, determine if the security controls are correctly implemented and effective, and identify the level of residual risk of the system.

2.4 Security Test and Evaluation Team

The security test and evaluation (ST&E) team consists of personnel independent of the IT infrastructure and business function and is responsible for performing the ST&E on the system to validate the results of the risk assessment and that the controls in the System Security Plan (SSP) are present and operating correctly on the system. The ST&E team should be independent in the sense that they should not have a) been involved in the development of the system and b) been involved in the other certification activities, such as writing the SSP and conducting the risk assessment.

In order to ensure independence, the ST&E team must be approved by the CO prior to the commencement of the C&A process.

The purpose of the ST&E is to ensure that the risk determinations made during the risk assessment are accurate and provide a thorough portrayal of the risks to the system and its data. The results of the ST&E, together with the rest of the certification package, will be presented to the CO so that the CO may make an accurate determination of the risk to the system, obtain concurrence from the ACIO-CS and thus provide an informed accreditation recommendation to the DAA.

2.5 Program Manager and System Owner

The Program Manager and System Owner represent the interests of the user community and the IT system throughout the system's life cycle. The program manager is responsible for the system during initial development and acquisition, and is concerned with cost, schedule, and performance issues. The system owner assumes responsibility for the system after delivery and installation, and is responsible for system operation, system maintenance, and disposal. Together they are responsible for ensuring the system is deployed and operated according to the security controls documented in the security plan and are also responsible for seeing that system users and security support personnel receive the requisite security training.

The program manager and system owner will coordinate the C&A effort and provide the necessary staff and information to the certification team. They will review the certification package before it is presented to the CO.

2.6 Information Systems Security Officer

For operational systems, the Information Systems Security Officer (ISSO) is responsible for the day-to-day security of a specific IT system including physical security, personnel security, incident handling, and security awareness, training, and education. The ISSO, in conjunction with the configuration control board (CCB) also identifies pending system or environment changes that may necessitate re-certification and re-accreditation of the system. For developmental systems, the ISSO serves as the principal technical advisor to the program manager for all security-related issues.

2.7 Other Supporting Roles and Role Delegation

There are other individuals within USDA such as user representatives, security program managers, operations managers, and facilities managers that may also have concerns or interests in the C&A process. User representatives typically represent the operational interests of the user community and serve as the liaison for that community throughout the life cycle of the system. User representatives may assist in the C&A process to ensure mission requirements are satisfied while meeting the security controls defined in the security plan. Security program managers ensure a standard C&A process is used throughout the agency, provide internal C&A guidance or policy, and, if appropriate, review certification packages prior to DAA review. Operations managers oversee the security operations and administration of IT systems. Facilities managers oversee changes and additions to facilities housing IT systems and ensure that changes in facility design or construction do not adversely affect the security of existing systems.

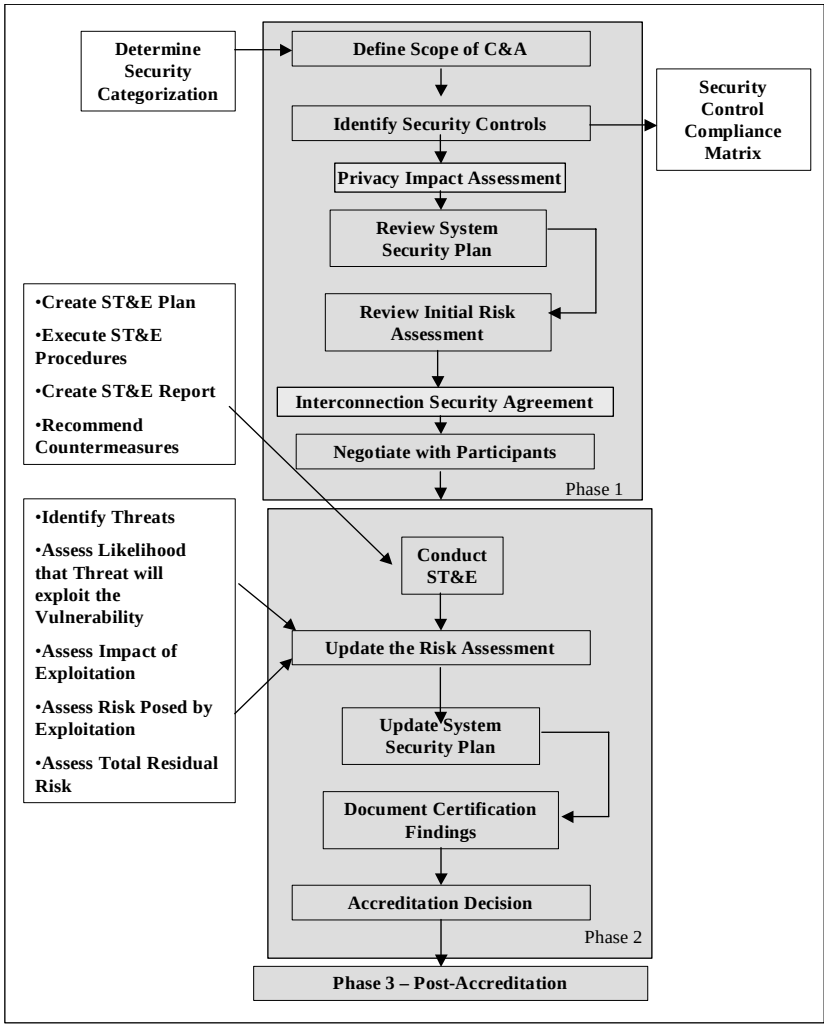
2.8 Associate Chief Information Officer for Cyber Security (ACIO-CS)

Prior to formal submission of the certification package to the DAA, the CO will submit the package and all supporting documentation to the ACIO-CS for a mandatory Independent Verification and Validation (IV&V). The ACIO-CS will perform an in-depth IV&V of the certification package and will either concur with the recommendation to accredit, recommend/concur with the need (and requisite mitigation plan) to issue an IATO or make the determination that the certification package is insufficient for accreditation or an IATO. The concurrence of the ACIO-CS is mandatory prior to submission to the DAA.

3 The C&A Process

The C&A process is comprised of three phases: the pre-certification phase; the certification and accreditation phase, and the post-accreditation phase. Phase 1, the pre-certification phase, has various steps that include: defining the scope of the C&A effort, identifying existing security controls**,** reviewing any approved Interconnection Security Agreements (ISA), conducting Privacy Impact Assessment (PIA), reviewing the SSP, reviewing the initial risk assessment, and negotiating with the participants. Phase 2, the certification and accreditation phase, consists of additional steps: conducting the ST&E, updating the risk assessment with findings from the ST&E, updating the SSP, documenting certification findings; and forwarding the certification findings to the DAA for an accreditation decision. Phase 3, the post-accreditation phase, consists of managing the configuration of the system and re-accreditation. The various phases and steps are depicted in Figure 3-1 and are described more fully in the following sections.

Figure 3-1
The C&A Process (High & Medium Systems)



Note: Low impact systems perform only Phase 1 and complete NIST 800-26 Self Assessment.

3.1 Phase 1: Pre-Certification

Phase 1 involves gathering information about the system to be certified, determining the scope of the certification effort, validating the initial System Security Plan (SSP) for the system, performing the initial validation of the risk assessment and system security controls, and determining the C&A schedule. During phase 1, the system owner or program manager will coordinate with all stakeholders in the C&A process to ensure that the certification schedule is set.

3.1.1 Step 1: Define the System and Scope of the C&A Effort (High, Medium, Low Systems)

During this phase, the certification team should gather all available system information (e.g., design documents, system descriptions, graphics, system plans, approved Interconnection Security Agreement, Privacy Impact Assessment, etc.) in order to get a comprehensive system description and to define the scope of the certification and accreditation effort. Defining the system involves cataloging the different types of software, hardware, and communications equipment comprising the system in order to understand what needs to be examined for the C&A effort.

During Phase 1, the C&A key participants - the DAA, the CO, the program manager, the system owner, the certification team, the ISSO, and other officials in the agency or department that have an interest in the system - should agree on the scope and schedule for C&A activities. It is recommended that the ACIO-CS be involved at this point to assure that the scope and schedule is adequate. The participants should also evaluate the system and determine the appropriate security categorization for the system in writing. The security categorization is determined by the levels of concern for confidentiality, integrity, and availability of data, and defines what activities will take place during the ST&E phase of the C&A effort. In addition, the certification team should inform the CO about who will be performing the ST&E. The CO must approve of the ST&E team and ensure they are fully independent from the IT infrastructure and the business function prior to the commencement of the rest of the C&A process.

3.1.1.1 Determine the Security Categorization (High, Medium, Low Systems)

In order to determine the appropriate security categorization for the system or application, the levels of concern must first be identified for confidentiality, integrity, and availability. FIPS PUB 199 provides guidance for assigning security categorization factors for information processed on federal systems. Each factor is assigned a level of low, moderate, or high. Confidentiality provides assurance that the system data is protected from disclosure to unauthorized personnel, processes, or devices. Integrity provides assurance that the data processed by the system is protected from unauthorized, unanticipated, or unintentional modification or destruction. Availability provides assurance that the system data and resources will be available to authorized users on a timely and reliable basis.

The format for documenting the security categorization is as follows:

CATEGORIZATION = [(confidentiality, RISK-LEVEL), (integrity, RISK-LEVEL), (availability, RISK-LEVEL)]

If the level is Low, Low, Low, agencies can certify and accredit the system using a modified process that requires only Phase 1 activities and the completion of NIST-800-26 prior to the formal accreditation of the system. However, if the score contains one rating of medium or high, the system must be rated as medium or high impact and proceed through the complete process described in Section 3.

Table 3-1 below provides guidance on how to determine which level of concern should be assigned to each factor.

Table 3-1
Levels of Concern for Confidentiality, Integrity, and Availability

	Level of Risk		
	LOW	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C §3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective repairs.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of confidentiality could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.
Integrity Guarding against improper information modification, destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C. §3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The unauthorized modification or destruction of information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of integrity could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

	Level of Risk		
	LOW	**MODERATE**	**HIGH**
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C. §3542]	The disruption of access to information could be expected to have a limited adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause a negative outcome or result in limited damage to operations or assets, requiring minor corrective repairs.	The disruption of access to information could be expected to have a **serious** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause significant degradation in mission capability, place the agency at a significant disadvantage, or result in major damage to assets, requiring extensive corrective actions or repairs.	The disruption of access to information could be expected to have a **severe** or **catastrophic** adverse effect on agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A loss of availability could be expected to cause a loss of mission capability for a period that poses a threat to human life, or results in a loss of major assets.

*Adapted from FIPS PUB 199, "Security Categorization of Federal Information and Information Systems", Table 1

3.1.2 Step 2: Identify Security Controls and Construct a Compliance Matrix (High, Medium & Low Systems)

During this step, the team should identify all security controls that should be present on the system including those specified in the SSP, review system privacy implications to include preparation of a Privacy Impact Analysis (PIA) and Systems of Records (SOR) Notice (if required), and additional requirements needed to secure the system at the proper security categorization. The controls should be compiled from USDA Cyber Security Manual 3500, other federal guidance, including OMB A-130, NIST 800-53, FISMA, and industry best practices.

The security controls should include management, operational, and technical controls for the system, as it will be operated, as well as environmental controls and physical security controls. Once the security controls are identified, a Security Controls Compliance Matrix (SCCM) shall be constructed. This matrix should list each security control, the reference from which the security control was derived, and whether or not the control has been implemented. The SCCM shall be completed during ST&E and submitted as part of the certification package. Table 3-2 provides an example of an SCCM entry.

Table 3-2
Sample Security Controls Compliance Matrix

	Security Control	Compliance			Comments
		Yes	No	Other	
Assignment of Responsibilities					
1.	Responsibility for security has been assigned in writing to an individual trained in the technology used in the system and in providing security for such technology (OMB Circular A-130 Appendix III, Section A-3)				

3.1.3 Step 3: Conduct a Privacy Impact Assessment (PIA) and if required complete a System of Records Notice (SOR) (High, Medium, Low Systems)

During this step, agencies should determine the impact the system data has on individual privacy. Therefore, each agency shall complete the Privacy Impact Assessment detailed in Chapter 3, Part 2 of the Cyber Security Manual. This measure ensures that agencies have thoroughly examined the privacy implications of system data collection. In addition, The Privacy Act requires agencies to publish a System of Records (SOR) Notice subject to 5 U.S.C. 552(E)(4). Specifically, a "system of records" is defined as a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. DM 3555-001, Chapter 11, Part 1, Certification and Accreditation, Appendix C, contains additional guidance on SOR Notices. in the Appendices. SOR shall be reviewed and updated every two years to ensure they remain current.

3.1.4 Step 4: Review the System Security Plan (High, Medium, Low Systems)

The system security plan should provide a system description, a list of the security requirements for the system, and should explain how the system security controls meet the security requirements. The initial SSP should be created during system development as part of the security requirements definition for the system. SSPs should be updated whenever changes are made to the security posture of the system.

During this step, the existing SSP should be reviewed to ensure that it accurately follows the methodology in the USDA OCIO's Annual Guide to System Security Plans and NIST 800-18, "Guide for Developing Security Plans for Information Technology Systems," and describes the most current system configuration and all the security controls included in the system. The team should also verify that the controls described are appropriate for the security categorization and that the SSP provides information about any user organizations, both internal and external, that connect to the system. If the system does interconnect with other systems or organizations, details about the security controls on those connections shall be documented in an ISA.

Specific review criteria for SSPs are presented in Appendix G, "Base Level Document Evaluation Criteria." There are separate SSP evaluation documents for GSS and **applications.** These criteria will be used by the ST&E team to review the SSP, so it is essential that the SSP fulfill the criteria presented.

3.1.5 Step 5: Review the Initial Risk Assessment (High, Medium, Low Systems)

After the SSP is reviewed, the initial risk assessment should be inspected to ensure that it identifies all apparent threats and vulnerabilities in the IT system and is consistent with the guidance provided in the USDA Risk Assessment Methodology, DM 3540-001, and NIST 800-30, "Risk Management Guide for IT Systems". The risk assessment should also determine the overall level of risk present on the system given the type of data the system processes, the security controls on the system, and the system's operating environment. The initial risk assessment should be performed before the system is fielded to verify that the security requirements specified during development have been met. Risk assessments shall be updated every time there is a change to the security controls on the system that might affect the residual risk to the system.

Please note: The NIST 800-26 Self Assessment Checklist or equivalent is not an acceptable substitute for a Risk Assessment. These checklists may be used as reference material to a Risk Assessment, but do not contain sufficient discussion and analysis of a system's characterization, mitigation or residual risk.

Specific review criteria for risk assessments are presented in Appendix G, "Base Level Document Evaluation Criteria." These criteria will be used by the ST&E team to review the risk assessment report, so it is imperative that the risk assessment fulfills the criteria presented.

3.1.6 Step 6: Review the Interconnection Security Agreement (ISA) (High, Medium, Low Systems)

If this system will be connected to other IT systems, the business owner must discuss the requirements for connectivity with the other system's business owner and work to identify the security requirements for this connection. The ISA is started during the Initiation Phase of the SDLC, is refined during the Acquisition/Development Phase but the ISA may not be completed until the actual system Implementation Phase. An ISA will be done for each system that will be connected to the new system. Additional guidance on preparing the ISA is contained in Chapter 15, Part 1, Security Controls in the System Development Life Cycle (SDLC).

3.1.7 Step 7: Negotiate with Participants (High, Medium, Low Systems)

After steps 1 through 4 are complete, all the participants, including the DAA, the CO, the program manager, the system owner, and certification team should meet to review the extent and scope of the planned C&A effort. The participants should review the confidentiality, integrity, and availability levels determined for the system and should verify that they are accurate and that the security categorization is appropriate for the system. The participants should also review the SCCM to ensure that it accurately reflects the security requirements applicable to the system. At this point, a schedule should be set for the remaining steps in the C&A effort. This step should also occur for Low Impact/Low /Risk systems even though the required actions are less stringent.

The checklist below provides a quick reminder of all activities that should take place during Phase 1 of the C&A process.

Phase 1 Checklist	
	Has the scope of the C&A effort been defined?
	Has the security categorization been determined and documented?
	Have the Security Controls been identified? Has a review of the approved ISA been done? Has a PIA been conducted?
	Has a Security Control Compliance Matrix been constructed?
	Has the System Security Plan been reviewed?
	Has the Risk Assessment been reviewed?
	Have all participants in the C&A process negotiated a schedule for the remaining C&A activities?

Guidance for Low Impact Systems: For low impact systems, the information system owner may employ the services of the Information Systems Security Officer or other designated individuals to prepare the security assessment report containing the results of the NIST 800-26, Self Assessment. The security assessment report, based on NIST 800-26, can be an abbreviated document synopsizing the results and highlighting those areas that need further attention. For low impact systems the accreditation packages consists of: the updated system security plan, an abbreviated NIST 800-26 Security Assessment Report, updated Risk Assessment, Security Categorization Document, and a Plan of Action and Milestones (POA&M). **Note: the POA&M is a new requirement**.

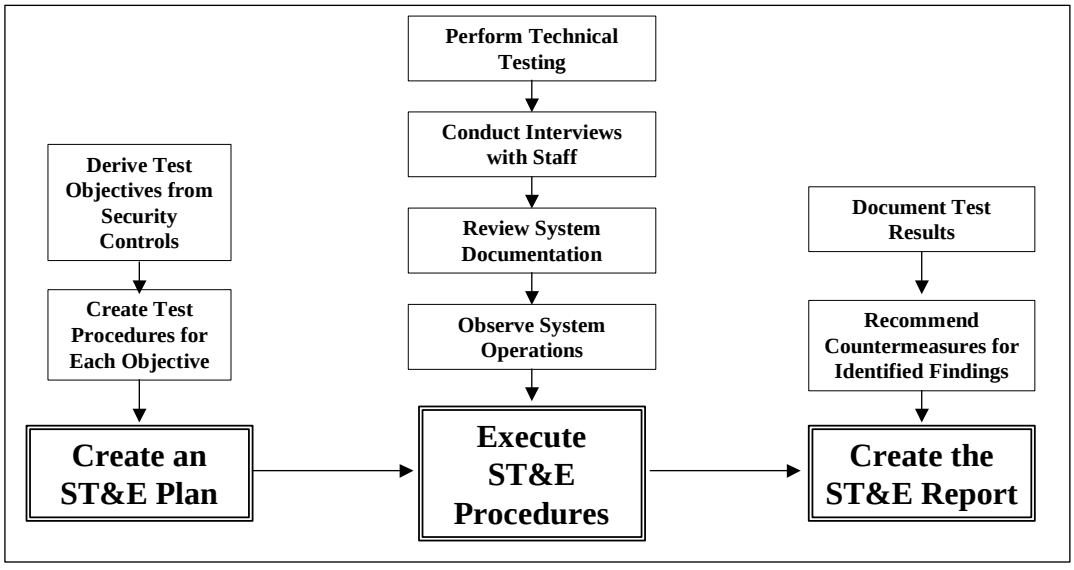
3.2 Phase 2: Certification and Accreditation (High & Medium Systems)

During the certification and accreditation phase, the certification team will conduct ST&E to evaluate the effectiveness of the security controls on the IT system, and then use the results of the ST&E to update the risk assessment and the SSP. The results of this phase will be documented as certification findings and included in the final certification package. The certification package will then be presented to the DAA for a final accreditation decision.

3.2.1 Step 8: Conduct a Security Test and Evaluation (High & Medium Systems)

During this step, the team should evaluate the effectiveness of the security controls through hands-on testing. ST&E consists of three steps: creating the ST&E Plan, executing the test procedures, and documenting the results in the ST&E Report with recommended countermeasures. Figure 3-2 illustrates the three main steps (and the sub-steps) involved in performing an ST&E.

Figure 3-2
Security Test and Evaluation Process



3.2.2 Create the ST&E Plan (High & Medium Systems)

There are two steps involved in writing an ST&E plan. First, test objectives should be derived from the security controls identified in Phase 1, Step 2 and compiled in the SCCM. The test objectives should correspond to the appropriate technical requirements to test the security features of operating systems and software used for the system, administrative, procedural, environmental, physical, and communications security requirements.

Second, detailed procedures shall be written to test each control or requirement. Procedures can consist of hands-on testing for technical requirements, interviews with personnel for administrative requirements, document review for procedural requirements, and observation of facilities for environmental and physical requirements, or a combination of techniques. The extent of the ST&E activities will vary according to the security categorization of the system. Systems that process information at a higher sensitivity or criticality level will need more involved verification activities, such as penetration testing, than systems that process non-sensitive information.

The USDA has created security checklists for many popular operating systems and software packages. These checklists should be used as the base technical test objective set for ST&E plans, where applicable. Table A-5 contains the most recent list of USDA checklists available. These lists can and should be used to develop the test procedures to be executed in the next step.

3.2.3 Execute the Test Plan (High & Medium Systems)

After the ST&E plan has been approved by the C&A officials, the test procedures in the plan shall be executed. An important part of the ST&E is the careful review of security-related documentation, such as the risk assessment, PIA (if required), SSP, Security Features User's Guide (SFUG), the Trusted Facility Manual (TFM), and the Contingency Plan in accordance with DM 3500, CS-032 and CS-033. A successfully tested and executable Contingency Plan is required for the completion of the ST&E. These documents should be reviewed to ensure that they are: 1) developed in accordance with the appropriate USDA and federal guidance; and 2) that they are up-to-date and usable for their intended purpose. A detailed list of security-related documentation that should be reviewed is included as Table A-4 of this document. Table A-7 provides the evaluation criteria that should be used to review each document.

During testing, two witnesses – one from the certification team and one person from the system owner's office – should witness all ST&E activities to ensure that all procedures are properly executed.

3.2.3.1 Create the ST&E Report and Recommend Countermeasures (High & Medium Systems)

After the testing activities are complete, any findings from the testing should be documented in a ST&E report. The report should identify which controls are complete, which security controls are only partially implemented and those controls that are either not implemented or are ineffective. These results will be used as input to update the risk assessment.

After the ST&E report is complete, the system owner and the program manager should discuss the appropriate countermeasures to be implemented. These countermeasures should address any security requirements that were found to be not implemented or ineffective. Recommended

countermeasures may be implemented immediately or may be included as part of a remediation plan and schedule for an IATO.

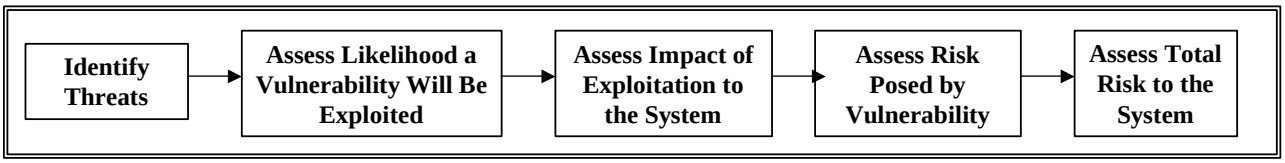
3.2.4 Step 9: Update the Risk Assessment (High & Medium Systems)

This step involves using the results from the ST&E to update the risk assessment and determine the remaining risk for the system once corrective actions have taken place to address findings from the ST&E. Updates to the risk assessment should be included in the form of an addendum to the original risk assessment report. Risk should be determined for both individual findings and the overall system or application. This risk determination will be included as part of the certification package. Both the USDA Risk Assessment Methodology and the NIST SP 800-30 should be used to ensure that all necessary risk assessment areas are completed.

The risk assessment update should consist of the following steps, as shown in Figure 3-3:

- The list of threats to the system should be reviewed. The list should include but not be limited to hackers, malicious insiders, attacks against the system facility, and natural disasters.
- Assess each system vulnerability identified during the ST&E. Evaluate the likelihood that one of the identified threats will exploit an identified vulnerability.
- Assess the possible impact to the system and the agency if the vulnerability was exploited.
- Make a determination of risk based on the likelihood that the threat will exploit the vulnerability, and the impact that would result.
- Evaluate the risks of all identified vulnerabilities to determine an overall level of risk for the system or application.

Figure 3-3
Risk Assessment Steps



3.2.5 Step 10: Update the System Security Plan, ISA and PIA (High & Medium Systems)

Using the guidance in NIST SP 800-18, the SSP should be updated to reflect the results of the ST&E activities and the final risk assessment. Updates should also be made in the approved ISA & PIA. Any countermeasures implemented as a result of the ST&E findings should be added to the list of system security controls.

3.2.6 Step 11: Document Certification Findings (High & Medium Systems)

Once the certification activities are complete, the certification team should document the findings from the certification process in a Security Evaluation Report (SER). This report will summarize the findings and other relevant security issues identified during certification activities. A template for the SER is included as Appendix F of this document. The certification team then compiles this report. Certification findings should include ST&E findings, risk

assessment findings, and any other relevant issues discussed during certification activities. These findings should be compiled along with the other certification documents into a certification package and forwarded to the CO for review. Table 3-3 below contains a list of the items that should be included as part of the certification package.

Table 3-3
Certification Package Contents **(High & Medium Systems)**

Certification Package	
	Security Controls Compliance Matrix (completed)
	Security Test and Evaluation Report Approved Interconnection Security Agreement PIA/SOR Notice (if required)
	Risk Assessment
	System Security Plan
	Security Evaluation Report

Note the Certification Package Contents for Low Impact Systems - For low impact systems the security accreditation package consists of: the updated System Security Plan, an updated Risk Assessment, an abbreviated NIST 800-26 Security Assessment Report, Security Categorization Document, and the Plan of Action and Milestones.

The CO will evaluate the risks and issues presented in the SER and the other documents in the certification package. The CO then develops a Certification Statement that states the extent to which the system meets its security requirements. As part of the Certification Statement, the CO also provides a recommendation for an accreditation decision. The CO then forwards the certification statement and the SER to the ACIO-CS for mandatory concurrence. If the ACIO-CS concurs, the CO will forward the package to the DAA with the recommended accreditation decision.

3.2.6.1 Interim Authority to Operate
See Section 1.2 for information on Interim Authority to Operate.

3.2.7 Step 12: Accreditation Decision (High, Medium & Low Systems)

During the final step of Phase 2, the DAA will review the Security Evaluation Report and issue the decision to issue a full accreditation or to deny accreditation after weighing the residual risk and other factors discussed in the package. In the case of a low impact system, the DAA will review the SSP, Risk Assessment and abbreviated Self Assessment and make a risk based decision to grant the system accreditation or deny the system accreditation because the risks to the system are not at an acceptable level. Based on an evaluation of residual risk, the CO's recommendation and the ACIO-CS' concurrence, the DAA can make a risk-based decision to grant system accreditation or to deny system accreditation because the risks to the system are not at an acceptable level. The accreditation decision will be documented in the final accreditation package, which consists of the accreditation letter and supporting documentation and rationale for the accreditation decision.

The following checklist provides a reminder of all the actions that should take place during Phase 2 of the C&A process **for high and medium impact systems**:

Phase 2 Checklist	
	Has the ST&E Plan been created and approved?
	Has security testing been performed? Have Privacy Implications been reviewed (if required)?
	Has the approved ISA been reviewed? Has the ST&E Report been written?
	Were the countermeasures recommended in the ST&E report implemented on the system?
	Has the Risk Assessment been updated?
	Has the System Security Plan been updated?
	Have the certification findings been documented?
	Has the certification package been forwarded to the CO?
	Has the certification package obtained ACIO-CS concurrence?
	Has the CO completed a Security Evaluation Report and forwarded it to the DAA?
	Has the DAA issued an accreditation decision?

Note the Certification Package Contents for Low Impact Systems - For low impact systems the security accreditation package consists of: the updated System Security Plan, an abbreviated Security Assessment Report, updated Risk Assessment, Security Categorization Document, and the Plan of Action and Milestones.

3.3 Phase 3: Post-Accreditation Phase

During the post-accreditation phase, the system configuration will be managed to ensure that changes to the system are monitored to ensure that they do not adversely affect the security posture of the system and to facilitate follow-on C&A activities. Additionally, the system owner should keep the SSP, risk assessment, as well as other documents current, adding any new security controls as they are implemented. Periodic testing (at least annually) of the Contingency Plan is a necessary component of the Post-Accreditation Phase and, although this may be a part of the SSP, it needs to be addressed at a higher level of visibility. Finally, at the end of Phase 3, the system will go through the C&A process again as part of the re-accreditation of the system.

3.3.1 Configuration Management

Once the system or application has been officially accredited, the system owner should maintain configuration control over the system to ensure that the security posture of the system is not threatened by authorized or unauthorized changes to system software or hardware. Any changes to system security settings, hardware, or software should be discussed and approved by the CCB. Additionally, a security professional should be on the CCB to ensure that security issues are covered and addressed.

Any changes that are implemented should be documented in the SSP (for security changes), design documentation (for software code changes), or the inventory list (for hardware and/or software changes). Large-scale system changes (e.g., software version changes, operating system changes) may require re-accreditation activities to ensure that the system has not be exposed to additional risk.

3.3.2 Re-Accreditation

Federal regulations mandate that systems be re-accredited every three years or when significant changes are made to the system configuration. Program managers and system owners should keep this in mind when planning system changes. If the system is not significantly altered, the system owner should begin the certification and accreditation process for re-accreditation in a timely fashion to ensure that the process is complete before the three-year anniversary of the system accreditation has passed.

The following checklist provides a reminder of all the actions that should take place during Phase 3 of the C&A process.

Phase 3 Checklist	
	Has the system owner maintained configuration control?
	Have all changes to the system been approved by the CCB?
	Have the hardware and software inventories been updated every time the system configuration changed?
	If major system changes have been implemented, has the system been re-accredited in its new configuration?
	Is the three-year anniversary of the system accreditation approaching? If so, have plans been made to begin the re-accreditation process?

4 Summary

Certification and accreditation includes technical and non-technical assessments that establish the extent to which the system or application meets a set of specified security requirements for its task and operational environment. The job of the Certifying Official is to provide a technical evaluation. The ACIO-CS will provide assurance that the certification package meets federal and USDA policy and processes. The outcome of this process—the accreditation—assures the DAA that the level of security used will protect systems information and processing capabilities.

The C&A process should be integrated into the SDLC during CPIC process. New regulations state that every USDA general support system or application must have official approval to operate. If systems have not obtained official approval to operate prior to deployment, they must complete the C&A process and obtain approval to operate.

In summary, the C&A process comprises three phases: the pre-certification phase; the certification and accreditation phase, and the post-accreditation phase. Phase 1, the pre-certification phase, has several steps: defining the scope of the C&A effort, identifying existing security controls, reviewing the Interconnectivity Security Agreement (ISA), determining Privacy implications**,** reviewing the SSP, reviewing the initial risk assessment, and negotiating with the participants. Low Impact/Low Risk systems follow a streamlined certification process, but still require approval by the DAA in order to operate. Phase 2, the certification and accreditation phase, consists of additional steps that include: conducting the ST&E, updating the risk assessment with findings from the ST&E, reviewing PIAs, updating ISAs and SSP, documenting certification findings; and forwarding the certification findings to the DAA for an accreditation decision. Phase 3, the post-accreditation phase, consists of managing the configuration of the system and re-accreditation every three years or when the system changes significantly.

TABLE A-1: GLOSSARY OF TERMS

Accreditation: The formal declaration by the DAA that the system is approved to operate using a prescribed set of safeguards and should be strongly based on the residual risks identified during certification.

Application: A system that performs a clearly defined function for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system or an air traffic control system).

Availability: Available on a timely basis to meet mission requirements or to avoid substantial losses.

Certification: The comprehensive assessment of technical and non-technical security features and other safeguards associated with the use and environment of a system to establish whether the system meets a set of specified security requirements.

Certifying Officer (CO): The Certifying Officer assumes the role of an independent technical liaison for all stakeholders involved in the C&A process and is an objective third party, independent of the system developers. The Certifying Officer provides a comprehensive evaluation of the system, including technical and non-technical controls, to determine if the system is configured with the proper security controls in place.

Confidentiality: Protection from unauthorized disclosure.

Configuration Management Plan: A plan that describes the management controls involved in all changes and updates made to a system that affects security. The plan includes all documentation supporting these changes and updates. This plan is maintained throughout the C&A process and updated according to system development lifecycle (SDLC) activities.

Contingency Plan: Preventive measures established to assist an organization in their ability to quickly and cost effectively recover critical IT resources.

Continuity of Support: Preventative measures for protecting the IT systems as well as procedures for restoring any system disruption

Designated Accrediting Authority (DAA): The Designated Accrediting Authority determines accreditation based on security risks of the system, business case, and budget.

Disaster Recovery Plan: A plan that identifies recovery procedures in the event of natural or man-made disasters or catastrophes affecting the availability of the system. This plan is tested annually to ensure the continued effectiveness and adequacy of the plan.

General Support System: A collection of interconnected information resources under the control of a single authority and security policy, including personnel and physical security, which shares common functionality. Provides standard information security capabilities, such as boundary defense, incident detection and response, and key management, and also delivers common applications, such as office automation and electronic mail.

Information Sensitivity: The formal process of identifying each system in terms of its confidentiality, integrity, and availability.

Information System: An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (USC T44;C35;S3502)

Integrity: Protection from unauthorized, unanticipated, or unintentional modification.

Privacy Impact Assessment (PIA): A tool used to evaluate the impact that information systems have on an individual. The PIA process is designed to guide agency system developers and operators in assessing privacy through the early stages of development.

Residual Risk: The portion of risk that remains after security measures have been applied.

Risk Assessment: The process of analyzing threats to and vulnerabilities of an information system to determine the risks (potential for losses), and using an analysis as a basis for identifying appropriate and cost-effective measures.

Security Test and Evaluation: An evaluation of all hardware, software, and physical security features that are part of a system. This process involves testing these features to determine what threats and vulnerabilities exist for the system. The findings are documented, and recommendations are made that may be included in the risk assessment.

Significant Change: A significant change alters the mission, operating environment, or basic vulnerabilities of the systems. Examples of significant change include: increase/decrease in hardware, application programs, external users, hardware upgrades, additions of telecommunications capability, dial-in lines, changes to the program logic of application systems, relocation of the system to a new physical environment or new organization. Changes determined by the CCB to be significant will require re-accreditation. Changes that impact Privacy Act Data will require re-accreditation. Changes in protection requirements such as the sensitivity or classification level of the data being processed, increase in the mission criticality of the system or changes in the federal or USDA policies are also considered significant change. A violation or incident that calls into question the adequacy of the system security controls is considered a significant change. In addition, findings from any security review that identifies unprotected risk are considered a significant change. These could include the system IT security review, physical or information security inspection, internal control reviews, Office of the Inspector General (OIG) or General Accounting Office audits.

System Development Life Cycle (SDLC): A structured approach for systems development from planning and support to disposal of the system. A proven series of steps and tasks utilized to build and maintain quality systems faster, at lower costs, and with less risk.

System of Records (SOR) Notice: A system of records is defined as a group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System Security Plan: A set of requirements that are used to delegate how system security will be managed. This plan includes system identification, management controls, operational controls, and technical controls. The system security plan outlines responsibilities for all system users and describes the rules of behavior for those users.

TABLE A-2: ACRONYMS

ACIO-CS	Associate Chief Information Officer for Cyber Security
C&A	Certification and Accreditation
CCB	Configuration Control Board
CIO	Chief Information Officer
CO	Certifying Officer
CPIC	Capital Planning Investment Control
DAA	Designated Approving Authority
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IATO	Interim Approval to Operate
ISA	Interconnection Security Agreement
ISSO	Information Systems Security Officer
IT	Information Technology
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIACAP	National Information Assurance Certification and Accreditation Process
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information Systems Security
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PUB	Publication
SCCM	Security Control Compliance Matrix
SCL	Security Certification Level
SDLC	System Development Life Cycle
SER	Security Evaluation Report
SFUG	Security Features Users' Guide
SOR	System of Records
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation
TFM	Trusted Facility Manual
USDA	United States Department of Agriculture

TABLE A-3: REFERENCES

Computer Fraud and Abuse Act
As amended 1994 and 1996, U.S.C. Section 1001 and 1030 Amended Title 18 Crimes and Criminal Procedure.

FIPS 102 National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Guidelines for Computer Security Certification and Accreditation, September 1983

FIPS 191 National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Guideline for the Analysis of Local Area Network Security November 1994

FIPS 199 National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS), Security Categorization of Federal Information Systems (Draft), May 2003

FISMA (P.L. 107-307), Federal Information Security Management Act (FISMA) January 2003.

NIST SP 800-18 National Institute of Standards and Technology (NIST), Guide for Developing Security Plans for Information Technology Systems, December 1998

NIST SP 800-26 National Institute of Standards and Technology (NIST), Security Self Assessment Guide for IT Systems, November 2001

NIST SP 800-30 National Institute of Standards and Technology (NIST), Risk Management Guide for IT Systems, January 2002

NIST SP 800-34 National Institute of Standards and Technology (NIST), Contingency Planning Guide for Information Technology Systems, Currently under development

NIST SP 800-47 National Institute of Standards and Technology (NIST), Security Guide for Interconnecting Information Technology Systems, September 2002

NSTISSI No. 1000 National Security Telecommunications and Information System Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), April 2000.

OMB A-123 Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-123 (Management Accountability and Control), 21 June 1995

OMB A-130	Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-130, Appendix III, 28 November 2000
Privacy Act	(http://www.usdoj.gov/04foia/privstat.htm)

TABLE A-4: DOCUMENTATION

To fully address system security throughout the system development life cycle, various documents should be created and maintained throughout the life of the system. These documents and a brief description of their contents are listed below, along with resources that provide information on how to develop each document.

Document	Description	References
Agency Self Assessment	The agency Self Assessment should be completed in accordance with NIST guidance to ensure that system security controls are maintained to protect system assets and information.	NIST SP 800-26
System Security Plan	The SSP should contain a description of the security controls required for the system and how those controls are implemented as part of the system's security posture.	NIST SP 800-18 DM 3565-001
Security Test and Evaluation Plan	The ST&E Plan should contain procedures and/or checklists for validating that each required security control is implemented.	NIST SP 800-26
Security Test and Evaluation Report	The ST&E Report contains results from functional and security testing conducted on the system as required by the security categorization.	NIST SP 800-26
Risk Assessment Report	The Risk Assessment report should contain the findings from the ST&E Report as well as an evaluation of the risk that each finding poses to the system. The residual risk to the entire system should be determined.	NIST SP 800-30 DM 3540-001
Contingency and Disaster Recovery Plans	Contingency plans and disaster recovery plans contain all procedures that will be taken in the event of an incident that shuts down the system or a large emergency that destroys the system entirely. These procedures should provide for system and data restoration in a certain amount of time based on system criticality.	NIST SP 800-34 DM 3570-001
Trusted Facility Manual (TFM)	The TFM should contain procedures for system administrators that explain how to operate the system or application in the most secure manner. Emergency backup and system shutdown procedures should be included in the TFM.	NCSC-TG-016 NCSC-TG-015 CS-032 Guidance
Security Features User's Guide (SFUG)	The SFUG should be written for system and application users and should clearly explain the security procedures and precautions that	NCSC-TG-026 CS-033 Guidance

Document	Description	References
	users are expected to follow, i.e., procedures for maintaining password secrecy, etc.	
Standard Operating Procedures	These procedures should include the day-to-day processes for running the system or application. These can be incorporated into the TFM or SFUG or can be standalone documents.	N/A
Configuration Management Plan	The CM plan should address configuration management through the operations and maintenance phase of the system life cycle. The Plan should contain procedures for maintaining configuration control over system components, software, and documentation.	EIA-649 DM 3520-001
User Manuals	Manuals providing instructions for users on how to operate the system. May be combined with the SFUG.	N/A
Vendor-Supplied Hardware Manuals and Documentation	Any hardware user manuals, system administrator manuals, or other hardware documentation provided by the vendor.	N/A
Vendor-Supplied Software Manuals and Documentation	Any software user manuals, system administrator manuals, or other software documentation provided by the vendor.	N/A
Accreditation Statement	The accreditation letter signed by the DAA, along with any other supporting documentation submitted in support of the certification package.	N/A
Waiver Documentation	Any system/security waiver or policy exception request that has bee approved and in force. Includes and approval documentation and any fix POA&M information	N/A
Interconnectivity Security Agreements	Agreements between agencies or departments with interconnecting information systems. If this system will be connected to other IT systems, the business owner must discuss the requirements for connectivity with the other system's business owner and work to identify the security requirements for this connection. The ISA is started during the Initiation Phase of the SDLC, is refined during the Acquisition/Development Phase but the ISA may not be completed until the actual system Implementation Phase. An ISA will be done for each system that will be	NIST PUB 800-47 DM 3540-001 DM 3575-001

Document	Description	References
	connected to the new system.	
Application or System Design Documentation	Any design documentation, system specifications, or software requirements specifications as required by the USDA.	N/A
Privacy Impact Assessment	A Privacy Impact Assessment must be performed to ensure the security of the data. If required, a Systems of Record Notice must also be completed.	Privacy Act DM 3515-002

TABLE A-5: USDA CHECKLISTS

The USDA has developed information security checklists for the following operating systems and software applications:

- UNIX
- Windows NT (server and desktop)
- IBM AS 400
- Personal Electronic Devices
- Windows XP
- Telework & Remote Access
- Mainframe
- Telecommunications
- Web Farm
- Novell Networks
- Windows 2000
- Portable Laptops & Desktop Computers

TABLE A-6: SECURITY EVALUATION REPORT

TITLE [Use only CAPITOL letters] (ACRONYM)

SECURITY EVALUATION REPORT

Subject: Conditional Certification of the TITLE (ACRONYM).

Purpose: In compliance with P.L. 100-235, January 8, 1998 "Computer Security Act of 1987" and in accordance with FIPS PUB 102, "Guideline for Computer Security Certification and Accreditation", this security evaluation report has been performed to satisfy the OMB Circular A-130 requirements to periodically certify and accredit systems every three years.

Introduction: ACRONYM provides … PURPOSE/FUNTION

System Architecture: ACRONYM operates in ARCHITECTURAL DESCRIPTION…

(List ONLY the software components tested.)

Documentation:

A *ACRONYM Risk Assessment* dated DATE, and related documents were submitted.

The *ACRONYM Security Test and Evaluation Plan* dated DATE was submitted with the certification documentation. The security test and evaluation was conducted at FACILITY LOCATION on DATE. A *ACRONYM Security Test and Evaluation Report* was submitted DATE. Response to the security findings listed in the *ACRONYM Security Test and Evaluation Report* was received on the following date: DATE.

[If there are multiple responses list the date of each response.]

Major Findings: This section is divided into three parts: clarifications, safeguards, and vulnerabilities.

Clarifications: None

Safeguards: ACRONYM relies on …DESCRIPTION OF SECURITY SAFEGUARDS IN THE SYSTEM…

Vulnerabilities:

The following vulnerabilities were identified during certification activities:

The RISK LEVEL shall be indicated for each finding as follows:

Conditions of Certification: Any conditions of this certification are listed below and are identified as either restrictions or recommended corrective actions**.**

Restrictions: [Conditions].

Recommended Corrective Actions: The following actions are recommended for implementation to further reduce the risk associated with ACRONYM**:**
[The RISK LEVEL is NOT included in this section.]

Mandatory Concurrence: The ACIO-CS has performed an in-depth IV&V and has found the following : *Any conditions for accreditation, correction actions etc. will be detailed here. If the certification package, in the judgment of the ACIO-CS, is not adequate for accreditation, the reasons will be detailed here.*

TABLE A-7: BASE LEVEL DOCUMENT EVALUATION CRITERIA

Introduction

This document contains Certification and Accreditation (C&A) Base Level Document Evaluation Criteria checklists that are intended to provide standardized criteria for developing and evaluating C&A documentation during the C&A process for Major Applications (MAs) and General Support Systems (GSS). The organization responsible for developing the C&A documentation should use the checklists to assist them while developing the documents and to ensure the documents are ready for evaluation purposes by the Security Test and Evaluation (ST&E) team to support certification of the respective system. The ST&E team should use the criteria checklists during their evaluation of the system's security in order to determine whether the existing documents possess the critical elements necessary to meet Federal and Department-level security requirements for certification and accreditation.

With the exception of the security plan checklists, which are different for agency level security plans, GSS, and MAs, all the checklists should be completed for each certification and accreditation effort. The evaluator should select the appropriate security plan checklist(s) for the system depending on whether the system undergoing evaluation is a GSS or an MA.

Format

Each checklist identifies the critical requirements specific to each document and provides columns where the evaluator marks whether or not the requirement is fulfilled and annotates any specific comments next to the requirement. Directly after the requirements checklist is a section for the evaluator to add overall comments about the state of the document and whether or not it meets the necessary requirements for certification. There is also a section for evaluator recommendations – if the evaluator does not feel that the document meets enough of the requirements for certification, he or she can list specific recommendations for the agency to implement in order to improve the document.

By signing the evaluation checklist, the evaluator is attesting to the fact that the evaluation is complete and correct, to the best of their knowledge, and that the document adequately describes the critical elements for the respective document. If the evaluator feels that the agency needs to revise the document in order to meet the necessary standard for certification, they should state this explicitly in the Evaluator Comments and Evaluator Recommendations sections. Once the necessary changes have been made, the document should be re-evaluated using a new checklist for the revised document. The final completed checklists should be submitted as part of the ST&E report, which is reviewed by the Certifying Officer as part of the certification package and process.

2. Scoring

There is no set scoring method. Whether or not a particular document has met enough of the criteria in order to be adequate for the purposes of system certification is the judgment of the evaluator. The evaluator should explain briefly in the Evaluator Comments section why he or

she feels that the document meets the requirements for certification, particularly if there are specific requirements that have not been met.

System Identification _____Configuration Management Plan

Requirement*	Yes	No	Comments
Is there a CM Plan for the GSS/MA?			
Does the Plan identify a Configuration Management Specialist (CMS)?			
Does the Plan identify a Configuration Management Authority (CMA)?			
Does the Plan identify a Configuration Control Authority (CCA)?			
Does the Plan Identify a Configuration Control Board (CCB) for the GSS/MA?			
Does the Plan contain an approval signature?			
Is there a CCB charter for the GSS/MA?			
Is there an ISSO or ISSPM assigned to the CCB?			
Is the CCB charter signed by the CMA and CCA?			

Evaluator Comments:

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

* These criteria were derived from CS-009, *Guidance on Configuration Management*, Part 1 – Policy and Responsibilities and *USDA Guidelines for Writing Configuration Management Plans (CMPs)* Ver 1.1.

System Identification _____ Security Features Users Guide (SFUG)

Requirement*	Yes	No	Comment
Is the SFUG marked "For Official Use Only"?			
Is the SFUG accessible only on an Intranet site?			
Does the SFUG contain required technical security features information?			
Does the SFUG contain required Security Policy Information?			
Does the SFUG contain required security-related command information?			

Evaluator Comments:

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

* These criteria were derived from the *USDA Guidelines for Writing the Security Feature Users Guide (SFUG).*

System Identification _____ Trusted Facility Manual (TFM)

Requirement*	Yes	No	Comment
Does the TFM provide or reference the required information necessary to configure and install a specific secure system?			
Does the TFM present or reference cautions about functions and privileges that should be controlled when running a secure facility?			
Does the TFM provide or reference procedures for examining and maintaining the audit files?			
Does the TFM provide or reference detailed audit record structure for each type of audit event?			
Does the TFM provide or reference the administrator functions related to security, to include changing the security characteristics of a user?			
Does the TFM provide guidelines on the consistent and effective use of the protection features of the system?			
Does the TFM explain how the protection features of the system interact?			
Does the TFM provide guidelines on facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner?			
Does the TFM include or reference procedures to ensure that the system is initially started in a secure state and procedures to resume secure system operation after any lapse in system operation?			
Is an accurate and up-to-date copy of the TFM retained at each site's off-site back-up storage facility in order to support disaster recovery operations?			
Is the TFM marked "For Official Use Only"?			

Evaluator Comments:

* These criteria were derived from the *USDA Guidelines for Writing Trusted Facility Manuals (TFM).*

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

System Identification _____ Risk Assessment Report

A. System Introduction and Characterization

Requirement*	Yes	No	Comment
Is the purpose of the assessment described?			
Has the scope of the system, in terms of both system boundaries and areas to be assessed, been explained?			
Is the system's business or technical requirements explained?			
Is the information infrastructure explained?			
Has the IT assets to be assessed been identified?			
Has the data flow been explained?			
Has the interface to other systems been explained and identified?			
Has the software and hardware components been identified?			
Has the system security architecture been explained and identified?			
Has the system security architecture, which depicts the operating system, been explained and identified?			
Has the system security architecture, which examines the facilities where the system is contained, been explained and identified?			
Has the system security architecture, which explains the information storage requirements been explained and identified?			
Has the applicable system security policies governing the system (agency policies, federal requirements, laws, etc.) been explained and identified?			
Has value of the information been determined?			

B. Findings

Requirement	Yes	No	Comment
Have the system security vulnerabilities been explained and identified?			
Have the potential threats and impacts been explained and identified?			
Has the threat analysis been explained?			
Has the impact analysis been explained?			

* These criteria were derived from NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*, and the *USDA Risk Assessment Methodology* guide.

C. Analysis and Recommendations

Requirement	Yes	No	Comment
Have the findings been analyzed in terms of a Business Risk?			
Have the recommendations for mitigating each risk been identified and explained?			
Have the recommendations for mitigating each residual risk (if any) been identified and explained?			

Evaluator Comments:

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

System Identification _____ Overall Agency Security Plans

Requirement*	Yes	No	Comment
Does the plan address the appropriate management of IT security within the USDA agency/mission area?			
Does the plan address the current security management philosophy and specific functions of the ISSPM(s)?			
Does it include audits of system patches, personnel clearances, use of unauthorized or illegal software, incident response and reporting, change management procedures, security controls or as defined in DR 3140-1?			
Does the security plan, discuss in detail how your agency uses management controls to protect information assets, ensure that systems are heading towards certification and accreditation, conducting periodic reviews of information security procedures to ensure they work as intended and providing support for the role of the ISSPM in the organization?			
Does the security plan, discuss in specific detail the implementation of security policy and program activities? This portion of the plan should identify the assessments on which the determinations were made and policies created to meet the requirements of CIA.			
Does the plan, identify, describe or clarify the policy that establishes and maintains the ISSP within the USDA agency, mission area or program?			
Does it include the specific internal ISSP policies issued during the past year and those being planned for the upcoming year? These can be policies, notices, or directives and should be noted by subject and date issued.			

* These criteria were derived from NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

Requirement*	Yes	No	Comment
Does the plan, identify and discuss long-term strategies to incorporate Information Systems Security (ISS) into the overall agency mission and into next generation of agency IT systems? The long-term Information Systems Security Program Strategy is based on the organizations: Policy Integration; Technology needs; Resource base and budget requirements; Security accomplishments/setbacks of the previous year; New initiatives (Telecommuting, PKI, VPN, E-Commerce, etc.,); Security goals and challenges for the upcoming year; conformance to departmental architecture (infrastructure/security)?			
Does the security plan provide the foundation for linking security planning and activities from the Capital Planning and Investment Control (CPIC) and Government Information Security Reform Act (GISRA) now called the Federal Information Security Management Act (FISMA)?			
Has the plan developed Performance Measures for their security program?			
Does it describe in detail the Overall Performance Standards for the agency Security Program and how they are measured?			
Does the plan discuss the agency's security program risk assessment methodology?			
Does it include a Risk Assessment Report, vulnerabilities found and mitigation strategies?			
Does the plan discuss your agency efforts to implement privacy protection to include privacy training and number of Privacy Impact Assessments conducted?			
Does the plan discuss the implementation of configuration management procedures and techniques within your agency?			
Does the plan discuss in detail your agency’s compliance program?			
Does the plan discuss the upcoming agency specific plans for implementing an internal Security Awareness and Training Program and specialized training? This program should include details on planned annual security seminars, use of electronic media, such as e-mail or bulletin boards to enhance security awareness, and plans for briefing new employees/contractors on security awareness.			

Requirement*	Yes	No	Comment
If the agency does not have an active security training and awareness program, does it provide specific details, including time frames, on the plans to meet this requirement?			
Does the plan, include a statement as to whether all individuals working for the agency (federal employees as well as contractors) have received the appropriate background screening, suitability determination, and security clearance (if required) appropriate for the position to which they are assigned?			
Does the plan discuss the ISS program's incident handling strategy and the internal procedures developed to support DM 3500-1, Chapter 1, USDA Computer Incident Response Procedures?			
Does the plan discuss the Program contingency planning process to include: (1) identifying the mission, business, or critical functions; (2) identifying the resources that support the critical functions; (3) selecting contingency planning strategies; (4) anticipating potential contingencies or disasters; (5) analyzing vulnerabilities and risks, and (6) physical and environmental security. Information should also be included on Business Resumption Plan and Contingency of Operations Plan (COOP)?			

Evaluator Comments:

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

Requirement*	Yes	No	Comment
DOES THE PLAN DESCRIBE THE FUNCTION OR PURPOSE OF THE APPLICATION AND THE INFORMATION PROCESSED?			
Does the plan describe the processing flow of the application from system input to system output?			
Does the plan provide a general description of the technical system?			
Does it include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)?			
Does the plan describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources?			
Does the plan list interconnected systems and system identifiers?			
Does the plan require that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information?			
Does the plan describe, in general terms, the information handled by the system and the need for protective measures?			
Does the plan describe the risk assessment methodology used to identify the threats and vulnerabilities of the system?			
Does the plan discuss performance measures should be established around criteria such as Level of System Compromises, Timeliness of User Administration and Overall System Availability or other measure that reflect security?			
Does the plan list any independent security reviews conducted on the system in the last three years?			
Does it include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result?			
Does the plan include a set of rules of behavior and does it contain a signature page to acknowledge receipt?			

* These criteria were derived from NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

Requirement*	Yes	No	Comment
Do the rules of behavior clearly delineate responsibilities and expected behavior of all individuals with access to the system, state the consequences of inconsistent behavior or non-compliance and include appropriate limits on interconnections to other systems?			
Does the plan state which phase(s) of the life cycle the system, or parts of the system are in?			
Does the plan provide the date of authorization, name, and title of management official authorizing processing in the system?			
If not authorized, does it provide the name and title of manager requesting approval to operate and date of request?			
Does the plan state if individuals have received background screenings appropriate for the position to which they are assigned?			
Does the plan address the physical security measures provided for the system and the facility in which it is housed in accordance with the Cyber Security Manual, Chapter 2?			
Does the plan address physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems?			
Does the plan describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media (discuss user support, audit trails, restricting access to output products, external labeling, controlling storage)?			
Does the plan describe the procedures (contingency plan) that would be followed to ensure the application continues to be processed if the supporting IT systems were unavailable (agreements for backup, documented backup procedures, location of stored backups, tested contingency/disaster recovery plans)?			
Does the plan discuss restriction/controls on those who perform maintenance and repair activities and special procedures for performance of emergency repair and maintenance?			
Does the plan discuss version control that allows association of system components to the appropriate system version?			

Requirement*	Yes	No	Comment
Does the plan discuss procedures for testing and/or approving system components (operating system, other system, utility, applications) prior to promotion to production?			
Does the plan discuss change identification, approval, and documentation procedures?			
Does the plan discuss virus detection and elimination software installed?			
Does it describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends?			
Does the plan discuss if intrusion detection tools installed on the system?			
Does the plan discuss if penetration testing performed on the system?			
Does the plan discuss documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures?			
Does the plan describe the awareness program for the system (posters, booklets, and trinkets)?			
Does it describe the type and frequency of application-specific and general support system training provided to employees and contractor personnel (seminars, workshops, formal classroom, focus groups, role-based training, and on-the job training)?			
Does the plan discuss if there are procedures for reporting incidents handled either by system personnel or externally?			
Does the plan describe the method of user authentication (password, token, and biometrics)?			
Does the plan describe the level of enforcement of the access control mechanism (network, operating system, and application)?			
Does the plan describe how the access control mechanism supports individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual)?			
Does the plan describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users?			

Requirement*	Yes	No	Comment
Does the plan discuss the audit trail support accountability by providing a trace of user actions?			
Does the plan discuss audit trail include sufficient information to establish what events occurred and who (or what) caused them? (type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.)			

Evaluator Comments:

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

System Identification _____Major Application Security Plans

Requirement*	Yes	No	Comment
Does the plan describe the function or purpose of the application and the information processed?			
Does the plan describe the processing flow of the application from system input to system output?			
Does the plan provide a general description of the technical system?			
Does it include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)?			
Does the plan describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources?			
Does the plan list interconnected systems and system identifiers?			
Does the plan require that written authorization (MOUs, MOAs) be obtained prior to connection with other systems and/or sharing sensitive data/information?			
Does the plan describe, in general terms, the information handled by the system and the need for protective measures?			
Does the plan describe the risk assessment methodology used to identify the threats and vulnerabilities of the system?			
If there is no system risk assessment, does it include a milestone date (month and year) for completion of the assessment?			
Does the plan discuss performance measures should be established around criteria such as Level of System Compromises, Timeliness of User Administration and Overall System Availability or other measure that reflect security?			
Does the plan include a set of rules of behavior and does it contain a signature page to acknowledge receipt?			

* These criteria were derived from NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

Requirement*	Yes	No	Comment
Do the rules of behavior clearly delineate responsibilities and expected behavior of all individuals with access to the system, state the consequences of inconsistent behavior or non-compliance and include appropriate limits on interconnections to other systems?			
Does the plan state which phase(s) of the life cycle the system, or parts of the system are in?			
Does the plan provide the date of authorization, name, and title of management official authorizing processing in the system?			
If not authorized, is the name and title of manager requesting approval to operate and date of request, provided?			
Does the plan state if all positions been reviewed for sensitivity level?			
Does the plan state if individuals have received background screenings appropriate for the position to which they are assigned?			
Does the plan address the physical security measures provided for the system and the facility in which it is housed in accordance with the Cyber Security Manual, Chapter 2?			
Does the plan address physical access, fire safety, failure of supporting utilities, structural collapse, plumbing leaks, interception of data, mobile and portable systems?			
Does the plan describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media (discuss user support, audit trails, restricting access to output products, external labeling, controlling storage)?			
Does the plan discuss if the application software developed in-house or under contract?			
Does the plan discuss if the government owns the software? Was it received from another agency?			
Does the plan discuss if the application software a copyrighted commercial off-the-shelf product or shareware?			
Does it describe if it been properly licensed and enough copies purchased for all systems?			

Requirement*	Yes	No	Comment
Does the plan discuss virus detection and elimination software installed? If so, are there procedures for updating virus signature files, automatic and/or manual virus scans, and virus eradication and reporting?			
Does the plan discuss if intrusion detection tools installed on the system?			
Does the plan discuss if penetration testing performed on the system?			
Does the plan discuss documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures?			
Does it list the documentation maintained for the application (vendor documentation of hardware/software, functional requirements, security plan, general system security plan, application program manuals, test results documents, standard operating procedures, emergency procedures, contingency plans, user rules/procedures, risk assessment, certification/accreditation statements/documents, verification reviews/site inspections)?			
Does the plan describe the awareness program for the system (posters, booklets, and trinkets)?			
Does the plan describe the major application's authentication control mechanisms and the method of user authentication?			
Does the plan describe how the access control mechanism support individual accountability and audit trails (e.g., passwords are associated with a user ID that is assigned to a single person)?			
Does the plan discuss the controls in place to authorize or restrict the activities of users and system personnel within the application?			
Does the plan describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users?			
Does the plan discuss if the public accesses the major application?			
Does the plan discuss the audit trail support accountability by providing a trace of user actions?			

Requirement*	Yes	No	Comment
Does the plan discuss audit trails designed and implemented to record appropriate information that can assist in intrusion detection?			

Evaluator Comments:

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

System Identification _____ Privacy Impact Assessment

Requirement*	Yes	No	Comment
Has a Privacy Impact Assessment Form been developed for the system?			
Has a Privacy Policy Analyst been assigned?			
Has the system owner addressed what data is to be used, how the data is to be used, and who will use the data?			
Has the system developer addressed whether implementation of the owner's requirements presents any threats to privacy?			
Have any privacy risks been identified by the system owner, Privacy Policy Analyst or system developer?			
Has the individual been identified and documented who has access to the data in a system?			
When an individual has been granted access to a system, has their access been limited, where possible, to only that data needed to perform their assigned duties?			
Are procedures in place to detect and deter browsing or unauthorized access, when individuals using other systems (International, Federal, State, or Local entities) are granted access to all of the data in that system?			
Are data retention procedures documented?			
Are the intended and potential monitoring capabilities of the system, defined and safeguarded to ensure the privacy of customers and prevent unnecessary intrusion?			

Evaluator Comments:

* These criteria were derived from USDA Cyber Security Privacy Requirements.

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

System Identification _____Disaster Recovery and Business Resumption Planning

Requirement*	Yes	No	Comments
Is there a Disaster Recovery Plan for the GSS/MA?			
Does the Plan describe the system's Concept of Operations?			
Does the Plan provide a general description of the system architecture and functionality and how this system supports the business process			
Does the Plan identify the roles and responsibilities of the key players, such as the management team, damage assessment team, and system executive?			
Does the Plan outline the contingency planning organization?			
Does the Plan document the system's operational status and completed contingency actions?			
Does the Plan document the Notification and Activation, and Recovery Phases for contingencies?			
Does the Notification and Activation Phase describe the scope and magnitude of disruptive events that would necessitate plan activation?			
Does the Recovery Phase include detailed, sequential steps to take to shut down the system at the damaged site and establish temporary operations at another location or using alternate system components?			
Does the Recovery Phase include a description of the testing that should be done before bringing the alternate system online?			
Does the Reconstitution section focus on activities required to restore the system and its operating environment to normal conditions?			
Does the Reconstitution section include a description of the operational testing of the permanent system before operations are returned to it?			
Does the Plan discuss the need and requirements for concurrent processing?			
Does the Plan define the criteria for deactivation of the Plan?			
Does the Plan address the requirement for training on and periodic testing of the Plan?			

* These criteria were derived from USDA OCIO IT Disaster Recovery and Business Resumption Planning Certification and Accreditation Checklist, Version 1.0.

Requirement*	Yes	No	Comments
Does the Plan contain populated Appendices A through I as described in the USDA OCIO IT Disaster Recovery and Business Resumption Planning Certification and Accreditation Checklist?			

Evaluator Comments:

Evaluator Recommendations:

Evaluator Signature: _____ Date: _____

TABLE A-8:

ACCREDITATION LETTER SAMPLES

Security Accreditation Decision Letter (Authorization to Operate)

From: Authorizing Official Date:

Thru: Senior Agency Information Security Officer

To: Information System Owner

Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

After reviewing the results of the security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current system security plan, the security assessment report, and the plan of action and milestones), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is acceptable. Accordingly, I am issuing an *authorization to operate* the information system in its existing operating environment. The information system is accredited without any significant restrictions or limitations. This security accreditation is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system. The security accreditation of the information system will remain in effect as long as: (i) the required security status reports for the system are submitted to this office every [TIME PERIOD]; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) the system has not exceeded the maximum allowable time period between security accreditations in accordance with federal or agency policy. A copy of this letter with all supporting security certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

Signature

Title

Enclosures

Security Accreditation Decision Letter (Interim Authorization to Operate)

From: Authorizing Official Date:

Thru: Senior Agency Information Security Officer

To: Information System Owner Subject: Security Accreditation Decision for [INFORMATION SYSTEM]

After reviewing the results of the security certification of the [INFORMATION SYSTEM] and its constituent system-level components (if applicable) located at [LOCATION] and the supporting evidence provided in the associated security accreditation package (including the current system security plan, the security assessment report, and the plan of action and milestones), I have determined that the risk to agency operations, agency assets, or individuals resulting from the operation of the information system is *not* acceptable. However, I have also determined that there is an overarching need to place the information system into operation or continue its operation due to mission necessity. Accordingly, I am issuing an *interim authorization to operate* the information system in its existing operating environment. An interim authorization is a limited authorization to operate the information system under specific terms and conditions and acknowledges greater agency-level risk for a limited period of time. The information system is *not* considered accredited during the period of limited authorization to operate. The terms and conditions of this limited authorization are described in Attachment A. A process must be established immediately to monitor the effectiveness of the security controls in the information system during the period of limited authorization. Monitoring activities should focus on the specific areas of concern identified during the security certification. Significant changes in the security state of the information system during the period of limited authorization should be reported immediately. This interim authorization to operate the information system is valid for [TIME PERIOD]. The limited authorization will remain in effect during that time period as long as: (i) the required security status reports for the system are submitted to this office every [TIME PERIOD]; (ii) the vulnerabilities reported during the continuous monitoring process do not result in additional agency-level risk which is deemed unacceptable; and (iii) continued progress is being made in reducing or eliminating vulnerabilities in the information system in accordance with the plan of action and milestones. At the end of the period of limited authorization, the information system must be either authorized to operate or the authorization for further operation will be denied. Renewals or extensions to this interim authorization to operate will be granted only under the most extenuating of circumstances. This office will monitor the plan of action and milestones submitted with the accreditation package during the period of limited authorization. A copy of this letter with all supporting security certification and accreditation documentation should be retained in accordance with the agency's record retention schedule.

Signature

Title

Enclosures

TABLE A-9, INTERIM AUTHORITY TO OPERATE (IATO) FORM

IT Certification and Accreditation IATO Request Submission

Name of System:

Risk Level of System:

Name of DAA:	Email:	Telephone Number:
Name of CO:	Email:	Telephone Number:
Name of C&A POC:	Email:	Telephone Number:

---

1. Are all of the Phase 1, Certification and Accreditation Activities, complete?

2. Provide an explanation of the exception requested. Identify each vulnerability.

3. Identify the mitigation strategy, such as system replacement, for mitigating risks to the information residing on the system, identified as an “Action Item”.

4. Attach the formal Business Case necessitating the service

5. Identify the resource estimated funded/unfunded/reallocation

6. Provide the scheduled completion date

7. Attach Plan of Action & Milestones (POA&M) with interim completion dates

8. Provide current status

Appendix B
USDA PRIVACY IMPACT ASSESSMENT FORM

Project Name: _____
Description of Your Program/Project:

_____
_____
_____
_____
_____

DATA IN THE SYSTEM

1. Generally describe the information to be used in the system.	
2a. What are the sources of the information in the system?	
2b. What USDA files and databases are used? What is the source agency?	
2c. What Federal Agencies are providing data for use in the system?	
2d. What State and Local Agencies are providing data for use in the system?	
2e. From what other third party sources will data be collected?	
2f. What information will be collected from the customer?	
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	
3b. How will data be checked for completeness?	

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	
5a. Do other systems share data or have access to data in this system? If yes, explain.	
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	
6b. How will the data be used by the agency?	
6c. Who is responsible for assuring proper use of the data?	

ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	
2b. Will the new data be placed in the individual's record (customer or employee)?	
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	
2d. How will the new data be verified for relevance and accuracy?	
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	
4b. What are the potential effects on the due process rights of customers: • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making;	

• use of new technologies.	
4c. How are the effects to be mitigated?	

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers.	
2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	
2b. Explain any possibility of disparate treatment of individuals or groups.	
2c. What are the retention periods of data in this system?	
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	
2e. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	
3a. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?	
3b. How does the use of this technology affect customer privacy?	
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	

4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	
4c. What controls will be used to prevent unauthorized monitoring?	
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name. (SORs can be viewed at www.access.GPO.gov)	
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	

Appendix C
System of Records (SOR) Notice Guidance

The Privacy Act requires agencies to publish in the Federal Register a "notice of the existence and character of the system of records" subject to the Act (5 U.S.C. 552(e)(4)). Specifically, a "system of records" is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

The Privacy Act also requires agencies to send reports to Congress and the Office of Management and Budget (OMB) on the agency's intention to establish any new system of records, and under certain specified circumstances, the agency's intention to alter an existing system of records.

The report on a new or altered systems of records must be prepared and distributed no later than 30 days prior to establishment of a new system of records. This 30-day period is established to provide Congress and OMB an opportunity to review the proposed new or altered system and to provide comments, if desired. The 30-day period commences on the day the transmittal letter, with attachments, is signed and dispatched.

The Director, OMB, has the authority to waive the 30-day advance notification period provided that the transmittal letter specifically requests a waiver and the Department can demonstrate compelling reasons for not waiting the 30-day period.

Appendix D
INTERCONNECTION SECURITY AGREEMENT

Purpose – The purpose of this Interconnection Security Agreement (ISA) is to identify and document to all signatories satisfaction:

- Existing risks and mitigation strategies for all of the systems being interconnected, regardless of whether they are General Support Systems (GSS) or Major Applications (MA). Note: Any automated process that relies on Information Technology (IT) must be considered either a GSS or a MA.

- Any additional risks and mitigation strategies introduced through the interconnection of these systems for all participating systems. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, "Security Guide for Interconnecting Information Technology Systems" states *"A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. The document describes various benefits of interconnecting IT systems, identifies the basic components of an interconnection, identifies methods and levels of interconnectivity, and discusses potential security risks associated with an interconnection."*

- Documentation of all systems impacted by the interconnection, regardless of their participation in this agreement. (In the event a MA or GSS is not a signatory to this agreement, their role in the interconnection must be documented and a separate ISA must be prepared.)

- Provide appropriate levels of assurance (appropriate is very subject, might be well to include specifics) in accordance with NIST SP 800-47 and to the satisfaction of all signatories that the documented risk and mitigation strategies are operating as stated and are effective.

INTERCONNECTION STATEMENT OF REQUIREMENTS – This section shall contain:

- a clear description of the systems covered by this agreement,

- each systems intended purpose and target community,

- data sensitivity (information to and from systems is ***Sensitive-but-Unclassified*** unless specified otherwise),

- a description of the interconnection, including a graphic representation of the interconnection, the purpose of the interconnection and a clear description of the authorities under which all of the systems operate. (This can include statutory/regulatory requirements, project goals and should also clearly state the responsible management unit and system owner.)

This agreement shall be reviewed and updated on an annual basis or should be amended whenever major changes to the systems concerned are planned and executed. A change log and a new signature page should be attached whenever these events occur.

SYSTEM SECURITY CONSIDERATIONS – General information, data descriptions and data/work flows shall be documented in this section as well as risks and mitigation strategies so that a clear picture is presented to each participant of any residual risk. Any residual risks should be associated with either the business or mission component, administrative component or the customer component. To that end, the following documents shall be included (where data sensitivity allows) to the ISA:

- **Risk Assessments –** Risk Assessments for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended Risk Assessment shall become an attachment to this agreement. A copy of the Residual Risks accepted by the DAA should also be included.

- **System Security Plans –** System Security Plans for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended System Security Plan shall become an attachment to this agreement.

- **Configuration Management Plan –** Configuration Management Plans for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended Configuration Management Plan shall become an attachment to this agreement.

- **Trusted Facilities Manual –** Trusted Facilities Manuals for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the amended Trusted Facilities Manual shall become an attachment to this agreement.
- **Security Test and Evaluation Plan/Report –** Security Test and Evaluation Plans and subsequent reports for systems included in this agreement shall be amended by all participants to include the details of the agreement. A copy of the Security Evaluation Report shall become an attachment to this agreement.

- **Miscellaneous Security Assurance –** Additional citations should be included to address any additional security concerns and any deviations from USDA or NIST Guidance and/or Policy. Additional citations should also be included for USDA policies that delegate specific security responsibilities to agencies/staff offices for execution. Examples include, but are not limited to:

    - **Incident Reporting**
    - **Employee/Contractor Trusted Behavior Expectations**
    - **Information Exchange Security**
    - **Maintenance and Review of appropriate records, logs and audit trails**
    - **Applicable Certification & Accreditation/Interim Authority to Operate**
    - **Any other agency/staff office policies or practices**

Executive Summaries/Sign-Off – An Executive summary shall be prepared that details all residual risks and is tied directly to the portion of the ISA that contains all appropriate signatures. Conditions for revocation of an ISA authority shall appear in this area as well.