



U.S. Department of Agriculture

---



Office of Inspector General  
Northeast Region

# Audit Report

## Cooperative State Research Education and Extension Service Application Controls Review of the Cooperative Research Education and Extension Management System

Report No. 13501-01-Hy  
July 2005

---



UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250



July 8, 2005

REPLY TO

ATTN OF: 13501-01-Hy

TO: Colien Hefferan  
Administrator  
Cooperative State Research Education and Extension Service

ATTN: Louise Ebaugh  
Deputy Administrator  
Office of Extramural Programs

FROM: Robert W. Young  
Assistant Inspector General /S/  
for Audit

SUBJECT: Application Controls Review of the Cooperative Research Education and Extension Management System

This report presents the results of our Application Controls Review of the Cooperative Research Education and Extension Management System of the Cooperative State Research Education and Extension Service. Your response to the official draft, dated June 1, 2005, is included as exhibit A. Excerpts of your response and the Office of Inspector General's position are incorporated into the Findings and Recommendations section of the report. Based on your response, we were able to reach management decision on the report's 14 recommendations. Please follow your internal agency procedures for reporting final action to the Office of the Chief Financial Officer.

Please note that Departmental regulation 1720-1 requires final action to be completed within 1 year of management decision.

We appreciate the courtesies and cooperation extended to us by members of your staff during this audit.

Attachment

# ***Executive Summary***

## ***Cooperative State Research, Education, and Extension Service Application Controls Review of the Cooperative Research, Education, and Extension Management System (Audit Report No. 13501-01-Hy)***

---

### **Results in Brief**

The Cooperative State Research Education and Extension Service (CSREES), an agency of the U.S. Department of Agriculture, advances knowledge of agriculture, the environment and human health and well being by supporting research, education, and extension programs in the Land-Grant University System, and other partner organizations. CSREES does not perform actual research, education, and extension, but helps fund these programs at the State and local levels through its grant program. It monitors grant funding and conducts much of its other business by way of Information Technology (IT), principally computer applications and networks.

CSREES uses the Cooperative Research Education Extension Management System (CREEMS) to manage its grants throughout their life cycle from proposal receipt through post award review. CREEMS serves as a key application in CSREES' management of financial operations. CSREES uses the system to authorize payment of federal funds and CREEMS is the source of data entry into the agency's accounting system. We evaluated CREEMS to determine if adequate controls were in place and functioning effectively to ensure transactions were properly authorized, accurately processed, and reported.

We determined that CSREES had not complied with numerous information system security program requirements for CREEMS. The agency had not developed formal policies and procedures to govern the information security program. Specifically, we found that CSREES had not (1) documented its risk assessment, (2) prepared a comprehensive contingency plan, (3) provided annual security awareness training to all users, (4) completed the official authorization, by a designated approving agency official, to place or maintain a system in operational use, (5) implemented adequate logical and physical access controls, and (6) provided adequate legal notice regarding improper access or use of CREEMS.

CSREES management recognized that IT support was not sufficient to meet their overall business requirements. Accordingly, it reorganized the agency's IT functions by transferring all IT responsibilities into a single division. We found that many of the individuals assigned to develop and implement security policy have been with CSREES for approximately a year and that many of the policy and procedure development needs have not yet been addressed.

We used security software to scan the CSREES network that houses CREEMS. Our assessments identified 21 high and 35 medium IT security vulnerabilities. Some examples of high vulnerabilities include administrator accounts with easily guessed passwords, disabled accounts containing blank passwords, and shared accesses, which were incorrectly configured to allow access to the network. During our fieldwork, we provided CSREES with our scan results and the agency began corrective action. Additionally, we observed that CSREES did not adequately control user accounts with administrative level privileges. These security issues make CREEMS less reliable and more vulnerable to intentional or unintentional damage. As a result, the integrity, reliability, and confidentiality of the application may be jeopardized.

We also found that CREEMS and the other systems that comprise the CSREES financial management system did not use consistent calculation processes as required by Office of Management and Budget (OMB) Circular A-127, "Financial Management Systems." As a result, CSREES personnel had to perform substantial, time-consuming reconciliation and data consolidation between the systems before actually entering data into the corporate accounting system.

## **Recommendations In Brief**

We recommend that CSREES take immediate steps to mitigate identified risks to its IT resources. In particular, CSREES needs to develop and implement policies and procedures that comply with government-wide and Departmental IT security requirements. The agency should continue to monitor and resolve the high and medium risk vulnerabilities identified. Further, the agency should modify the IT components of its financial system to use the same payment allocation processes.

**Agency Response** CSREES agreed with the report's recommendations. We have incorporated excerpts from CSREES' response in the Findings and Recommendations section of this report along with the Office of Inspector General (OIG) position. CSREES' response is included as Exhibit A.

**OIG Position** Based on CSREES' response, we were able to reach management decision on the report's 14 recommendations.

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

---

CIO	Chief Information Officer
CREEMS	Cooperative Research Education Extension Management System
CSREES	Cooperative State Research Education and Extension Service
DHHS	U.S. Department of Health and Human Services
FFIS	Foundation Financial Information System
FISMA	Federal Information Security Management Act of 2002
FMFIA	Federal Managers' Financial Integrity Act
FY	Fiscal Year
IT	Information Technology
NIST	National Institute of Standards and Technology
OCFO	Office of Chief Financial Officer
OCIO	Office of Chief Information Office
OIG	Office of Inspector General
OMB	Office of Management and Budget
OO	Office of Operations
PMS	Payment Management System
USDA	U.S. Department of Agriculture

# Table of Contents

---

Executive Summary .....	i
Abbreviations Used in This Report .....	iii
Background and Objectives .....	1
Findings and Recommendations.....	3
<b>Section 1. CREEMS not in Compliance with Information System Security Program Requirements.....</b>	<b>3</b>
Finding 1    Inadequate Security and Contingency Planning for CREEMS .....	3
Recommendation No. 1.....	6
Recommendation No. 2.....	7
Recommendation No. 3.....	7
Recommendation No. 4.....	8
Recommendation No. 5.....	8
Finding 2    Access Controls Were Inadequate.....	8
Recommendation No. 6.....	11
Recommendation No. 7.....	12
Recommendation No. 8.....	12
Recommendation No. 9.....	12
<b>Section 2. Network Vulnerability .....</b>	<b>14</b>
Finding 3    CSREES Did Not Complete Sufficient Vulnerability Scans .....	14
Recommendation No. 10.....	16
Recommendation No. 11.....	16
Recommendation No. 12.....	17
Finding 4    Unneeded Access Privileges to the CREEMS Domain .....	17
Recommendation No. 13.....	18
<b>Section 3. Compliance with Laws .....</b>	<b>19</b>
Finding 5    Manual Reconciliation of CREEMS Data Required Monthly .....	19
Recommendation No. 14.....	21
Scope and Methodology.....	22
Exhibit A – Agency Response .....	23

# ***Background and Objectives***

---

## **Background**

Congress created the Cooperative State Research Education and Extension Service (CSREES) in 1994 by combining the former Cooperative State Research Service and the former Extension Service. This move united the research, education and extension portfolios of both agencies, and consolidated their expertise and resources under one leadership structure.

CSREES' mission is to advance knowledge for agriculture, the environment, human health and well-being by supporting research, education, and extension programs in the Land-Grant University System, and other partner organizations. CSREES accomplishes its mission by (1) helping States identify and meet research, extension, and education priorities that affect agricultural producers, small business owners, and youth and families; and (2) providing funding to Land-Grant Universities and competitively awarded grant funds.

CSREES provides funding to support state Agricultural Experiment Stations and the Cooperative Extension System nationwide at Land-Grant Universities. In most cases, the States are required to match the Federal formula dollars they receive with non-federal contributions. As the U.S. Department of Agriculture's (USDA) primary extramural research agency, CSREES also provides funds to researchers at institutions of higher education all over the United States.

Cooperative Research Education Extension Management System (CREEMS) manages grants throughout their life cycle from proposal receipt through post-award review. CSREES uses several systems to support the financial management of grant operations. These include CREEMS, U.S. Department of Health and Human Services (DHHS) Payment Management System (PMS) and the Foundation Financial Information System (FFIS), the USDA's corporate accounting system.

In June 1998, the Chief Financial Officer's Council released a report endorsing the use of one of three existing systems by the Federal government for grant payments by October 1, 2002. All Department of Defense organizations are to utilize the Defense Procurement Payment System. All civilian Federal departments and agencies are to use one of the following two systems: the Automated Standard Application for Payment System provided by the Financial Management Service of the U.S. Department of the Treasury or the PMS provided by the DHHS. CSREES chose to use the DHHS system.

CREEMS provides the grant payment authorization information that CSREES personnel send to PMS. The PMS makes payments to grantees. Monthly, CSREES personnel reconcile payment data from PMS and CREEMS. After

completion of the reconciliations, CSREES' staff enters CREEMS transaction data into FFIS. In Fiscal Year (FY) 2003, CREEMS authorized the disbursement of over \$1 billion of Federal funds.

Historically, CSREES units independently acquired or developed systems to fulfill their specific business needs. This disjointed approach caused compatibility issues. CSREES management recognized that Information Technology (IT) support was not sufficient to meet their overall business requirements. Accordingly, in March 2002, CSREES management created the position of Chief Information Officer (CIO) at the Deputy Administrator level. All IT staff and their responsibilities were concentrated into the Information System and Technology Management division headed by the CIO.

Improving the overall management of IT resources and information security has emerged as a top priority within the USDA. Computer security is needed because undesirable events during computer processing can have negative effects such as denial of benefits, unauthorized disclosure of sensitive information, and loss of Government money or resources.

Various laws have emphasized the need to protect agencies' sensitive and critical data, including the Privacy Act of 1974 and the Paperwork Reduction Act of 1995. Departmental responsibilities regarding information security were reemphasized in the Clinger-Cohen Act of 1996 and Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection." Additionally, the Federal Information Security Management Act of 2002 (FISMA) strengthened Federal Government information security by reauthorizing and expanding the information security, evaluation, and reporting requirements originally enacted into law as the Government Information Security Reform Act, which had expired. FISMA also directed the Department of Commerce's National Institute of Standards and Technology (NIST) to prescribe standards and guidelines pertaining to Federal information systems.

## **Objectives**

Our objective was to determine if adequate controls were in place and functioning effectively to ensure transactions were properly authorized, processed, and reported by CREEMS. Our audit included reviewing elements of security, as these controls are an integral factor for ensuring the integrity of the application's operations. Specifically, we reviewed access controls, risk assessment, contingency planning, security awareness training, and system certification procedures. As CREEMS is part of CSREES' financial management system, we also reviewed compliance with the Federal Managers' Financial Integrity Act (FMFIA).



# Findings and Recommendations

## Section 1. CREEMS not in Compliance with Information System Security Program Requirements

---

CSREES had not complied with numerous information system security program requirements. We attribute this to the fact that the agency had not developed formal policies and procedures to govern the information security program. As a result, CREEMS, a major IT application, was more at risk and less capable of recovery in the event of an accident, disaster, and intentional or unintentional event. Specifically, we determined that CSREES had not (1) documented its risk assessment, (2) prepared a comprehensive contingency plan, (3) provided annual security training to all users, (4) completed the official authorization, by a designated approving agency official, to place or maintain a system in operational use, (5) implemented adequate logical and physical access controls, or (6) provided adequate legal notice regarding improper access or use of CREEMS.

CSREES management recognized that IT support was not sufficient to meet their overall business requirements. In 2002, CSREES reorganized the agency's IT functions by transferring all IT responsibilities into a single division headed by a CIO at the Deputy Administrator level. This division has been hiring staff over the ensuing period. We found that many of the individuals assigned to develop and implement security policy have been with CSREES for approximately a year and that many of the policy and procedure development needs have not yet been addressed.

---

### Finding 1

### Inadequate Security and Contingency Planning for CREEMS

CSREES had not adequately planned for the security and continued operation of CREEMS. Security requirements have not been addressed because formal policy and procedures to implement the information security program had not been developed. As a result, the agency has not identified all risks and agency managers cannot implement controls to reduce unidentified risks. Additionally, CSREES cannot be assured that it can continue business operations or timely recover the application should any threats be realized.

OMB Circular A-130,<sup>1</sup> established a minimum set of controls to be included in automated information security programs, including performing risk assessments, establishing contingency plans and recovery procedures in the event of a disaster, establishing a comprehensive security plan, and certifying to the effectiveness of the application security controls. OMB Circular A-130<sup>2</sup>

---

<sup>1</sup> OMB Circular A-130 Appendix III Security of Federal Automated Information Resources, dated November 2000, Section A.1.

<sup>2</sup> OMB Circular A-130 Section 9 a 5.

further states that agencies must develop internal agency policies and procedures and oversee, evaluate, and otherwise periodically review activities for conformity with policies. We found that recently hired security staff were in the process of developing the policies and procedures.

### Risk Assessment

The security of a system will degrade over time, as the technology evolves and as people and procedures change. NIST 800-30<sup>3</sup> states the risk assessment is the first process in the risk management methodology. Organizations use risk assessments to determine the extent of the potential threats and the risks associated with an IT system throughout its life cycle. The output of this process helps to identify appropriate controls for reducing or eliminating risks during the risk mitigation process.

The CREEMS security plan stated that an internal risk assessment had been performed in April 2003. However, CSREES could not provide any documentation to support that the assessment was actually completed. The employee responsible for the assessment no longer works for CSREES. More significantly, without any updated documentation of risks, CSREES management cannot be assured they have taken appropriate steps to protect CREEMS.

### Contingency Plans

Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. OMB Circular A-130, Appendix III, requires managers to plan how they will perform their mission and/or recover from the loss of existing application support. Agency contingency plans should assure that there is an ability to recover and provide sufficient service to meet the minimal needs of users. We interviewed various business units about contingency planning. The units stated that without CREEMS, they doubted their ability to function or stated it would be very difficult to operate.

At the conclusion of our fieldwork in August 2004, the CREEMS contingency plan was under revision. Our review of the draft contingency plan disclosed that the plan lacked sufficient detail to ensure recovery. Although CSREES made adequate plans to store their backup tapes off-site, it did not consider the hardware or software needed to recover the system. Additionally, the plan did not list the roles and responsibilities of individuals responsible for recovery activities, identify functions needing restoration, or

---

<sup>3</sup> NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, dated October 2001, Chapter 3.

establish the priority for function restoration. As a result, CSREES cannot be assured of its ability to quickly and effectively recover CREEMS.

### Security Awareness Training

CSREES had not ensured that employees and contractors received annual security awareness training. This occurred because the agency had insufficient controls to ensure employees complied with the USDA requirement. FISMA requires awareness training to inform personnel of information security risks and their responsibilities in complying with agency policies and procedures designed to reduce these risks. OMB Circular A-130, Appendix III<sup>4</sup> requires that all individuals be appropriately trained to fulfill their security responsibilities before allowing them access to agency systems. The Circular notes that, over time, attention to security tends to dissipate, therefore, individuals should periodically receive refresher training to assure that they continue to understand and abide by the applicable rules. USDA cyber security guidance<sup>5</sup> requires awareness training be provided on an annual basis and employees acknowledge in writing the completion of annual refresher security awareness training.

We compared the list of CSREES employees who received security awareness training in FY 2003 to CREEMS users and found that 71 of 243 users (29 percent) had not taken the required training. Four of these users were IT staff and/or contractors involved with the application development. We also noted that CSREES did not maintain adequate evidence of training completion such as signed attendance logs or individual training certificates for on-line courses. CSREES personnel stated that the agency had obtained a verbal waiver from the USDA Office of the Chief Information Officer (OCIO), which authorized it to provide the training for these users in early FY 2004. We did not confirm the existence of the waiver with OCIO but observed that CSREES had not completed the required training by early FY 2004. Our review of training records through April 2004 revealed that none of the 71 users had received security awareness training. CSREES management was aware that some users had not completed the required security training and made the decision to allow continued access. Untrained users increase the risk of inadvertent or intentional damage to CREEMS because of their lower level of security awareness.

### Processing Approval Accreditation

---

<sup>4</sup> OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, dated November 2000, Section A.3.a.2.b.

<sup>5</sup> Cyber Security Guidance Memorandum 015 Guidance on Computer Security Awareness Training Programs, dated April 2002, Part 1 Section 2 and Section 3.c.6.

Processing accreditation is the official authorization, by a designated agency approving official, to place or maintain a system in operational use. It assigns the responsibility for the safe and secure operation of the system to a designated official. The accrediting official is to base the accreditation decision on facts and supporting documentation. Accreditation represents a type of quality control. OMB Circular A-130, Appendix III<sup>6</sup> requires that security accreditation be completed at least every 3 years.

The USDA OCIO's Certification and Accreditation Guidance lists two phases, (1) the pre-certification phase, and (2) the certification and accreditation phase. The pre-certification phase includes identifying existing security controls and performing an initial risk assessment. The certification and accreditation phase includes conducting the Security Test and Evaluation and forwarding the certification findings to the designated approving official for an accreditation decision. Although CREEMS was implemented in 1999, a system accreditation has not been completed.

The OCIO informed all USDA agencies that OMB had expressed interest in the accreditation process. Further, OMB had informed the Department that future funding of systems could be jeopardized for inadequate accreditation. OCIO established a deadline of September 2004 to obtain accreditation for all major USDA applications including CREEMS.

In response to the OCIO deadline, CSREES created a project group and schedule to complete the CREEMS accreditation by July 1, 2004. Due to difficulties in obtaining contractor support, the certification and accreditation was delayed. However in an April 21, 2005, meeting CSREES officials advised us that the CREEMS certification and accreditation had recently been completed.

## **Recommendation No. 1**

Develop and implement internal agency information system security program policies and controls including processes for risk assessment, contingency planning, security awareness training and system accreditation.

### **Agency Response.**

CSREES completed the Certification and Accreditation for the CREEMS application. As a result of the completion of the Certification and Accreditation of CREEMS, security policies have been reviewed and established, and the risk assessment was addressed through the development of the Risk Assessment document. Security awareness training is vigorously

---

<sup>6</sup> OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, dated November 2000, Section A.3.b.4.

pursued within the Agency as evidenced by 100 percent completion rate in 2004. The CREEMS system was accredited on March 30, 2005, and the target date for the development of a comprehensive contingency plan is July 31, 2005.

**OIG Position.**

We accept CSREES' management decision. For final action, CSREES needs to provide the Office of Chief Financial Officer (OCFO) the CREEMS processing accreditation and the comprehensive contingency plan.

**Recommendation No. 2**

Perform and document a risk assessment that meets NIST guidelines.

**Agency Response.**

CSREES performed and documented a risk assessment, following NIST guidelines, for CREEMS on October 14, 2004.

**OIG Position.**

We accept CSREES' management decision. For final action, CSREES needs to provide the OCFO the risk assessment.

**Recommendation No. 3**

Develop a contingency plan based on the risk assessment including arrangements for business operation without IT support and application recovery procedures.

**Agency Response.**

CSREES has the CREEMS application recovery contingency plan internal to the CREEMS in place. Additional work remains to be completed on a more comprehensive plan and is detailed in the Plan of Action and Milestones reported at the conclusion of the Certification and Accreditation for CREEMS. The target date for the completion and validation of a comprehensive contingency plan for CREEMS is July 1, 2005.

**OIG Position.**

We accept CSREES' management decision. For final action, CSREES needs to provide the OCFO with the comprehensive contingency plan.

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

Develop and implement procedures to suspend CREEMS access to employees who do not successfully complete required security training.

##### **Agency Response.**

CSREES has developed and documented a comprehensive policy and procedure for ensuring that all CREEMS users have completed the required security training. There is a clear escalation plan that starts with additional reminders to take the training and ends with a suspension of access to CREEMS and other Agency systems in the event that Security Training requirements are not met by Agency personnel. The security awareness training plan was issued in October 2004.

##### **OIG Position.**

We accept CSREES' management decision. For final action, CSREES needs to provide the OCFO with the security training policy.

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

Implement procedures for management monitoring to ensure the timely completion of work needed to support accreditation.

##### **Agency Response.**

CSREES completed the Certification and Accreditation process for CREEMS on March 30, 2005.

##### **OIG Position.**

We accept CSREES' management decision. For final action, CSREES needs to provide the OCFO with the CREEMS processing accreditation signed by the designated agency approving official.

---

#### **Finding 2**

##### **Access Controls Were Inadequate**

CREEMS access control settings and warning banners did not comply with Department requirements and industry best practices. This occurred because management controls had not been established to perform a periodic review of the system configuration settings and the individuals authorized access to the computer room. As a result, the application and its data were vulnerable to unauthorized access, modification, or destruction.

## Logical Access Settings

We reviewed the access settings for accounts with administrative level access privileges to the CREEMS application (program) and general CREEMS application users (all other access privilege levels). In addition, we reviewed access settings to the CREEMS domain. A domain is a group of computer and other hardware devices on a network, which are administered as a unit. The domain administrator is the most trusted user and performs functions such as updating operating system software and adding or deleting users. Operating software runs the computer, performing basic tasks such as recognizing keyboard input, tracking directories, and controlling devices such as disk drives and printers.

## General CREEMS Application

- CREEMS has no minimum password length or content requirements. NIST guidance recommends a minimum length of six characters.<sup>7</sup>
- CREEMS has no requirement to periodically change passwords. NIST recommends periodically changing passwords.<sup>8</sup>
- User sessions with no activity remained logged into the system for 150 minutes. NIST recommends termination after 30 minutes.<sup>9</sup>

## CREEMS Administrator Level Settings

- Unsuccessful login attempts are unlimited. Departmental guidance requires a limit of three unsuccessful attempts.<sup>10</sup>
- Password lifetime is unlimited. The Department specifies a maximum life of 90 days.<sup>11</sup>
- Administrative privilege users' sessions remain active (i.e., open) indefinitely. NIST recommends 30 minutes.<sup>12</sup>

## CREEMS Domain

- A password can be reused after one change. Departmental guidance requires five changes before reuse.<sup>13</sup>

---

<sup>7</sup> NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, dated September 1996, Section 3.11.4.

<sup>8</sup> Ibid

<sup>9</sup> NIST Special Publication 800-43 Systems Administration Guidance for Securing Microsoft Windows 2000 Professional Security, Computer Security, dated November 2002, Appendix B, security option 3.2.3.5.

<sup>10</sup> USDA Windows NT 4.0 Workstation Security Assessment Guide, dated 2001, Test 2, step 8.

<sup>11</sup> Ibid Test 2 step 4.

<sup>12</sup> NIST Special Publication 800-43 Systems Administration Guidance for Securing Microsoft Windows 2000 Professional Security, Computer Security, dated November 2002, Appendix B, security option 3.2.3.5.

<sup>13</sup> USDA Windows NT 4.0 Workstation Security Assessment Guide, dated 2001, Test 2, step 7.

- Account lockout duration is set to 5 minutes. The Department specifies 60 minutes.<sup>14</sup>
- Account lockout occurs after four invalid password entries. The Department specifies lockout after three invalid attempts.<sup>15</sup>
- Once logged on to the domain, sessions remain active indefinitely. NIST recommends termination of session after 30 minutes of inactivity.<sup>16</sup>

CSREES personnel informed us that the settings had not been reviewed since they were originally established during CREEMS development, which occurred in 1999. Further, they stated that CSREES had not established a policy to periodically review access configuration settings. NIST states that periodic reassessment of security is needed. NIST guidance<sup>17</sup> notes that computers and the environments in which they operate are dynamic. In particular, system data, risks, and security requirements are ever changing. NIST states that strict adherence to procedures is rare and procedures become outdated over time. These issues make it necessary to periodically reassess the security of IT systems. During the course of our fieldwork, CSREES personnel informed us that they were reviewing and updating the access settings.

#### Physical Access to CSREES Servers

CSREES did not know all persons authorized to enter its computer room. Additionally, the agency had not assessed the need for continued access. CSREES did not have a policy to perform periodic reviews of computer facility access. As a result, the computer facility that houses CREEMS is vulnerable to physical damage.

CSREES' computer room is part of USDA's Headquarters facility. USDA Office of Operations (OO) provides facilities management services and operations for all activities in and around the Washington Metropolitan Area and USDA Headquarters. This includes maintaining the electronic key access to areas within the USDA Headquarters facility.

We obtained a list of persons with access to the computer room, from OO. This list showed 70 individuals were authorized access to the computer facility. CSREES records showed only 24 individuals had access to the computer room. CSREES personnel stated that they had not established a policy to perform access reviews.

---

<sup>14</sup> Ibid, Test 2 step 9.

<sup>15</sup> Ibid, Test 2, step 8.

<sup>16</sup> NIST Special Publication 800-43 Systems Administration Guidance for Securing Microsoft Windows 2000 Professional Security, Computer Security, dated November 2002, Appendix B, security option 3.2.3.5.

<sup>17</sup> NIST Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems, dated September 1996, Section 2.7.



During our fieldwork, we provided CSREES with the OO listing for their review. CSREES personnel informed us that they could not identify 48 of the names on the OO listing but thought some may have been former contractors, construction workers or electricians. Additionally, they reported that CSREES no longer employed 8 of the 24 individuals on the computer room access list they had provided us.

During our audit, CSREES personnel reported that they had coordinated with OO and updated the computer room access. CSREES has authorized computer room access for 27 individuals.

#### Network Access Warning Banner May Not Be Legally Sufficient

Our review determined that CSREES did not provide an adequate warning banner in its introduction to the CSREES network. The lack of an adequate warning banner places CSREES at risk, since legal action for improper access or use of CREEMS will be limited because of inadequate notice.

OCIO issued required language for warning banners for all USDA networks. Our review revealed that the CSREES warning banner did not include the language required by USDA.<sup>18</sup> Specifically, the CSREES banner did not include reference to statutes and potential fines or imprisonment. Additionally, CSREES had determined to place the banner on each workstation rather than upon entry to the CSREES network. The banner installation had not been completed for all workstations.

The current security officer was unaware that the warning banners were installed at the workstation level rather than the network entry points.

### **Recommendation No. 6**

Review and modify CREEMS logical access settings for the application to meet with NIST standards, Departmental regulations and industry best practices.

#### **Agency Response.**

CSREES has revised its existing access settings for CREEMS as of December 5, 2004. The access settings are in compliance with accepted standards, regulations and best practices.

#### **OIG Position.**

---

<sup>18</sup> Cyber Security Guidance Memorandum 017 Required Language for Agency Warning Banners, dated December 2002.

We accept CSREES' management decision. For final action, CSREES needs to provide the OCFO with the revised access settings.

#### **Recommendation No. 7**

Develop and implement management controls for the CREEMS domain to ensure compliance with NIST standards and Departmental regulations, regarding configuration settings.

##### **Agency Response.**

CSREES revised the CREEMS network domain management controls on December 5, 2004, as part of the Certification and Accreditation process. The management controls implemented are consistent with Departmental regulations and NIST standards, regulations regarding best practices.

##### **OIG Position.**

We accept CSREES' management decision. For final action, CSREES needs to provide the OCFO a copy of the domain management controls.

#### **Recommendation No. 8**

Develop and implement management controls to ensure procedures are in place to periodically review computer room access privileges. The procedures should include eliminating privileges for individuals no longer needing computer room access.

##### **Agency Response.**

CSREES has developed policies and procedures, effective March 2004, to ensure that computer room access is reviewed on a periodic basis and modified as necessary. A point of contact was assigned in April 2004.

##### **OIG Position.**

We accept CSREES' management decision. For final action, CSREES needs to provide the OCFO a copy of the computer room access policies and procedures.

#### **Recommendation No. 9**

Develop and implement management controls to ensure the installation of a warning banner containing the required Departmental language at the network entry points.

**Agency Response.**

CSREES completed this requirement on December 5, 2004.

**OIG Position.**

We concur with the management decision. For final action, CSREES needs to provide the OCFO a copy of the banner and policies for banner installation.

## Section 2. Network Vulnerability

---

Our vulnerability scans disclosed weaknesses in CREEMS security administration. We found (1) a number of risk indicators that could be exploited from inside and or outside the network, and (2) individuals with administrative level access privileges, which they did not need. As a result, CREEMS is vulnerable to cyber-related attacks, jeopardizing the integrity, reliability and confidentiality of the application.

To conduct our assessment we used two commercially available software products: one designed to identify over 1,300 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Information Protocol, and the other, which tests the system policy settings of the operating system.

---

### Finding 3

### CSREES Did Not Complete Sufficient Vulnerability Scans

CSREES did not perform sufficient vulnerability scanning of the network used by CREEMS. The agency had installed the Department mandated scanning software on old equipment, which was unable to scan the entire network. Our scans of the network segment used by CREEMS disclosed a large number of risk indicators that could be exploited from both inside and outside the network. As a result, CSREES was vulnerable to cyber-related attacks, jeopardizing the integrity and reliability of the CREEMS application.

OMB Circular A-130, Appendix III<sup>19</sup> requires agencies to assess the vulnerability of information assets, identify threats, quantify the potential losses from threat realization, and develop countermeasures to eliminate or reduce the threat or amount of potential loss. Furthermore, the OCIO established a policy<sup>20</sup> that agencies regularly scan their system for known vulnerabilities using a Department purchased vulnerability-scanning tool. CSREES officials stated that the agency performed periodic scanning. However, our scans identified a large number of risk indicators.

During March 2004, we scanned<sup>21</sup> six network components, including the local area networks located in Washington, D.C. used by the CREEMS production and development environments. While our scan identified vulnerabilities, we did not attempt to determine whether the vulnerabilities have been exploited.

---

<sup>19</sup> OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources, Section B, dated November 30, 2000.

<sup>20</sup> "Cyber Security Manual" Departmental Manual 3500-2, Chapter 6, Part 1, dated April 4, 2003.

<sup>21</sup> Office of Inspector General (OIG) used the same tool specified by the OCIO.

Our scans disclosed that a developmental server contained the majority of the vulnerabilities identified. This server was located on the same network as the production environment, thereby exposing all other components in the network to potential system threats. A breakdown of the vulnerabilities identified is shown below.

	Hosts Scanned	High	Medium	Low	Total
Internal	6	21	35	46	102
External	6	0	5	0	5

High-risk vulnerabilities allow immediate remote or local access, or immediate execution of code or commands with unauthorized privileges. Medium risk vulnerabilities have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures, or low risk issues applied to major Internet components. Low risk vulnerabilities deny service or provide non-system information that could be used to formulate structured attacks on a target, but not directly gain unauthorized access.

The high-risk access vulnerabilities that threaten the CREEMS application included:

- Administrator accounts had passwords that were easy to guess. The administrator is the most trusted user of the system and can perform any function in the environment. This could allow an attacker to obtain or possibly alter the information being stored on the network.
- Disabled accounts contained blank passwords, which could enable attackers access to network resources, including the ability to take over and replace processes, and to access other computers on the network.
- The operating system had an error, which could allow an attacker to run programs including malicious code (e.g., viruses and worms) and execute arbitrary code on the system. As a result, an attacker could execute commands to freely access a system and take over or destroy any critical or sensitive data maintained on the systems.
- Shared accesses were incorrectly configured and allowed access to the entire hard drive. This could allow attackers to easily obtain or change system information and gain information about open connections with other systems. An attacker could also use this information to disable the system.

During our fieldwork, we provided CSREES with our scan results in order to permit the immediate initiation of corrective action. CSREES staff stated that

they had been unable to fully scan the CSREES network because the scanning software was installed on old equipment with limited memory. They noted that only 64 of 400 computers could be scanned at a time and that the process was “barely” completed overnight. Further, they stated that the agency had not issued any written implementation guidance for the scanning policy. In April 2004, CSREES security staff reported that the hardware with increased memory was available. They provided a scanning report, dated May 20, 2004 of the same six network components OIG had scanned. The CSREES scan disclosed 7 high, 65 medium, and 155 low vulnerabilities. OIG did not verify the results of this scan. CSREES officials attributed the increase in medium and low risk vulnerabilities to an updated version of vulnerabilities. This further demonstrates the need for regular, periodic vulnerability scanning.

### **Recommendation No. 10**

Take immediate action to correct all high and medium risk vulnerabilities identified by our vulnerability scans. Require IT officials to track each vulnerability and certify that actions have been taken to remedy the problem for all vulnerabilities identified by our scans.

#### **Agency Response.**

CSREES has developed both policies and procedures to address periodic network/system vulnerability scans. At the conclusion of each scan, the results are reviewed and addressed by the responsible groups under the direction of the CSREES security officer. Based on the latest network scan conducted on May 2, 2005, CREEMS has zero high or medium vulnerabilities.

#### **OIG Position.**

We concur with the management decision. For final action, CSREES needs to provide the OCFO a copy of the May 2, 2005, scans showing zero high and medium vulnerabilities.

### **Recommendation No. 11**

Assess low-risk vulnerabilities to identify trends and initiate actions on those areas in the aggregate that could lead to more serious vulnerabilities.

#### **Agency Response.**

At the conclusion of monthly scans, CSREES reviews all vulnerabilities and if necessary, takes action. During the review of scan results, CSREES evaluates the recurring low-risk vulnerabilities each time with the intent of eliminating them during the normal course of applying patches and software upgrades.

### **OIG Position.**

We concur with the management decision. For final action, CSREES needs to provide the OCFO a copy of the scanning policies and procedures including requirements to assess scan results.

### **Recommendation No. 12**

Prepare and implement written procedures to conduct monthly scanning of all resources within the production environment and to perform corrective action on the vulnerabilities identified.

### **Agency Response.**

CSREES completed on May 2, 2005, the policies and procedures required to support both monthly scans and action plans for any identified vulnerabilities for all environments.

### **OIG Position.**

We concur with the management decision. For final action, CSREES needs to provide the OCFO a copy of the scanning policies and procedures.

---

## **Finding 4**

### **Unneeded Access Privileges to the CREEMS Domain**

Individuals had unneeded administrative level access privileges to the CREEMS domain. CSREES' IT staffs were unaware of individual user access privileges because a policy to periodically review access had not been established. As a result, higher risks of intentional or inadvertent damage to the operating systems of the computers that house CREEMS exist.

A domain is a group of computers and other hardware devices on a network, which is administered as a unit. The domain administrator is the most trusted user and performs functions such as updating operating system software and adding or deleting users. Operating software runs the computer, performing basic tasks such as recognizing keyboard input, tracking directories, and controlling devices such as disk drives and printers. The CREEMS domain consists of seven servers, including the production and test servers, which house the CREEMS application.

OMB Circular A-130. Appendix III<sup>22</sup> states that a number of controls are

---

<sup>22</sup> OMB Circular A-130, Appendix III, Section B, November 30, 2000.

used to prevent and detect harm to systems. Controls include the use of “least privilege,” which is the practice of restricting a user's access to the minimum necessary to perform his or her job.

We used software to scan the policy settings for the CREEMS domain. The software identified 20 user accounts that had administrator level privileges for at least a portion of the CREEMS domain. We observed that one of the accounts was assigned to a person no longer employed by CSREES. Additionally, we identified two accounts that were not assigned to individuals (e.g., guest account), a condition that made it difficult to assign accountability (i.e., determine the tasks individuals performed). These results indicate CSREES did not always adequately restrict the use of the most trusted access privilege.

We provided CSREES with our scan results in order to permit a more thorough review of the accounts with administrative level privileges. In June 2004, CSREES’ staff informed us that the number of accounts with administrative privileges had been reduced to four. They stated the accounts were originally granted to individuals when CSREES was being designed and implemented. As the application is operational the number of individuals needing administrator level of access has dropped. They stated that they had not performed any access reviews prior to our audit because a review policy had not been established. We reviewed the four accounts and determined a need for access existed.

### **Recommendation No. 13**

Prepare and implement written procedures to conduct periodic reviews of CREEMS domain access privileges.

#### **Agency Response.**

As of May 2, 2005, CSREES had developed and implemented written procedures for handling domain access privileges.

#### **OIG Position.**

We concur with the management decision. For final action, CSREES needs to provide the OCFO a copy of domain access review procedures.



### Section 3. Compliance with Laws

---

#### Finding 5 Manual Reconciliation of CREEMS Data Required Monthly

Payment information within the different systems that comprise the CSREES financial management system did not agree because the systems use different processes to allocate payments. As a result, CSREES personnel perform substantial, time-consuming manual reconciliations before entering data into USDA's corporate accounting system FFIS.

The FMFIA requires each agency to establish accounting and administrative controls to permit the preparation of reliable financial reports.<sup>23</sup> Implementation instructions issued in OMB Circular A-127<sup>24</sup> require that agency financial management systems provide financial information in a timely and useful fashion. The Circular defines an integrated financial system as a unified set of financial systems and the financial portions of mixed systems<sup>25</sup> necessary to manage agency financial operations. Financial management includes reporting the agency's financial status to central agencies, Congress, and the public. Further, the Circular requires that common processes shall be used for processing similar kinds of transactions throughout the system to enable the transactions to be reported in a consistent manner.

CSREES uses several systems to manage and account for grant operations. These include CREEMS, the PMS operated by DHHS and FFIS. CREEMS functions include authorizing grant payments and providing the obligation and disbursement data, which CSREES personnel enter into FFIS. CREEMS provides the grant payment authorization information that CSREES personnel enter into PMS. The PMS makes payments to grantees. Annually PMS processes over 5,000 payments disbursing in excess of \$1 billion for CSREES. FFIS is USDA's corporate administrative financial management information system implemented by the USDA OCFO.

CSREES officials stated that CREEMS had not been reviewed for compliance with Federal financial reporting requirements since it was not a financial system. They stated CSREES used FFIS as their accounting system as required by the OCFO. We concluded that the CREEMS is a "mixed system," as defined by OMB Circular A-127, because it is the source of financial data entered into FFIS. Our review revealed that CSREES' financial management systems did not comply with the requirements regarding standardized

---

<sup>23</sup> FMFIA (P.L. 97-255) Section 1.

<sup>24</sup> OMB Circular A-127 Financial Management Systems dated July 1993, Section 7.e.

<sup>25</sup> Mixed system means an information system that supports both financial and non-financial functions.

processing among system components or timely reporting of financial information.

PMS allocates the usage of funds differently than CREEMS in certain instances. These cases involve grants funded from different budget authorities or where funding authority is for more than 1 year. For example, as shown in the following table, in a case where both 1 year<sup>26</sup> and multiple years' sources funded a grant, CREEMS applies all payments to 1 year funding source first. In contrast, PMS applies payments on a pro rata basis, which is the percentage that 1 year funding represents of the total grant.

Assume a \$30,000 grant funded as follows with an initial funds distribution of \$1,500.		
Funded from appropriations available for 1 year		\$ 10,000
Funded from appropriations available for 2 years		\$ 20,000
Allocation of Funds		
	CREEMS	PMS
1 year funding	\$1,500	\$ 500
2 years funding	\$ 0	\$1,000

Prior to data entry into FFIS, CSREES personnel reconcile the payment data between CREEMS and PMS. Additionally, they perform manual consolidation of data for entry into FFIS. This is a labor-intensive process that takes considerable time. For example, we observed that it took 5 weeks, until April 8, 2004, to enter \$56 million of February 2004 research grant expenditures into FFIS. CSREES personnel stated delays of this nature occur every month for the research grants.

OMB established November 15, 2004, as the due date for the annual performance and accountability report, which includes the USDA consolidated financial statements. OCFO issued a schedule of financial management milestones stating that the USDA consolidated statements would be submitted for auditor review by October 28, 2004.

A 5 week delay in FFIS data entry for September's activities would result in some CSREES transactions not being included in the financial statements. Accordingly, CSREES personnel stated they had to provide an estimate rather than actual data for a portion of September transactions. The use of estimates rather than actual transaction data increases the risk of misstatement in financial reporting. Misstatement may arise from using inadequate data or

<sup>26</sup> One year funding must be used within the federal FY the grant was authorized.

inappropriate estimation methods. The estimate for CSREES transactions was well below the materiality level<sup>27</sup> established for the USDA consolidated financial statements, therefore, OIG did not modify its opinion on the FY 2004 financial statements. However, we concluded that as of September 30, 2004, the CSREES financial management system was not in compliance with the FMFIA because of the inconsistent processing procedures used by the financial system components. CSREES officials informed us that, as of April 2005, they are working to ensure that CREEMS and PMS use the same allocation methodology and the noncompliance will be eliminated by July 1, 2005.

#### **Recommendation No. 14**

Modify the financial management systems to ensure that all components use the same payment allocation processes.

#### **Agency Response.**

CSREES has been working with the DHHS-PMS staff to change the allocation methodology used by the DHHS-PMS (to correspond with the allocation methodology used by CREEMS) to process payments when multiple financial data codes and Treasury Symbols are involved. CSREES Funds Management and CREEMS staff met with the DHHS-PMS staff on May 2, 2005, to review the results of a pilot test, implementing the new allocation methodology. The target date for implementation of the new allocation methodology by the DHHS-PMS for CSREES grants is June 30, 2005.

#### **OIG Position.**

We concur with the management decision. For final action, CSREES needs to provide the OCFO a copy of the revised allocation procedures and evidence of implementation by DHHS.

---

<sup>27</sup> The magnitude of an item's omission or misstatement in a financial statement that, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item.

# ***Scope and Methodology***

---

Our review was part of a nationwide audit of seven USDA agencies with major applications. Systems were selected from a USDA OCIO prepared listing of 123 major systems. We reviewed controls established by CSREES to ensure that the CREEMS application transactions were properly authorized, processed and reported. We conducted our review at the CSREES Headquarters located in Washington, D.C. We reviewed the controls in place at the time of our audit. We conducted our review through interviews, review of CSREES procedures and records, examination of CREEMS system settings, and by observation. We used commercially available software applications to assist us in our review. We identified vulnerabilities in CREEMS, but did not perform tests to determine whether the vulnerabilities had been exploited.

To accomplish our audit objectives, we:

- Reviewed agency, Departmental, and other federally mandated IT security policies and procedures;
- Interviewed CSREES officials responsible for managing the agency's IT systems;
- Interviewed CREEMS users throughout CSREES;
- Performed vulnerability scans on the CREEMS domain networks using commercially available operating system vulnerability software; and
- Performed detailed testing of CREEMS system settings and application security controls.

Audit fieldwork was performed from March 2004 through August 2004. The audit was conducted in accordance with Generally Accepted Government Auditing Standards.

# Exhibit A – Agency Response

Exhibit A - Page 1 of 6



United States  
Department of  
Agriculture




Cooperative State  
Research, Education,  
and Extension Service

Washington, DC  
20250-2200

JUN 1 2005

TO: Robert W. Young  
Assistant Inspector General for Audit

FROM: Colien Hefferan   
Administrator

SUBJECT: Draft Audit Report No. 13501-01-Hy – Application Controls Review for the  
Cooperative Research Education and Extension Management System

This is in response to your May 16, 2005, memorandum requesting our written response to the official draft of the subject audit, specifying corrective actions taken or planned on each audit recommendation and proposed completion dates for implementing such actions.

The Cooperative State Research, Education, and Extension Service (CSREES) has, since the completion of the U.S. Department of Agriculture (USDA) Office of Inspector General (OIG) fieldwork, successfully conducted and completed a Certification and Accreditation for all its major systems including the Cooperative Research, Education and Extension Management System (C-REEMS). The process of preparing for and the actual conduct of the Certification and Accreditation, in and of itself, addressed many of the findings and recommendations outlined in the audit report.

In addition to the Certification and Accreditation evaluation process conducted since the audit, the C-REEMS project team has fully implemented a new hardware infrastructure along with significant software conversions and upgrades that further contribute to the general security and integrity of the system.

The entire software infrastructure required to support the C-REEMS application is now hosted on a separate sub net within the overall CSREES network infrastructure. The segregation of C-REEMS servers on the sub net allows for greater control over the network traffic that passes through the C-REEMS environments. The hardware purchased has allowed for the development of separate development, testing and production environments. These separate environments support a more disciplined approach to applications development as well as providing enhanced ability to test operating system and application security patches.

The overall operating system environment for the C-REEMS servers was converted from a Microsoft Windows platform to Red Hat Linux, Enterprise edition. There are several significant advantages to be achieved by this conversion. The Linux operating system is generally less

vulnerable to software viruses, worms and other disruptive events to the system's performance. The Linux operating system provides a better mechanism for standardizing its installation on the server.

Attachment A includes our responses to the 14 recommendations under the five audit findings. CSREES has completed corrective action on 11 of the 14 recommendations and plans to complete corrective action on the remaining three recommendations by July 31, 2005. Below is our response to your overall recommendation in the "Executive Summary":

*Recommendation in Brief: We recommend that CSREES take immediate steps to mitigate identified risks to its IT resources. In particular, CSREES needs to develop and implement policies and procedures that comply with governmentwide and Departmental IT security requirements. The agency should continue to monitor and resolve the high and medium risk vulnerabilities identified. Further, the agency should modify the IT components of its financial system to use the same payment allocation processes.*

Agency Response: CSREES had completed the Certification and Accreditation process for C-REEMS on March 30, 2005. CSREES will complete and validate the comprehensive contingency plan for C-REEMS by July 31, 2005. The Department of Health and Human Services-Payment Management System (DHHS-PMS) payment allocation process will be modified to reflect the same payment allocation process used in C-REEMS.

CSREES appreciates the audit work conducted by the OIG auditors as their efforts have improved and will contribute to CSREES management of information technology resources and processes as well as financial management. Questions regarding this memorandum can be directed to Jon Kavalauskas, Oversight Staff, on (202) 401-4313.

**Cooperative State Research, Education, and Extension Service (CSREES) Response  
to the May 16, 2005, Draft USDA Office of Inspector General  
Audit Report No. 13501-01-Hy: Application Controls Review for  
the Cooperative Research Education and Extension Management System (C-REEMS)**

**Section 1. C-REEMS not in Compliance with Information System Security Program  
Requirements**

**Finding 1. Inadequate Security and Contingency Planning for C-REEMS**

**Recommendation 1:** *Develop and implement internal agency information system security program policies and controls including processes for risk assessment, contingency planning, security awareness training and system accreditation.*

**Agency Response:**

CSREES completed the Certification and Accreditation for the C-REEMS application. As a result of the completion of the Certification and Accreditation of C-REEMS, security policies have been reviewed and established, and the risk assessment was addressed through the development of the Risk Assessment document. Security awareness training is vigorously pursued within the Agency as evidenced by the 100 percent completion rate in 2004. The C-REEMS system was accredited on March 30, 2005, and the target date for the development of a comprehensive contingency plan is July 31, 2005.

**Recommendation 2:** *Perform and document a risk assessment that meets NIST guidelines.*

**Agency Response:**

CSREES performed and documented a risk assessment, following NIST guidelines, for C-REEMS on October 14, 2004.

**Recommendation 3:** *Develop a contingency plan based on the risk assessment including arrangements for business operation without IT support and application recovery procedures.*

**Agency Response:**

CSREES has the C-REEMS application recovery contingency plan internal to C-REEMS in place. Additional work remains to be completed on a more comprehensive plan and is detailed in the Plan of Action and Milestones reported at the conclusion of the Certification and Accreditation for C-REEMS. The target date for the completion and validation of a comprehensive contingency plan for C-REEMS is July 1, 2005.

**Recommendation 4:** *Develop and implement procedures to suspend C-REEMS access to employees who do not successfully complete required security training.*

**Agency Response:**

CSREES has developed and documented a comprehensive policy and procedure for ensuring that all C-REEMS users have completed the required security training. There is a clear escalation plan that starts with additional reminders to take the training and ends with a suspension of access to C-REEMS and other Agency systems in the event that Security Training requirements are not met by Agency personnel.

**Recommendation 5:** *Implement procedures for management monitoring to ensure the timely completion of work needed to support accreditation.*

**Agency Response:**

CSREES completed the Certification and Accreditation process for C-REEMS on March 30, 2005.

**Finding 2. Access Controls Were Inadequate**

**Recommendation No. 6:** *Review and modify C-REEMS logical access settings for the application to meet with NIST standards, Departmental regulations and industry best practices.*

**Agency Response:**

CSREES has revised its existing access settings for C-REEMS as of December 5, 2004. The access settings are in compliance with accepted standards, regulations and best practices.

**Recommendation No. 7:** *Develop and implement management controls for the C-REEMS domain to ensure compliance with NIST standards and Departmental regulations, regarding configuration settings.*

**Agency Response:**

CSREES revised the C-REEMS network domain management controls on December 5, 2004, as part of the Certification and Accreditation process. The management controls implemented are consistent with Departmental regulations and NIST standards, regarding configuration settings.

**Recommendation No. 8:** *Develop and implement management controls to ensure procedures are in place to periodically review computer room access privileges. The procedures should include eliminating privileges for individuals no longer needing computer room access.*



**Agency Response:**

CSREES has developed policies and procedures to ensure that computer room access is reviewed on a periodic basis and modified as necessary.

**Recommendation No. 9:** *Develop and implement management controls to ensure the installation of a warning banner containing the required Departmental language at the network entry points.*

**Agency Response:**

CSREES completed this requirement on December 5, 2004.

**Section 2. Network Vulnerability**

**Finding 3. CSREES Did Not Complete Sufficient Vulnerability Scans**

**Recommendation No. 10:** *Take immediate action to correct all high and medium risk vulnerabilities identified by our vulnerability scans. Require IT officials to track each vulnerability and certify that actions have been taken to remedy the problem for all vulnerabilities identified by our scans.*

**Agency Response:**

CSREES has developed both policies and procedures to address periodic network/system vulnerability scans. At the conclusion of each scan, the results are reviewed and addressed by the responsible groups under the direction of the CSREES security officer. Based on the latest network scan conducted on May 2, 2005, C-REEMS has zero High or Medium vulnerabilities.

**Recommendation 11:** *Assess low-risk vulnerabilities to identify trends and initiate actions on those areas in the aggregate that could lead to more serious vulnerabilities.*

**Agency Response:**

At the conclusion of monthly scans, CSREES reviews all vulnerabilities and if necessary, takes action. During the review of scan results, CSREES evaluates the recurring low-risk vulnerabilities each time with the intent of eliminating them during the normal course of applying patches and software upgrades.

**Recommendation 12:** *Prepare and implement written procedures to conduct monthly scanning of all resources within the production environment and to perform corrective action on the vulnerabilities identified.*

**Agency Response:**

CSREES completed on May 2, 2005, the policies and procedures required to support both monthly scans and action plans for any identified vulnerabilities for all environments.

**Finding 4. Unneeded Access Privileges to the C-REEMS Domain**

**Recommendation 13:** *Prepare and implement written procedures to conduct periodic reviews of C-REEMS domain access privileges.*

**Agency Response:**

As of May 2, 2005, CSREES had developed and implemented written procedures for handling domain access privileges.

**Section 3. Compliance with Laws**

**Finding 5. Manual Reconciliation of C-REEMS Data Required Monthly**

**Recommendation No. 14:** *Modify the financial management systems to ensure that all components use the same payment allocation processes.*

**Agency Response:**

CSREES has been working with the Department of Health and Human Services' Payment Management System (DHHS-PMS) staff to change the allocation methodology used by the DHHS-PMS (to correspond with the allocation methodology used by C-REEMS) to process payments when multiple financial data codes and Treasury Symbols are involved. CSREES Funds Management and C-REEMS staff met with the DHHS-PMS staff on May 2, 2005, to review the results of a pilot test, implementing the new allocation methodology. The target date for implementation of the new allocation methodology by the DHHS-PMS for CSREES grants is June 30, 2005.