



U.S. Department of Agriculture



Office of Inspector General  
Financial & IT Operations

# Audit Report

## Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts

Report No. 50501-4-FM  
October 2005

---



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington DC 20250



October 21, 2005

REPLY TO

ATTN OF: 50501-4-FM

TO: David Combs  
Chief Information Officer  
Office of the Chief Information Officer

THRU: Sherry Linkins  
Office of the Chief Information Officer  
Information Resources Management

FROM: Robert W. Young /s/ Tracy LaPoint (for)  
Assistant Inspector General  
for Audit

SUBJECT: Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts

This report presents the results of our audit of the Department's certification and accreditation efforts. The report identified weaknesses in the Department's process, and agency's implementation of that process, to ensure that agency systems are accredited appropriately.

Your response to our draft report, dated October 7, 2005, is included in its entirety in exhibit B, with excerpts incorporated in the Findings and Recommendations section of the report. Based on the information provided in the response, we have reached management decision for Recommendations 1, 2, 3, 4, 5, 6, and 9. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer. For Recommendations 7 and 8, additional information is needed to reach management decision. Please refer to the OIG Position sections of the report for specific details.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation of the outstanding recommendations noted above. Please note that the regulation requires management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

We appreciate the courtesies and cooperation extended to us during the audit.

# ***Executive Summary***

## ***Review of the U.S. Department of Agriculture's Certification and Accreditation Efforts (Audit Report No. 50501-4-FM)***

---

### **Results in Brief**

This report presents the results of our audit of the U.S. Department of Agriculture's (USDA) certification and accreditation (C&A) efforts. Security accreditation is the official management decision to authorize operation of an information system and to explicitly accept the risk, if any, to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification.

We found that:

- Agency officials accredited their systems (see exhibit A), based in part on the recommendation of the certifying official, despite the fact that the supporting documentation did not meet National Institute of Standards and Technology (NIST) and Department guidelines;
- system risk ratings based on the confidentiality, integrity, and availability of the data residing on the system were inconsistent with Federal Information Processing Standard 199 which established the methodology to use when assigning risk ratings; and
- independent testing and evaluation processes did not provide adequate assurances that controls were in place and operating effectively.

We also found that agency and departmental oversight of the C&A process as well as the continuous monitoring phase of the process could be improved significantly. These conditions occurred because, as evidenced by our last 5 years' Government Information Security Reform Act and Federal Information System Management Act reports and despite repeated pledges of corrective action, the Department and its agencies have not addressed the Office of Management and Budget (OMB) requirement that major applications and general support systems be certified and accredited. Only after OMB made a specific call for compliance by the end of fiscal year 2004 in its passback language, did the Department implement an ambitious process and schedule to meet the stringent timeframes. Further, the Department did not have controls in place to ensure that the documents prepared to support system accreditations met departmental and NIST guidelines. In addition,

agency personnel relied on the contractors completing the documentation to ensure all requirements were met adequately.

Given these timeframes and the absence of prior accreditations, the agencies could not have produced complete, accurate, and trustworthy information given the depth and breadth of documentation required to adequately support each accreditation. Ultimately, the Department and its agencies expended an estimated \$20.3 million with outside contractors to fulfill the C&A requirements. However, the results, based on our analysis, were of little utility.<sup>1</sup>

The Department was prepared to use its fiscal year 2004 C&A efforts to report compliance with OMB Circular No. A-130, which had been previously reported as a material weakness in the Department's financial statements and our Federal Information Security Management Act reports. While the Department's efforts were commendable, completion of the first accreditation process is not the panacea to correct the Department's security weaknesses; rather it was the first step in identifying controls, documenting and testing those controls, and ensuring that the process gets integrated into each system's development life cycle as OMB intended.

The following are the deficiencies we identified in our review.

- Accrediting officials within the Department accredited systems based on inadequate and incomplete documentation. The Department did not have controls in place to ensure that the documents prepared to support system accreditations met departmental and NIST guidelines. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. As a result, not all system controls may have been documented and tested. Systems may continue to be at risk if all controls are not implemented effectively.
- Agencies had not applied the appropriate risk levels to their systems in accordance with NIST guidance or, in some cases, their own procedures. Further, agencies have not ensured that the risk ratings they assigned remained consistent throughout all of the C&A documents. This occurred because multiple contractors were employed to produce the various C&A documents without being privy to each other's conclusions and the agencies did not have controls in place to ensure the adequacy and sufficiency of the documentation supplied by the contractors. Further, the

---

<sup>1</sup>Estimated cost figures were obtained from an Office of the Chief Information Officer (OCIO) provided tracking spreadsheet. This figure has not been audited nor was it our objective to determine the actual amount expended within the Department for the C&A process.

agencies had not effectively monitored contractor compliance, and the agencies had not ensured the proper controls were applied based on the assessed risk level. Without a proper risk level assignment, the agencies cannot design adequate risk-based security programs to ensure the appropriate security controls are in place to protect the confidentiality, integrity, and availability of their information systems.

- Agencies and their contractors had not conducted Security Testing and Evaluation (ST&E) testing based on NIST requirements of validating whether documented security controls were in place and operating effectively. This occurred mainly due to the agencies not having effective controls in place to ensure that contractor-provided services and deliverables were completed appropriately, and because of the stringent timeframes imposed to complete the ST&E. As a result, the accreditation decisions were based on incomplete information regarding the effectiveness of security controls in the information systems.
- Agencies had not fulfilled the requirements of full system accreditation by establishing effective configuration management or continuous control monitoring of their systems. In fact, many agencies identified these processes as weaknesses on their Plan of Actions and Milestones reporting. The agencies lack the controls necessary to continually monitor their systems' security, and have historically addressed mandatory information technology security requirements only when reported in Office of Inspector General or U.S. Government Accountability Office reports. As a result, accrediting officials and system owners can not be assured that system configurations are maintained and properly controlled, and that controls are periodically tested for continued effectiveness.
- OCIO had not adequately tracked or monitored the status of agencies' activities. Further, our review continued to show weaknesses in OCIO's ability to accurately maintain a Department-wide inventory of systems. OCIO relied on the agencies to report systems, timeframes, and milestones without independent verification. This resulted in the USDA reporting inaccurate system authorization percentages to OMB.

## **Recommendations In Brief**

We recommended that OCIO:

- Require the agencies to reevaluate the accreditation decision and the documentation prepared during Phase I of its C&A efforts, and ensure that the accreditation is supported by complete, accurate, and trustworthy documentation which meets the requirements of NIST and departmental guidance;

- establish processes and controls, including an oversight function, to ensure agencies establish the proper risk ratings for its systems;
- require all agencies to implement controls to ensure the ST&E process provides the level of assurance needed by the accrediting official to render an informed decision; and
- OCIO should establish controls to periodically evaluate the accuracy of information provided by the agencies.

**Agency Response** OCIO generally agreed with the findings and recommendations in this report. Its response is presented in its entirety as exhibit B of this report.

## ***Abbreviations Used in This Report***

---

ACIO-CS	Associate Chief Information Office-Cyber Security
AQAS	Agricultural Quarantine Activity System
ARS	Agricultural Research Service
C&A	Certification and Accreditation
DAA	Designated Approving Authority
EAR	Enterprise Architecture's Repository
EP	Estimates Processing System
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FNS	Food and Nutrition Service
FSA	Farm Service Agency
F&ITO	Financial & IT Operations
FAS	Foreign Agricultural Services
GAO	U.S. Government Accountability Office
GISRA	Government Information Security Results Act (superseded by FISMA)
GSM	Guaranteed Sales Manager System
IATO	Interim Authority To Operation
IT	Information Technology
IV&V	Independent Validation and Verification
JFMIP	Joint Financial Management Improvement Program
NASS	National Agricultural Statistics Service
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PFCS	Program Funds Control System
POA&M	Plan of Actions and Milestones
PPQ	Plant Protection and Quarantine
SCCM	Security Control Compliance Matrix
SP	Special Publication
ST&E	Security Testing and Evaluation
SSO	State Statistical Offices
USDA	U.S. Department of Agriculture

# Table of Contents

---

<b>Executive Summary .....</b>	<b>i</b>
<b>Abbreviations Used in This Report .....</b>	<b>v</b>
<b>Glossary .....</b>	<b>vii</b>
<b>Background and Objectives .....</b>	<b>1</b>
<b>Findings and Recommendations.....</b>	<b>3</b>
<b>Section 1 - Agencies Accredited Their Systems Based on Incomplete and Unreliable Supporting Documentation .....</b>	<b>3</b>
Finding 1    Documents Supporting Agency C&A Did Not Meet Federal Guidelines .....	4
Recommendation No. 1.....	8
Recommendation No. 2.....	9
Finding 2    Agencies Inaccurately and Inconsistently Applied System Risk Ratings .....	10
Recommendation No. 3.....	12
Finding 3    Security Testing and Evaluation (ST&E) Phase Did Not Yield Assurances That System Security Controls Were in Place and Operating Effectively.....	12
Recommendation No. 4.....	15
Recommendation No. 5.....	15
Recommendation No. 6.....	16
<b>Section 2 – Agencies and the Department Have Not Implemented Effective Oversight and Monitoring Processes .....</b>	<b>17</b>
Finding 4    Agencies Have Not Implemented Effective Oversight and Monitoring .....	17
Recommendation No. 7.....	19
Finding 5    OCIO Monitoring and Oversight Could be Strengthened.....	19
Recommendation No. 8.....	21
Recommendation No. 9.....	22
<b>Scope and Methodology.....</b>	<b>23</b>
<b>Exhibit A – List of Agencies and Systems Reviewed .....</b>	<b>24</b>
<b>Exhibit B – Agency Response.....</b>	<b>26</b>



# ***Glossary***

---

Certification and Accreditation – A process mandated by the Office of Management and Budget Circular No. A-130 requiring that IT system controls be documented and tested by technical personnel and given the formal authority to operate by an agency official.

Network – Two or more computers connected to one another by a common communication standard.

Physical Access Controls – Processes or activities that physically limit access to computer systems or networking devices. For instance, locking rooms where systems are stored.

Environmental Controls – Processes or activities that provide the optimum operating environment for computer systems and networking components. For instance, air conditioning systems that keep systems from overheating.

Local Area Network – A group of computers located in a small geographical area (such as a single office building) connected by a common communication standard.

Major Application – One or more related applications that support a critical function of the agency and/or that contain data considered sensitive by law.

Security Testing and Evaluation – One phase of the certification and accreditation where an independent party evaluates and conducts testing of the controls established in and around a system. The purpose is to determine whether controls as stated in the system documentation are adequate and operating as prescribed.

# ***Background and Objectives***

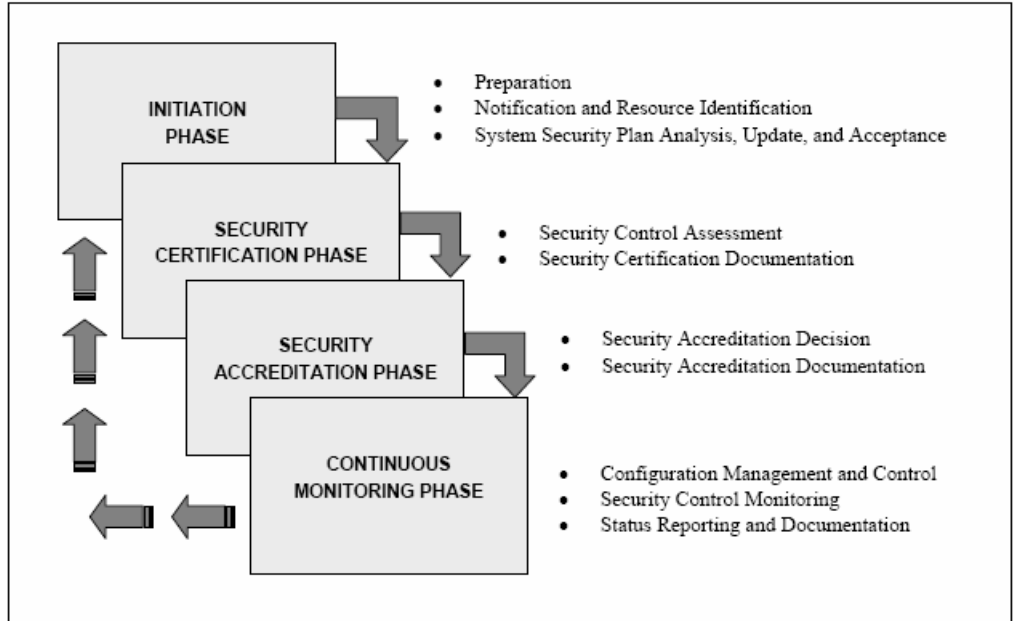
---

## **Background**

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk, if any, to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Required by the Office of Management and Budget (OMB) Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources,” dated November 30, 2000, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision.

The security certification and accreditation (C&A) process consists of four distinct phases: (1) Initiation Phase, (2) Security Certification Phase, (3) Security Accreditation Phase, and (4) Continuous Monitoring Phase. Each phase in the security C&A process consists of a set of well-defined tasks and subtasks that are to be carried out, as indicated, by responsible individuals (e.g., the Chief Information Officer, authorizing official, authorizing official’s designated representative, senior agency information security officer, information system owner, information owner, information system security officer, certification agent, and user representatives).



Although the requirement to perform system C&A has been in place since OMB Circular No. A-130 was originally issued in the mid-1980's, the Department and its agencies have not addressed the requirement. With the passage of the Government Information Security Reform Act (GISRA) in 2000 and superseded by the Federal Information Security Management Act (FISMA) in 2002, information technology (IT) security has received additional attention in the Federal sector. We have reported continually the lack of compliance with OMB Circular No. A-130 in the two GISRA and three FISMA reports we have issued.

A significant force behind the Department's C&A efforts in 2004 was budget passback language handed down from OMB on the Department's fiscal year 2005 budget request. OMB required that the Department certify and accredit all of its systems by the end of fiscal year 2004.

**Objectives**

The audit objective was to determine the adequacy of the Department's C&A process and whether the process yielded adequate and reliable documentation to properly accredit the Department's systems as intended by OMB Circular No. A-130.

# ***Findings and Recommendations***

## ***Section 1 - Agencies Accredited Their Systems Based on Incomplete and Unreliable Supporting Documentation***

---

It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system. We found that:

- Agency officials accredited their systems, based in part on the recommendation of the certifying official and reliance on contractors, despite the fact that the supporting documentation did not meet National Institute of Standards and Technology (NIST) and Department guidelines (i.e., thorough description of system boundaries and baseline security controls);
- system risk ratings based on the confidentiality, integrity, and availability of the data residing on the system were inconsistent with Federal Information Processing Standard (FIPS) Publication 199 which established the methodology to use when assigning risk ratings, and
- independent testing and evaluation processes did not provide adequate assurances that controls were in place and operating effectively.

This occurred because, despite repeated audit disclosures and pledges of corrective action, the Department and its agencies had not addressed the OMB requirement that major applications and general support systems be certified and accredited. Only after OMB made a specific call in its passback language for compliance by the end of fiscal year 2004, did the Department implement an ambitious process and schedule to meet the stringent timeframes. Further, discussions with agency personnel disclosed that, due to the timeframes allotted, they relied on the contractors completing the documentation to meet the requirements adequately.

Given the timeframes allotted and the absence of prior accreditations, the agencies could not have produced complete, accurate, and trustworthy information given the depth and breadth of documentation required to adequately support each accreditation. Agencies relied primarily on their contractors to address the C&A requirements without controls in place to ensure the adequacy and sufficiency of the documentation prepared by the

contractors. Without this trustworthy information, agency officials could have accepted greater risks than those already identified, overlook necessary controls, and may be ill prepared to address security-related incidents.

---

**Finding 1****Documents Supporting Agency C&A Did Not Meet Federal Guidelines**

Accreditation officials within the Department accredited systems based on inadequate and incomplete documentation. The Department did not have controls in place to ensure that the documents prepared to support system accreditations met departmental and NIST guidelines. As a result, not all system controls may have been documented and tested (see also Finding 3), and systems may be at risk if all controls were not implemented effectively.

FISMA requires each Federal agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The information security program must include:

- Periodic assessments of risk;
- policies and procedures based on risk assessments;
- plans for providing adequate information security;
- security awareness training to users;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices;
- processes to plan, implement, and evaluate the actions necessary to remediate any deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations.

Security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule

constraints.<sup>2</sup> By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully *accountable* for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation. It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

We identified numerous deficiencies in the six system C&A's we reviewed (see exhibit A) that have a material impact on the accrediting officials ability to make an informed decision on system accreditation, and the agency's ability to manage an effective security program for its systems. Despite these weaknesses, the accrediting officials fully accredited all six systems based, in part, on the recommendation of the certifying official. Further, agency personnel noted that due to the timeframes involved, they relied on their contractor completing the documentation to meet the requirements adequately. The following describes the most notable weaknesses in our review.

#### Risk Assessments and System Accreditation Boundaries

One of the most difficult and challenging problems for authorizing officials and senior agency information security officers is identifying appropriate security accreditation boundaries for agency information systems. System accreditation boundaries define the hardware, software, and other elements which make up the system. Typically, these boundaries have the same function or mission objective and essentially the same operating characteristics and security needs, and reside on the same general operating environment. Accreditation boundaries for agency information systems need to be established before conducting the initial risk assessments and developing the system security plans. Risk assessments influence the development of the security controls for information systems and generate much of the information needed for the associated system security plans. Risk assessments can be accomplished in a variety of ways depending on the specific needs of the agency.

When defining the system accreditation boundaries for its financial data warehouse, the Office of the Chief Financial Officer (OCFO) had not documented all of the system resources, such as the hardware and software, that made up the system boundaries. Without a complete list, all the associated risks to the system cannot be identified. Further, OCFO completed only an executive level risk assessment and placed reliance on the

---

<sup>2</sup>Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

Office of the Chief Information Officer's (OCIO) network to provide security for this system without ensuring that OCIO's network had been properly certified and accredited. The OCIO network was undergoing C&A at the same time and had not been formally accredited.

The Farm Service Agency (FSA) prepared its system's risk assessment with a proper technical description of the system, but had not defined the scope of the risk assessment including the system accreditation boundaries or the areas to assess.

Finally, Rural Development provided a technical description of the system, but had not defined the system accreditation boundaries, or the scope of the risk assessment. Further, the risk assessment had not described the business or technical requirements of the system.

### Baseline Security Controls

Baseline security controls provide a starting point for agencies in addressing the necessary safeguards and countermeasures required for their information systems. Common security controls should be identified during a collaborative agency-wide process with the involvement of the senior agency information system security officers, information system owners, security officer, and authorizing officials. Agencies should perform additional analyses to determine if adjustments to the baseline set of security controls are needed based on specific threats to each system.

None of the five agencies had documented the baseline security controls in the six system C&As we reviewed (see exhibit A). Rural Development documented the baseline security controls for its Program Funds Control System as "To be determined." A Rural Development official stated that its Guaranteed Loan System was developed before security was a requirement within the system development lifecycle. However, the Department had a system development lifecycle process in place that included security provisions since 1988.<sup>3</sup> Furthermore, that agency formally adopted by reference the Department's development lifecycle process in its own procedures.

Rural Development also placed reliance that its Program Funds Control System was developed using a Joint Financial Management Improvement Program (JFMIP) certified commercial product. The certification process includes consideration and evaluation of security features. While it would be correct to rely on those controls if no changes had been made to the commercial package, the Security Plan states that the system is a commercial

---

<sup>3</sup>Department Manual 3200-001, "Application System Life Cycle Management," dated March 3, 1988. (This manual has been declared obsolete as of April 5, 2005.)

product with some customization to meet selected business requirements and development of software processes to interface with required legacy systems. Because of these modifications, Rural Development needed to conduct its own testing to ensure the controls tested during JFMIP compliance were still functioning as intended.

### Security Plan

The development of system security plans is another important activity in an agency's information security programs that directly support security accreditation and are required by FISMA and OMB Circular No. A-130, Appendix III. System security plans provide an overview of the information security requirements and describe the security controls in place or planned for meeting those requirements. System security plans can include as references or attachments, other important security-related documents produced as part of an agency's information security program.

OCFO had not fully described and documented in its Mainframe Financial Data Warehouse security plan the system boundaries as well as system hardware and software component details, including vendor and licensing information. The system security plan states that a description of system components are listed in the disaster recovery plan. However, our review found that the disaster recovery plan did not have a complete and accurate listing. Additionally, the system security plan stated that service level agreements with interconnecting systems were pending, and the security plan did not include system rules of behavior.

Rural Development prepared a security plan for its Guaranteed Loan System but did not document that system's controls. While the agency did document certain security controls in its security controls compliance matrix, the documentation was inadequate for the system under review since those controls were not application specific, but rather described the general control environment within which the system operated.

The National Agricultural Statistics Service (NASS) had not documented in its Estimates Processing System security plan (1) the flow of information through the system, (2) the risk assessment methodology applied when assigning risk, (3) the physical security measures in place to protect the system, or (4) the controls in place to authorize or restrict the activities of users and system personnel with access to the system.



## Disaster Recovery Procedures

According to NIST, one of the essential elements in an effective security program is a plan and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.<sup>4</sup>

OCFO did not document several critical elements in its system disaster recovery plan including (1) roles and responsibilities of key officials during the recovery process, (2) the testing that should be performed at the alternate site before the system is ready to process transactions, (3) the specific training and testing procedures, or (4) how backup tapes and other critical material from off-site storage are sent to the recovery site. OCFO also placed reliance on another agency to re-establish system operations after a disaster is declared. To complicate matters, the listing of system hardware and software components contained in the disaster recovery plan was not complete and contained the incorrect software versions needed to restore the system's operations.

Rural Development had not documented its Program Funds Control System's architecture, location, and other critical technical considerations. The system's architecture is critical during system recovery because it documents the security devices in place to protect the data residing on the system, and describes the internal and external connections to other systems. Further, the Rural Development had not identified the specific instructions for system shutdown or the establishment of the system in a new location. Finally, Rural Development had not documented the testing that should be performed on the alternate system before its placed into operation, or that all employees should be trained in their responsibilities during a disaster.

NASS documented in its Estimates Processing System's disaster recovery plan a statement to refer to the system's trusted facilities manual for critical disaster recovery details. When we reviewed the trusted facilities manual, that document referred us back to the system's disaster recovery plan. Therefore, NASS had not documented the specifics of the disaster recovery process.

### **Recommendation No. 1**

OCIO should require the agencies to reevaluate the accreditation decision and the documentation prepared during Phase I of its C&A efforts, and ensures that the accreditation is supported by complete, accurate, and trustworthy documentation which meets the requirements of NIST and departmental guidance.

---

<sup>4</sup>NIST Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004.

**Agency Response** OCIO met with each of the agencies cited in this audit finding and agencies have said that they have documentation that verifies compliance before and after the audit. OCIO has asked the Office of Inspector General (OIG) to allow a contractor to verify the agency's evidence of compliance and validate security documentation. As part of the Department's oversight process and the post-accreditation stage of USDA's C&A policy, OCIO will also perform a detailed independent validation and verification (IV&V) of the accreditation packages of all accredited systems by September 30, 2006 to ensure that they are accurate, trustworthy, and meet the requirements of NIST and departmental policy.

**OIG Position** We concur with OCIO management decision. However, it should be noted that OCIO contracted for a similar IV&V at the same time we began our audit. Preliminary findings of that IV&V effort noted similar issues such as: (1) lack of complete documentation, (2) Plan of Actions and Milestones (POA&M) not updated with all known weaknesses, (3) inconsistency of risk ratings among the C&A documents and with OCIO's tracking system, and (4) Security Testing and Evaluation (ST&E) reports inconsistently prepared and applied.

## **Recommendation No. 2**

OCIO should develop and implement a policy that all agencies establish controls to ensure that the documentation prepared to support system accreditation is complete, accurate, reliable, and meets all NIST and other mandated documentation standards.

**Agency Response** USDA's C&A guidance will be signed into policy on September 30, 2005. This policy establishes controls to ensure that the documentation prepared to support system accreditation is complete, accurate, reliable, and meets all NIST and other mandated documentation standards. Specifically, USDA agencies must receive a required approval and concurrence from OCIO of the certification package before it can be forwarded to the designated approving authority (DAA) for an accreditation decision. OCIO will have 30 days to review the certification package for completeness, accuracy, reliability, and that it meets all NIST and USDA mandated documentation standards.

**OIG Position** We concur with OCIO management decision.

---

## Finding 2

### **Agencies Inaccurately and Inconsistently Applied System Risk Ratings**

The agencies had not applied the appropriate risk levels to their systems in accordance with NIST guidance or, in some cases, their own procedures. Further, agencies had not ensured that the risk ratings they assigned remained consistent throughout all of the C&A documents. This occurred because multiple contractors were employed to produce the various C&A documents without being privy to each other's conclusions. Further, the agencies relied on the contractors completing their documentation without effective monitoring and oversight. Without a proper risk assignment, the agencies cannot design adequate risk-based security programs to ensure the appropriate security controls are in place to protect the confidentiality, integrity, and availability of their information systems.

NIST SP 800-37 requires the security category of information systems to be determined using FIPS Publication 199, and documented in the system security plan. FIPS Publication 199 establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS Publication 199 defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). These levels are high, moderate, and low. Each agency must apply these definitions within the context of its own organization and the overall national interest.

Specific examples of misapplied and inconsistent risk levels are detailed below.

- Rural Development had its own definition for a “High” risk system as follows: “Information requires the greatest safeguards at the user level. Highly sensitive information includes critical or proprietary information, financial or grant data, and records subject to the Privacy Act.” Rural Development documented in its Program Funds Control System’s security plan that the sensitivity and criticality of the information stored within, processed by, or transmitted by the system is Privacy Act protected, unclassified data. Additionally, Rural Development documented in its Privacy Impact Assessment that the system includes customer social security or Federal tax identification numbers. Based on

its own definition, Rural Development should have rated the confidentiality for the system as “High.” However, the agency rated its system’s confidentiality as “Low.” Rural Development also inconsistently applied risk rating between its security plan and risk assessment as follows:

	<b>Security Plan</b>	<b>Risk Assessment</b>
Confidentiality	Medium	Low
Integrity	High	Medium
Availability	Medium	High

- NASS documented the risk to its Estimates Processing Systems as follows:

Confidentiality - High. Data residing on the system is considered to be sensitive but unclassified.

Integrity - High. Data must be accurate in order to maintain the integrity of the agency’s final reports.

Availability - Moderate. Both the application and data must be available to ensure the agency meets its mission and announce final reports on their announced due date.

However, NASS documented risk ratings in the same application’s Security Plan as follows: Confidentiality – Moderate; Integrity – Moderate; and, Availability – Low.

- FSA had not rated any of its systems as “High” risk, rather it rated a majority of its systems as “Moderate.” FSA rated the Guaranteed Sales Manager System we reviewed as “Moderate” but documented that the system contained sensitive information that must be protected from unauthorized, unanticipated, or unintentional modification. FSA documented that the compromise of this application or the general data could result in fraud, misallocation of funds, and access to sensitive records.
- Finally, the Agricultural Research Service (ARS), while not one of the agencies we specifically selected for review, reported all of its systems as “Low” risk. ARS operates research facilities across the country and maintains critical research data on its systems, some of which may impact the health of the American population. However, by rating its systems as low risk, the agency averted the requirement to conduct full system

accreditations, and instead conducted a less costly and more streamlined C&A process.

### **Recommendation No. 3**

OCIO should establish a policy requiring agencies to establish controls to ensure that proper risk ratings are applied to its systems.

**Agency Response** USDA's C&A guidance will be signed into policy on September 30, 2005. This policy requires agencies to use FIPS Publication 199 to determine the appropriate security categorization for the system or application and provide this determination in writing. OCIO will provide detailed training on this process and continue to provide oversight through mandatory C&A concurrence, annual security reviews, and IV&V of the Department's C&A process.

**OIG Position** We concur with OCIO management decision.

---

### **Finding 3 Security Testing and Evaluation (ST&E) Phase Did Not Yield Assurances That System Security Controls Were in Place and Operating Effectively.**

Agencies and their contractors had not conducted thorough ST&E testing to validate whether security controls were in place and operating effectively. This occurred mainly due to the stringent timeframes imposed to complete the ST&E, and the agencies' reliance on contractors without controls to ensure that contractor-provided services and deliverables were completed adequately. As a result, the accrediting official could not be assured, by an independent party, of the appropriateness and effectiveness of each system's security controls.

NIST describes how to establish and how to carry out a C&A program for computer security.<sup>5</sup> Certification consists of a technical evaluation of a sensitive application to see how well it meets security requirements. As part of the certification process, the ST&E is an independent review of the security controls in place. NIST identified four tasks in a basic ST&E: (1) are application security requirements acceptable, (2) do application security functions satisfy the requirements, (3) do the security functions exist, and (4) does the implementation method provide assurance that security functions are acceptably implemented?

---

<sup>5</sup>FIPS Publication 102, "Guideline For Computer Security Certification And Accreditation," dated September 27, 1983.

The major purpose of certification is to determine whether application safeguards satisfy security requirements. This process is only meaningful if the application has well-defined security requirements. For certification to be useful, the security requirements embedded in the application must be *examined critically* to determine whether they are reasonable and whether they comply with Federal, agency, and user requirements. Accurate, complete, and understandable security requirements are fundamental to certification. Other testing should include authentication (e.g., passwords), authorization (e.g., subject/object definition and capabilities), and security monitoring as well as proper operation, performance, and (ideally) penetration resistance of these functions. Most importantly, however, testing should establish that controls are acceptably implemented.

Just a few of the instances where we identified inadequate ST&E testing are discussed below.

- Our review of the ST&E report for Guaranteed Loan System disclosed that the ST&E team did not perform any tests on the controls internal to that specific system. The ST&E team limited testing to a review of the security plan, Trusted Facilities Manual, and interviews with Rural Development personnel.
- The ST&E team within NASS limited its tests to the use of automated vulnerability scan tools; and because of time constraints, manual assessments were based solely on the use of questions generated from the Estimates Processing System's Security Control Compliance Matrix (SCCM). The ST&E team also reviewed the Security Features Users Guide, Trusted Facilities Manual, Privacy Impact Analysis, System Security Plan, and the Initial Risk Assessment. The ST&E report does not identify any validation of controls, or processing of test transactions.
- According to Rural Development's Program Funds Control System ST&E report, the assessment team conducted an analysis of the controls listed in the System Security Plan, the findings of the Risk Assessment, and all of the controls listed in SCCM with the exception of those deemed outside the system boundary. The controls listed in the system's SCCM are general in nature and applied to all of the agency's systems. We found no evidence that specific controls related only to that system were tested.
- The ST&E team for the Animal and Plant Health Inspection Service's Agricultural Quarantine Activity System, using an automated vulnerability testing tool, identified 60 high and 15 medium risk vulnerabilities in the database application on which the system resides. Many of these vulnerabilities related to the existence of default or blank

passwords, excessive privileges assigned to non-administrator users, and the ability to authenticate users without the encryption of passwords. Despite these findings, the ST&E team inappropriately concluded that the system vulnerabilities were considered to be very low.<sup>6</sup>

- Finally, contractors employed to test FSA's Guaranteed Sales Manager System were not furnished with basic documents needed for their review. According to the ST&E report, the contractors were not furnished with a copy of the System Security Plan that documents controls in the system, or the Contingency Plan. A thorough review of controls can not be conducted without access to these documents. Further, the ST&E team conducted vulnerability scans on a segment of the general control environment that contained no components of the system under review; and deemed many of the areas of security testing, such as logical access controls, data integrity, and validation controls, as not applicable. It is doubtful that the team's findings provided any value to the accrediting official of the system being tested.

The lack of quality within the ST&E process can be further demonstrated by comparing them to agencies' POA&Ms, an OMB-required plan to address significant IT weaknesses. Rural Development reported on its POA&M, dated August 31, 2004, 56 outstanding common security control weaknesses and 183 application-specific weaknesses for its Guaranteed Loan System, some of which were identified by prior OIG audits, that would be corrected by September 30, 2005. By contrast, the ST&E team reported only 24 weaknesses in that same application, and 5 of those reported weaknesses dealt with incomplete documentation, which should have been completed prior to the ST&E, such as the security plan and Security Features Users Guide. We found no evidence to suggest that the agencies attempted to reconcile the weaknesses found in the POA&M with those identified by the ST&E team.

As of March 10, 2005, NASS reported that OIG-identified weaknesses still existed. That POA&M identified 3 system-specific weaknesses and an additional 58 general control weaknesses that materially affect its Estimates Processing System's accreditation. By contrast, the ST&E team for that system reported only one medium weakness in the system regarding the documentation of job descriptions that accurately reflect assigned duties and responsibilities and to segregate duties as necessary.

The ST&E process provides the accrediting official with assurance, through independent testing and verification, that the controls documented in the security plan and other security planning documents have been implemented

---

<sup>6</sup>We did not attempt to contact the contractor that performed the ST&E. The contractor completed their ST&E months prior to our review.

and are operating effectively with the desired results. Therefore, it is critical that the Department establish controls to ensure the quality of this process.

#### **Recommendation No. 4**

OCIO should establish a policy which requires all agencies to implement controls to ensure the ST&E process provides the level of assurance needed by the accrediting official to render an informed decision.

**Agency Response** USDA's C&A guidance will be signed into policy on September 30, 2005. This policy requires all agencies to conduct a detailed ST&E to ensure the ST&E process provides the level of assurance needed by the accrediting official to render an informed decision. It also requires agencies to develop test objectives derived from the security controls identified in Phase I. These 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. It then requires agencies to write detailed procedures to test each control or requirement.

Procedures 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. OCIO will ensure compliance to this policy through compliance reviews, C&A tracking activities, and IV&V.

**OIG Position** We concur with OCIO management decision.

#### **Recommendation No. 5**

OCIO should establish a policy which requires agencies to implement controls ensuring that all ST&E findings are included in the agency POA&Ms.

**Agency Response** USDA's C&A guidance will be signed into policy on September 30, 2005. This policy requires agencies to conduct a ST&E, document all ST&E findings that require correction, and include them in the agency POA&Ms. OCIO-Cyber Security will provide oversight to this process by identifying and tracking all agencies ST&E POA&Ms to ensure resolution or remediation.



**OIG Position** We concur with OCIO management decision.

**Recommendation No. 6**

OCIO should implement a policy and controls to perform its own sufficiency review of ST&E findings and conclusions prior to final accreditation by agency officials.

**Agency Response** USDA's C&A guidance will be signed into policy on September 30, 2005. OCIO has modified it to ensure that prior to formal submission of the certification package to the DAA, the certification officer will submit the package and all supporting documentation to the Associate Chief Information Office-Cyber Security (ACIO-CS) for a concurrence review. The ACIO-CS will perform an in-depth review 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 Interim Authority To Operation (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.

**OIG Position** We concur with OCIO management decision.

## **Section 2 – Agencies and the Department Have Not Implemented Effective Oversight and Monitoring Processes**

---

The certification and accreditation process does not occur periodically, but should be fully integrated into each system’s development lifecycle in the form of continuous monitoring and testing of controls. Agencies should establish policies over these monitoring activities and effect controls to ensure compliance with those policies. Further, the Department’s OCIO should establish processes and controls to ensure that each agency meets the requirements of the C&A process and other Federally mandated security controls, as well as maintain an accurate inventory of systems throughout the Department. Our review identified needed improvement by the agencies and OCIO in the area of continuous monitoring.

---

### **Finding 4                      Agencies Have Not Implemented Effective Oversight and Monitoring.**

Agencies had not fulfilled the requirements of full system accreditation by establishing effective configuration management or continuous control monitoring of their systems. Agencies had not adequately documented their controls over continuous system monitoring; many agencies identified weakness on their POA&M report. Further, despite continual reporting of IT weaknesses in the agencies by OIG and the U.S. Government Accountability Office, agencies have not proactively established controls to ensure they comply with Department, OMB, and NIST requirements. Finally, OCIO lacks effective policies and oversight to ensure that agencies have established effective controls. As a result, accrediting officials and system owners can not be assured that system configurations are maintained and properly controlled, and that controls are periodically tested for continued effectiveness.

According to NIST, a critical aspect of the security C&A process is the post-accreditation period involving the continuous monitoring of security controls in the information system over time. An effective continuous monitoring program requires:

- Configuration management and configuration control processes,
- security impact analyses on changes to the information system, and
- assessment of selected security controls in the information system and security status reporting to appropriate agency officials.

Agencies must recognize the importance of documenting proposed or actual changes to the information system and to subsequently determine the impact of those proposed or actual changes on the security of the system. Information systems will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the surrounding environment where the system resides. Documenting information system changes and assessing the potential impact those changes may have on the security of the system is an essential aspect of continuous monitoring and maintaining the security accreditation.

### Configuration Management

The implementation of a formal system configuration management plan is a requirement for system accreditation. Configuration management ensures, to the extent possible, that systems are configured alike to allow for testing of updates prior to implementation and expedite the mitigation of vulnerabilities. The configuration management plans we reviewed did not provide the level of detail needed to implement an effective configuration management program.

Rural Development failed to document critical elements of its Program Funds Control System's configuration management plan including the roles and responsibilities for ensuring proper configuration management execution; and the specific change control steps used to document, test, and implement system changes.

FSA did not document its configuration management plan at all. Currently, that agency reports that configuration management continues to be a weakness on its POA&M.

### Security Control Monitoring

Another critical element of the continuous monitoring process is to periodically select a subset of controls and conduct tests to ensure those controls continue to operate as intended. While this process is also one phase of the C&A process, OMB's revised Circular No. A-123, which becomes effective in fiscal year 2006, requires agencies to document and periodically test the effectiveness of their controls, especially on those systems that impact the agency's ability to produce accurate and reliable financial reporting data.<sup>7</sup>

None of the agencies (see exhibit A) had documented their procedures or processes for periodically selecting and testing controls in the systems we

---

<sup>7</sup>OMB's revised Circular No. A-123, "Management's Responsibility for Internal Control," dated December 21, 2004.

reviewed. At least two agencies, Rural Development and OCFO, reported in their POA&M that security control monitoring was an outstanding weakness.

Ensuring effective configuration management and periodic controls monitoring are essential processes in each system's life cycle, and are required for system accreditation and subsequent re-accreditations. Agency accrediting officials and system owners need to ensure that controls over configuration management and security monitoring are strictly enforced.

### **Recommendation No. 7**

OCIO must implement a policy and effective oversight to ensure that agencies implement controls over system configuration management and security controls monitoring.

#### **Agency Response**

USDA's Department Manual 3520-001, "Configuration Management Policy and Responsibilities," was approved July 17, 2004. This policy requires agencies to establish and implement a Configuration Management program that provides overall guidance and procedures for their systems. They must also create a Configuration Control Board, with an approved charter and operating procedures and provide a management plan signed by their Chief Information Officer describing the Configuration Management program they have implemented or a POA&M describing their approach to developing and implementing one. The ACIO-CS will ensure that Configuration Management Policy is implemented on all new existing information systems and networks that process classified or sensitive but unclassified information. It will also evaluate and report on agency or mission area compliance to the Chief Information Officer during periodic security reviews and evaluations including C&A.

#### **OIG Position**

While we agree with OCIO's proposed corrective actions, to reach management decision OCIO needs to provide us a summary of its planned process for ensuring that the agencies are complying with Department Manual 3520-001, "Configuration Management Policy and Responsibilities," dated July 17, 2004, and OCIO's timeframes for ensuring compliance.

---

### **Finding 5**

#### **OCIO Monitoring and Oversight Could be Strengthened.**

OCIO's methodology for tracking the status of C&A within the agencies had not met NIST guidelines and reflected C&A activities inaccurately. OCIO relied on the agencies to report timeframes and milestones without

independent verification. This resulted in the Department reporting inaccurate system accreditation percentages to OMB.

NIST requires agencies to prepare a plan of execution for their C&A activities.<sup>8</sup> This plan is to identify the appropriate resources (e.g., supporting organizations, funding, and individuals with critical skills) needed for the security certification effort, and contain specific tasks, milestones, and a delivery schedule for C&A activities. During our entrance conference, OCIO informed us that it had not required agencies to prepare a plan of execution for each of its systems. Instead, OCIO tracked the information required by the plan of execution, such as costs and timeframes, for each agency and system within the Department.

In its fiscal year 2004 FISMA report, OCIO reported, despite the lack of assurance that the C&As were performed adequately, that the U.S. Department of Agriculture (USDA) had completed certification and accreditation on 93 percent of USDA's systems. After our review of OCIO's tracking spreadsheet and consideration of the errors we found, we determined that only 86 percent of USDA systems had actually been accredited by fiscal yearend. The inaccuracies in OCIO's tracking spreadsheet made it difficult to determine the true status of the Department's C&A process.

Just a few of the inaccuracies we identified are described below.

- OCIO recorded that 9 of the 13 systems at the Food and Nutrition Service (FNS) had been accredited on September 30, 2002. Our work at FNS under another audit disclosed that FNS had not accredited any of its systems. The systems were certified, but not accredited. Certification is an attestation that security controls are in place and operating effectively. FNS' system certification did not include the ST&E process which assumes that an independent party has tested the system. Certification alone does not qualify as compliance with OMB Circular No. A-130.
- OCIO had not recorded the proper system risk rating because OCIO relied on the agencies to provide this information without adequate followup processes. We identified 47 of the 460 systems were missing an overall risk rating. Without a proper risk rating, OCIO could not ensure that systems are properly accredited in priority order.
- OCIO had not recorded all of the contractors and funding resources needed to complete the C&A efforts, once again due to its reliance on the agencies and inadequate followup processes. On the tracking spreadsheet dated September 30, 2004, we identified 89 systems where OCIO had not recorded the Phase I contractor, and 317 systems where OCIO had not

---

<sup>8</sup>NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004.

recorded the Phase II contractor.<sup>9</sup> Finally, we identified 40 and 272 systems in Phases I and II, respectively, where OCIO had not recorded any funding resources needed to complete the C&A process. In addition, OCIO had not recorded the C&A cost of either phase for 36 systems.

While we recognize that OCIO wanted to monitor the C&A process by maintaining the plan of execution, its tracking of the process was flawed and resulted in misreporting the true picture of the C&A process within the Department. OCIO should develop and implement oversight controls to ensure compliance with departmental, OMB, and NIST requirements for the C&A process.

OCIO's reliance on agency reporting of C&A information also led us to question the reliability of the Department's inventory of systems. In response to our fiscal year 2004 FISMA report, OCIO reported to have a more accurate inventory of systems within the Department. However, during our audit, OCIO requested that the agencies update its tracking system with the missing risk ratings, contractor information, and costs as noted above. OCIO presented us an updated system listing dated April 11, 2005, which contained an additional 65 systems (an increase of over 14 percent) from the tracking spreadsheet we used to select our sample of systems dated September 30, 2004. We noted in another audit currently underway that the agency combined numerous systems into one C&A. Those systems included program specific and administrative systems under different management control, different platforms, and different operating environments. OCIO informed us that they rely on the agencies to accurately report their system inventories and do not have adequate resources to verify the reported information. OCIO should establish controls to ensure that its system inventory remains up-to-date and can be reconciled with known system implementations and disposals.

## **Recommendation No. 8**

OCIO should establish procedures and controls to periodically evaluate the accuracy of information provided by the agencies.

### **Agency Response**

OCIO has made monitoring, oversight, validation, and verification of agency information a priority for the Department's security program. Beginning in 2006, OCIO will conduct a minimum of eight security reviews per year of agency security programs, continue to track and resolve POA&M from agency audits, and require agency certification packages to undergo

---

<sup>9</sup>The Department's C&A effort consisted of two phases. Phase I was the preparation of the security plan, risk assessment, and other documentation supporting the accreditation decision; and Phase II consisted mainly of the ST&E.

ACIO-CS review for concurrence before being submitted to the agency DAA.

**OIG Position**

While we agree with OCIO's proposed corrective actions, to reach management decision OCIO needs to provide us with an explanation of the controls it intends to establish to ensure that monitoring, oversight, validation, and verification, are conducted over every agency on a rotating basis; and its timeframe for implementing its controls over this process.

**Recommendation No. 9**

OCIO should establish controls to ensure the Department's inventory of systems remains up-to-date and can account for system implementations and disposals.

**Agency Response**

OCIO has established procedures to implement its Enterprise Architecture's Repository (EAR) to ensure that it has an accurate inventory of agency systems by December 31, 2005. Agencies are required to provide an accurate inventory by entering it into the EAR system. OCIO will ensure compliance by doing monthly status and updates on agency inventories, crosschecking the EAR with other processes that require systems inventories, and conducting security reviews.

**OIG Position**

We concur with OCIO management decision.

# Scope and Methodology

---

The scope of our review was nation-wide. We conducted this audit in accordance with “Government Auditing Standards.”

Fieldwork for this audit was performed in Washington D.C., and Kansas City, Missouri. Fieldwork was performed from January through June 2005.

To accomplish our audit objectives, we performed the following procedures:

- Judgmentally selected systems from OCIO’s system inventory based on risk rating, impact on the Department’s ability to prepare accurate and reliable financial statements, impact to the health or safety of the American public, and the individual contracting firms used by the agencies to complete the supporting C&A documentation. Our intent was to include critical systems and as many different contracting firms as possible.
- Reviewed security plans, risk assessments, security testing plans and results, and other documents prepared by the agencies or their contractors in support of the formal accreditation.
- Compared the content of the above documents to the requirements of departmental and other Federal guidance.
- Discussed and obtained clarification from knowledgeable agency and Department officials of the issues we identified during our review.

We originally planned to conduct a complete review of the C&A documentation supporting accreditation for 12 of the 460 systems reported by the Department’s OCIO as of September 30, 2004.<sup>10</sup> This report is based on our review of only six selected systems. (See exhibit A.) Due to the pervasive and recurring issues we identified in all six systems, and Department officials’ concurrence with our issues, we decided to discontinue fieldwork and issue our report.

---

<sup>10</sup>Due in part to our request that OCIO update some missing information on its tracking spreadsheet, the number of systems identified by the agencies and reported to OCIO increased to a total of 525 as of April 11, 2005.



## **Exhibit A – List of Agencies and Systems Reviewed**

<b>AGENCY</b>	<b>SYSTEM</b>	<b>SYSTEM DESCRIPTION</b>
Office of the Chief Financial Officer	Financial Data Warehouse – Mainframe	Financial Data Warehouse – Mainframe is a comprehensive data warehouse reporting tool which provides real-time access to key financial data for the U.S. Department of Agriculture. Financial Data Warehouse – Mainframe is an on-demand reporting application that is built upon the nightly financial extracts from the Foundation Financial Information System applications and the biweekly payroll detail for each agency.
Rural Development	Program Funds Control System (PFCS)	PFCS supports all budget, funds management, funds control and funds reporting functions required by the four large loan and grant program legacy systems of Rural Development and the Farm Service Agency (FSA). Program Funds Control System provides financial data in electronic form for posting to the existing Financial General Ledger system.
Rural Development	Guaranteed Loan System	Guaranteed Loan System is one of Rural Development's official accounting and financial management systems and supports the Guaranteed and Direct Business & Industry program, Guaranteed and Direct Community Facility program, Guaranteed Rural Rental Housing program, Guaranteed Single Family Housing program, and the Guaranteed Water & Waste program in Rural Development and also supports the Guaranteed Farm Loan Program in the FSA. Guaranteed Loan System is an online transaction entry and inquiry financial and accounting system accessed by over 1500 field offices, the national office, and finance office.
National Agricultural Statistics Service (NASS)	Estimates Processing System (EP)	The EP is responsible for the processing of agricultural statistics, statistical analysis, and the generation of reports based on these analyses. State Statistical Offices (SSO) transmits data and comments on speculative commodities to the secretary of the Agricultural Statistics Board through the NASS EP computer system. Under strict security conditions, analysts review the survey data and SSO recommendations to determine

# Exhibit A – List of Agencies and Systems Reviewed

		national and State estimates. These estimates drive market prices for speculative commodities. The Board presents its reports in printed and electronic form to the waiting public and press,
Animal Plant Health Inspection Service	Agricultural Quarantine Activity System (AQAS)	Strategic Goal 3 of USDA’s Strategic Plan is to enhance protection and safety of the nation’s Agriculture and Food Safety. Objective 3.2 related to that goal is to reduce the number and severity of agricultural pest and disease outbreaks. The Plant Protection and Quarantine (PPQ) program is responsible for intercepting and identifying agricultural pests and diseases at ports of entry throughout the United States. A family of systems, collectively called the AQAS, was developed to support the PPQ mission.
Farm Service Agency /Commodity Credit Corporation	Guaranteed Sales Manager System (GSM)	GSM is comprised of two subsystems, the Public Law (P.L.) 480 APLUS and the GSM Sales Manager sub-systems. The GSM serves as the subsidiary system program and accounting system for the FSA’s foreign guarantee programs. The GSM Web/PC is an application base system that supports both FSA and Foreign Agricultural Services (FAS). The application’s mission is to provide financial reporting to the FSA-Financial Management Division via Guaranteed Sales Manager System Data Warehouse and to provide application operation support for the FAS. The mission of P.L. 480 APLUS is to financially process loans that will provide agriculture products and equipments to underdeveloped foreign countries to assist in economic development. Through the use of the P.L. 480 APLUS, data required to verify and validate the performance indicators for food assistance for underdeveloped countries is captured. APLUS is maintained by the FSA under the auspices of the Commodity Credit Corporation and is jointly used by FSA and the FAS to provide complete financial management and accounting for this program.

# Exhibit B – Agency Response



United States  
Department of  
Agriculture

Office of the Chief  
Information Officer

1400 Independence  
Avenue SW

Washington, DC  
20250

OCT 7 2005

**TO:** Robert W. Young  
Assistant Inspector General for Audit  
Office of Inspector General

**FROM:** David M. Combs  
Chief Information Officer

**SUBJECT:** Response to Office of Inspector General (OIG) Audit #50501-4-FM  
"Review of the U.S. Department of Agriculture's Certification and  
Accreditation Efforts"

The Office of the Chief Information Officer (OCIO) has reviewed the subject audit and is providing our response. Over the past year and a half, OCIO has created processes to ensure that certification and accreditation (C&A) is included in all budgetary decision-making. A revised security policy and compliance procedures have been put in place that address the findings from this audit and ensure that agency Information Technology (IT) systems reach successful accreditation and satisfy United States Department of Agriculture (USDA) and Federal requirements for C&A. We seek acknowledgement of our program accomplishments.

We have included specific responses to each of the OIG findings and have asked for management decision for the following recommendations:

**FINDING 1: Documents Supporting Agency C&A did not Meet Federal Guidelines**

Recommendation #1: OCIO should require the agencies to reevaluate the accreditation decision and the documentation prepared during Phase I of its C&A efforts, and ensure that the accreditation is supported by complete, accurate, and trustworthy documentation, which meets the requirements of National Institute of Standards and Technology (NIST) and departmental guidance.

Agency Response: OCIO met with each of the agencies cited in this audit finding and agencies have said that they have documentation that verifies compliance before and after the audit. OCIO has asked the OIG to allow a third party auditor to verify the agency's evidence of compliance and validate security documentation. As part of the Department's oversight process and the post-accreditation stage of USDA's C&A policy, OCIO will also perform a detailed Independent Validation and Verification (IV&V) of the accreditation packages of all accredited systems by September 30, 2006 to ensure that they are accurate, trustworthy, and meet the requirements of NIST and departmental policy.

OCIO requests Management Decision for this recommendation.

Recommendation #2: OCIO should develop and implement a policy that all agencies establish controls to ensure that the documentation prepared to support system

AN EQUAL OPPORTUNITY EMPLOYER

accreditation is complete, accurate, reliable, and meets all NIST and other mandated documentation standards.

Agency Response: USDA's "C&A" Guidance will be signed into policy on September 30, 2005. This policy establishes controls to ensure that the documentation prepared to support system accreditation is complete, accurate, reliable, and meets all NIST and other mandated documentation standards. Specifically, USDA agencies must receive a required approval and concurrence of the certification package before it can be forwarded to the Designated Approving Authority (DAA) for an accreditation decision. OCIO will have 30 days to review the certification package for completeness, accuracy, reliability, and that it meets all NIST and USDA mandated documentation standards.

OCIO requests Management Decision for this recommendation.

**FINDING 2: Agencies Inaccurately and Inconsistently Applied System Risk Ratings**

Recommendation #3: OCIO should establish a policy requiring agencies to establish controls to ensure that proper risk ratings are applied to its systems.

Agency Response: USDA's "C&A" Guidance will be signed into policy by September 30, 2005. This policy requires agencies to use FIPS PUB 199 to determine the appropriate security categorization for the system or application and provide this determination in writing. OCIO will provide detailed training on this process and continue to provide oversight through mandatory C&A concurrence, annual security reviews, and IV&V of the Department's C&A process.

OCIO requests Management Decision for this recommendation.

**FINDING 3: Security Testing and Evaluation (ST&E) Phase did not Yield Assurances that System Security Controls Were in Place and Operating Effectively.**

Recommendation #4: OCIO should establish a policy, which requires all agencies to implement controls to ensure the ST&E process provides the level of assurance needed by the accrediting official to render an informed decision.

Agency Response: USDA's "C&A" Guidance will be signed into policy by September 30, 2005. This policy requires all agencies to conduct a detailed ST&E to ensure the ST&E process provides the level of assurance needed by the accrediting official to render an informed decision. It also requires agencies to develop test objectives be derived from the security controls identified in Phase 1. These 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. It then requires agencies to write detailed procedures to test each control or requirement.

## Exhibit B – Agency Response

Procedures 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. OCIO will ensure compliance to this policy through compliance reviews, C&A tracking activities, and IV&V.

OCIO requests Management Decision for this recommendation.

Recommendation #5: OCIO should establish a policy, which requires agencies to implement controls ensuring that all ST&E findings are included in the agency Plan of Action and Milestones (POA&Ms).

Agency Response: USDA's "C&A" Guidance will be signed into policy by September 30, 2005. This policy requires agencies to conduct a ST&E, document all ST&E findings that require correction, and include them in the agency POA&Ms. OCIO-Cyber Security will provide oversight to this process by identifying and tracking all agency ST&E POA&Ms to ensure resolution or remediation.

OCIO requests Management Decision for this recommendation.

Recommendation #6: OCIO should implement a policy and controls to perform its own sufficiency review of ST&E findings and conclusions prior to final accreditation by agency officials.

Agency Response: USDA's "C&A" Guidance will be signed into policy on September 30, 2005. OCIO has modified it to ensure that prior to formal submission of the certification package to the DAA, the Certification Officer will submit the package and all supporting documentation to the Associate Chief Information Office-Cyber Security (ACIO-CS) for a concurrence review. The ACIO-CS will perform an in-depth review 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 Interim Authority To Operation (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.

OCIO requests Management Decision for this recommendation.

**FINDING 4: Agencies Have Not Implemented Effective Oversight and Monitoring.**

Recommendation #7: OCIO must implement a policy and effective oversight to ensure that agencies implement controls over system configuration management and security controls monitoring.

Agency Response: USDA's DM 3520-001 Configuration Management (CM) Policy and Responsibilities was approved on July 17, 2004. This policy requires agencies to establish and implement a CM program that provides overall guidance and procedures for their systems. They must also create a Configuration Control Board, with an approved charter and operating procedures and provide a management plan signed by their Chief Information Officer describing the CM program they have implemented or a POA&M describing their approach to developing and implementing one. The ACIO-CS will ensure that CM is implemented on all new and existing information systems and networks that process Classified or Sensitive But Unclassified information. It will also evaluate and report on agency or mission area compliance to the CIO during periodic security reviews and evaluations including C&A.

OCIO requests Management Decision for this recommendation.

**FINDING 5: OCIO Monitoring and Oversight Could be Strengthened.**

Recommendation #8: OCIO should establish procedures and controls to periodically evaluate the accuracy of information provided by the agencies.

Agency Response: OCIO has made monitoring, oversight, validation, and verification of agency information a priority for the Department's security program. Beginning in 2006, OCIO will conduct a minimum of eight security reviews per year of agency security programs, continue to track and resolve POA&M from agency audits, and require agency certification packages to undergo ACIO-CS review for concurrence before being submitted to the agency DAA.

OCIO requests Management Decision for this recommendation.

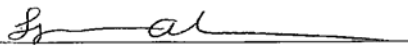
Recommendation #9: OCIO should establish controls to ensure the Department's inventory of systems remains-up-to-date and can account for system implementations and disposals.

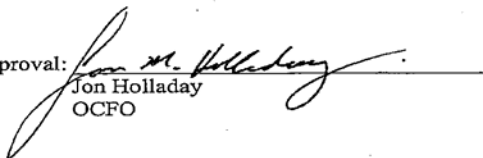
Agency Response: OCIO has established procedures to implement its Enterprise Architecture's Repository (EAR) to ensure that it has an accurate inventory of agency systems by December 31, 2005. Agencies are required to provide an accurate inventory by entering it into the EAR system. OCIO will ensure compliance by doing monthly status and updates on agency inventories, crosschecking the EAR with other processes that require systems inventories, and conducting security reviews. OCIO requests Management Decision for this recommendation.

# Exhibit B – Agency Response

If any additional information is needed, please have a member of your staff contact Kelvin O. Fairfax, OCIO-Cyber Security, Director, Programs and Evaluation, on telephone number (202) 720-2362.

cc: Jerry Williams, Deputy CIO, OCIO, Washington D.C.  
Lynn Allen, Associate CIO for Cyber Security, OCIO, Washington D.C.  
Kelvin O. Fairfax, Director, Program and Evaluations, OCIO Cyber Security  
Sherry Linkins, Management Analyst, OCIO, Washington, D.C.  
Jewel Moore, OIG, Washington, D.C.

Approval:   
Lynn Allen  
Associate Chief Information Officer  
Cyber Security

Approval:   
Jon Holladay  
OCFO