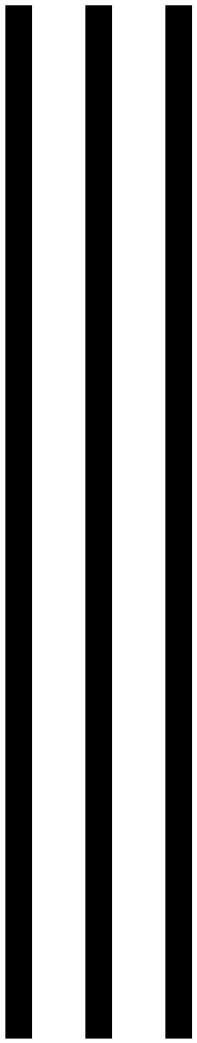

U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

AGRICULTURAL RESEARCH SERVICE SECURITY OVER THE AGRICULTURAL RESEARCH SERVICE'S INFORMATION TECHNOLOGY RESOURCES

Report No.
02099-1-FM

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: December 4, 2001

REPLY TO
ATTN OF: 02099-1-FM

SUBJECT: Security Over the Agricultural Resource Service's Information Technology Resources

TO: Floyd P. Horn
Administrator
Agricultural Research Service

This report presents the results of our audit of the security over information technology resources within the Agricultural Research Service (ARS) as of May 2001. Your written response to the draft report was considered in finalizing the report and is attached as Exhibit A. We concur with the proposed corrective actions but we cannot reach management decision on Recommendation Nos. 6 and 7 until we are provided timeframes for implementation of the cited actions.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days providing the timeframes for implementing the proposed actions for each of the above cited recommendations. Please note the regulation requires that management decision be reached on all findings and recommendations within a maximum of 6 months from report issuance.

We appreciate the cooperation and courtesies extended to our auditors during the audit.

/s/

RICHARD D. LONG
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

SECURITY OVER THE AGRICULTURAL RESEARCH SERVICE'S INFORMATION TECHNOLOGY RESOURCES AUDIT REPORT NO. 02099-1-FM

RESULTS IN BRIEF

We identified numerous and significant weaknesses in the Agricultural Research Service's (ARS) ability to adequately protect its information technology (IT) resources from potential disruptions. Significant IT security related weaknesses were found at each of the ARS sites visited. This included vulnerabilities related to ARS' IT equipment and networks. Our vulnerability scans disclosed weaknesses in ARS' system security administration. Specifically we found that scans of selected ARS systems disclosed a large number of risk indicators that could be exploited, and that system policy settings varied significantly from industry "best practices" which increased the potential risk to the agency. We attributed this condition to the absence of a standard security policy in place to protect the agency's networks. As a result, ARS' systems and networks are vulnerable to cyber-related attacks, jeopardizing the integrity and reliability of its data systems. ARS is committed to resolving the various security issues identified and has initiated actions to resolve the vulnerabilities we reported.

We also noted that ARS needs to establish a formal methodology for determining the type and extent of business continuity and contingency planning that is needed at various levels of the agency. None of the ARS sites we reviewed had a business continuity and contingency plan in place to ensure the continuity of operations in the event of a disaster or an interruption in services, nor did all of the sites use an offsite storage site for their critical files. ARS did identify the need for assessing risk and developing contingency plans in its fiscal year (FY) 2002 Capital IT Plan. This plan stated: "The goal of the program is to develop and implement cost effective solutions to emerging security threats, problems, and issues. Emphasis will be placed on security awareness and training, risk assessment, risk mitigation strategies, contingency planning, and network security." While ARS has been strengthening its coverage and direction of IT security, it needs to move more rapidly to assure ARS service units can continue processing in the event of unplanned disruptions. As a result, ARS has no assurances that it could continue processing its critical applications in the event of a disaster or interruption in services.

To test the vulnerability of ARS to the threat of security intrusions, we conducted an assessment of selected sites' networks, using commercially available software products, which are designed to identify risk indicators associated with various operating systems. Our assessments, using one such product, identified over 350 high and medium IT security vulnerabilities at the 9 sites reviewed. In addition, we identified numerous low risk vulnerabilities, many of which, while not critical to system security, can be an indication of systems administration problems. The results of our reviews were provided for corrective actions to agency management in two Management Alerts dated October 17, 2000, and May 30, 2001. ARS officials indicated they would take immediate corrective action on our Management Alerts.

The ARS has requested waivers from the U.S. Department of Agriculture (USDA) Office of Chief Information Office (OCIO) for 58 of its units to use non-USDA Internet Service Providers (ISP) (i.e., any non-USDA ISP such as a University or commercial ISP provider) Network. However, we found that the security plans for 6 of the 58 units we reviewed were neither complete nor had the units entered into a service level agreement with the non-USDA ISP to establish minimum security requirements. Departmental Regulations require an agency to ensure that security controls provided by a non-USDA ISP be adequate prior to the agency requesting a waiver from the USDA's OCIO.

We believe that in aggregate the IT Security Control weaknesses discussed in this report constitute a material control weakness as defined in the Federal Managers' Financial Integrity Act and should be included in the agency's FY 2002 report unless corrected.

KEY RECOMMENDATIONS

We recommended that ARS take appropriate immediate action to address the conditions noted, including the following:

- Ensure all necessary corrective actions are completed on all high and medium risk vulnerabilities identified during the audit.

- Establish and document a minimum set of security standards for all ARS field sites using industry "best practices."

- Conduct periodic assessments to ensure field office compliance with ARS internal security requirements.

- Prepare comprehensive and system specific contingency plans that address protection of information resources and recovery procedures, including the requirements for offsite storage of critical files, in the event of service disruptions and to include a description of these plans in each ARS sites' security plans.

- Ensure that Departmental Requirements regarding security are met for any Internet access waiver requests submitted.

AGENCY RESPONSE

The ARS agreed with the findings and recommendations and proposed corrective actions which adequately address each of the reported issues.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The Agricultural Research Service (ARS) is the principle inhouse research agency of the U. S. Department of Agriculture (USDA) and is one of the four component agencies of the Research, Education and Economics mission area. ARS conducts research to develop and transfer solutions to agricultural problems of high national priority and provides information access and dissemination to:

- Ensure high-quality, safe food and other agricultural products;
- assess the nutritional needs of Americans;
- sustain a competitive agricultural economy;
- enhance the natural resource base and the environment; and
- provide economic opportunities for rural citizens, communities, and society as a whole.

Effective July 2000, ARS created a Chief Information Officer (CIO) position and staff to plan and coordinate agency IT programs and activities, establish agency IT policies and standards, and implement an agency IT architecture. The ARS CIO organization works closely with senior program managers and staff in developing IT strategies to enhance mission performance, communications, and information management. In addition, the CIO organization works to make the most effective use of IT resources, establish meaningful performance measures for IT, and ensures compliance with departmental and governmental IT policies and regulations.

OBJECTIVES

Our primary audit objectives were to (1) determine if ARS had adequate security measures in place to protect sensitive data against cyber based penetration attempts; (2) determine if ARS had identified and prioritized critical data and operations and taken steps to prevent and minimize potential damage and interruption from unexpected interruptions; and (3) determine if ARS had received any waivers from the USDA Office of Chief Information Office (OCIO) to use non-USDA Internet Service Provider's (ISP) and whether the waiver requests were adequately justified and appeared reasonable.

SCOPE

This audit was conducted in accordance with generally accepted government auditing standards. We performed this audit at various sites within ARS. Our audit was performed during the period of August 2000 through May 2001.

METHODOLOGY

To accomplish our audit objectives, our examination consisted of the following:

- Reviewed IT policies and procedures relating to various security aspects of the ARS;
- interviewed responsible ARS security officials and other personnel responsible for managing IT resources;
- included vulnerability scans of various servers, routers, switches, fire walls and network servers;
- reviewed departmental and agency security procedures and directives;
- reviewed disaster recovery and contingency planning efforts applicable to the sites visited; and
- reviewed waiver requests and the supporting documentation.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	VULNERABILITIES EXPOSE ARS SYSTEMS TO THE RISK OF MALICIOUS ATTACKS

FINDING NO. 1

Our vulnerability scans disclosed weaknesses in ARS' system security administration. Specifically we found that scans of selected ARS systems disclosed a large number of risk indicators that could be exploited, and that system policy settings varied significantly from industry "best practices" which increased the potential risk to the agency. We attributed this condition to the absence of a standard security policy in place to protect the agency's networks. As a result, ARS' systems and networks are vulnerable to cyber-related attacks, jeopardizing the integrity and reliability of its data systems.

To conduct our assessment we used two commercially available software products – one designed to identify over 700 vulnerabilities associated with various operating systems that use Transmission Control Protocol/Information Protocol (TCP/IP),[1] and the other which tests system policy settings in the networks.

TCP/IP System Vulnerabilities

We conducted our vulnerability scans at various sites within ARS. Our assessments revealed over 350 high and medium risk vulnerabilities. We reported the weaknesses found at each location directly to agency management and corrective actions were initiated during our review. In addition, we identified over 2,300 low risk vulnerabilities, many of which, while not critical to system security, can be an indicator of the need for better system administration.

We found that at three of the sites visited, firewalls were in place between the sites and the non-USDA ISP. Our scans showed that the firewalls effectively protected the sites from outside penetration attempts. However, at these three sites, we did identify 84 high vulnerabilities and 74 medium vulnerabilities based upon our assessment of security inside

[1] TCP/IP, the suite of communication protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks.

the firewall. In addition, at six other sites visited adequate operational protection was not in place.

A breakdown of the vulnerabilities identified is shown below:

	High Risk	**Medium Risk**	**Low Risk**	**Total**
Site 1	3	12	139	154
Site 2	81	43	741	865
Site 3	1	27	332	360
Site 4	1	18	393	412
Site 5	0	8	422	430
Site 6	3	8	33	44
Site 7	3	48	117	168
Site 8	2	4	28	34
Site 9	7	86	119	212
TOTAL	101	254	2,324	2,679

These vulnerabilities, if left uncorrected could allow unauthorized users access to critical and sensitive ARS programs and systems. We met with ARS officials to discuss the results of our assessments and the procedures necessary to mitigate the vulnerabilities found. They concurred with our findings and are actively working to correct the vulnerabilities identified.

Selected Server Operating System Software

We conducted an assessment of the security of selected server operating system software at two of the sites visited. Our assessment software allowed us to compare ARS' security practices to the actual settings on the software. We were also able to compare the system's settings to the software product's "best practices[3]", which are based on standard practices from a wide variety of government and private institutions. We also compared ARS' internal security policies to those same "best practices." The software product identified weaknesses that may leave the operating system open to potential threats.

Our assessments disclosed that the majority of the weaknesses were in system monitoring, data integrity and data confidentiality areas. Weaknesses were found in numerous areas when the system's security standards were compared to industry "best practices" settings.

[3] The "best practices" are derived from the commercial software vendors proprietary methodology and extensive network, mainframe, and minicomputer studies. The "best practices" are continually updated based on the ongoing research of security professionals responsible for the networks of corporations and government agencies.

We also found that ARS does not have a minimum set of security standards applicable to each of its sites. ARS' headquarters provided us with an informal set of internal security standards which were subsequently verbally added to during our review. At another office, there were no written internal security standards. Instead, we were provided a template screen print of the security standards in use. In addition, the internal security standards in place at both sites varied considerably from the industry "best practices" provided with the software package. The results of our scans were provided to ARS management in two Management Alerts dated October 17, 2000, and May 30, 2001. In written replies to the two Management Alerts, ARS stated that they were taking immediate action to correct the cited vulnerabilities.

RECOMMENDATION NO. 1

Ensure all necessary corrective actions are completed on all high and medium risk vulnerabilities identified during our audit, including the vulnerabilities identified for the server software.

Agency Response

The ARS agreed with the recommendation and stated that systems administrators have taken action to correct all high and medium vulnerabilities.

OIG Position

We concur with the management decision

RECOMMENDATION NO. 2

Revise the ARS internal security standards to bring them in line with industry "best practices," or document why these practices do not apply to ARS. Establish and document a minimum set of security standards for all ARS servers.

Agency Response

The ARS agreed with the recommendation and plans to develop and implement an agency configuration management policy, which would expand on the Department-wide configuration management framework and policy. The planned completion date is June 30, 2002.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 3

Conduct periodic assessments to ensure field office compliance with ARS internal security requirements.

Agency Response

The ARS agreed with the recommendation and plans to develop and implement an agency security assessment policy identifying responsibilities, procedures, schedules, and controls for conducting internal security reviews, security plan reviews, and vulnerability scans. The ARS has purchased security software and has been training personnel in its use. The planned completion date for the proposed actions is June 30, 2002.

OIG Position

We concur with the management decision.

CHAPTER 2	ARS NEEDS TO ENSURE ITS SITES HAVE ADEQUATE BUSINESS CONTINUITY AND CONTINGENCY PLANS IN PLACE

FINDING NO. 2

ARS needs to establish a formal methodology for determining the type and extent of business continuity and contingency planning that is needed at various levels of the agency. In general, the ARS sites we reviewed did not have business continuity and contingency plans in place to ensure the continuity of operations in the event of a disaster or an interruption in services, nor did all of the sites use an offsite storage site for their critical files. ARS did identify the need for assessing risk and developing contingency plans in its FY 2002 Capital IT Plan. This plan stated: "The goal of the program is to develop and implement cost effective solutions to emerging security threats, problems, and issues. Emphasis will be placed on security awareness and training, risk assessment, risk mitigation strategies, contingency planning, and network security." While ARS has been strengthening its coverage and direction of IT security, it needs to move more rapidly to assure ARS service units can continue processing in the event of unplanned disruptions. As a result, ARS has no assurances that it could continue processing its critical applications in the event of a disaster or interruption in services.

OMB Circular No. A-130, Security of Federal Automated Information Resources, dated February 8, 1996, Appendix III, provides minimum controls to be included in Federal automated information security programs. Under Continuity of Support it states: "Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system."

Our review of the security plans prepared for each of the sites visited disclosed that, in the section entitled "Contingency Planning", the plans generally addressed the backup procedures in place for the local file systems but did not address alternate processing sites or the types of disasters which could impact on local operations. The plans also neither identified the critical applications nor the risks involved if these applications were not available for processing. For example, the security plan for one site stated: "There are no formal emergency, disaster, or contingency plans."

The absence of these plans is especially critical since ARS officials noted: "The administrative, financial, and personnel databases on the system contain information that must be available on the system and contain information that must be available on a timely basis to meet mission requirements and/or to avoid substantial losses." We also found that each site ranked as "High", at least one component of their general support system as handling sensitive information requiring protection to assure its integrity, availability, or confidentially.

We further found that the ARS sites were inconsistent in their use of an offsite storage facility for their critical files. Of the nine sites visited four were not storing their critical files offsite. In the case of a disaster or an interruption in service, these sites may not be able to continue processing unless their critical files are retrievable from a remote site.

Contingency planning directly supports an organization's goal of continued operations and addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. As noted above, ARS has stated that the information on its systems is critical and must be available to meet the agency's mission.

RECOMMENDATION NO. 4

Prepare comprehensive and system specific contingency plans that address protection of information resources and recovery procedures, including the offsite storage requirements, in the event of service disruptions. Include a description of these plans in each sites' security plans.

Agency Response

The ARS agreed with the recommendation and anticipates development and implementation of continuity and contingency policy and procedures by June 1, 2002. Agency systems will be prioritized and a timetable will be established to ensure that continuity and contingency plans for the most critical agency systems are developed and tested.

OIG Position

We accept the management decision.

CHAPTER 3	ARS NEEDS TO ENSURE ADEQUATE SECURITY AT SITES USING NON-USDA INTERNET SERVICE PROVIDERS

FINDING NO. 3

For the six sites visited, we noted that the security plans were incomplete and that the units had not entered into a service level agreement with the non-USDA ISP to establish minimum security requirements. Departmental Regulations (DR) require an agency to ensure that security controls provided by a non-USDA ISP be adequate prior to the agency requesting a waiver from using an USDA site. ARS did not perform sufficient steps at these sites to assure they had adequate security before the waiver was requested. As a result, the ARS sites are vulnerable to cyber attacks.

DR 3300-1, Appendix I, INTERNET, dated March 23, 1999, provides that the USDA OCIO will, prior to granting an agency waiver request, "Review security documentation to ensure that agency verification of security controls provided by private ISPs is adequate." It also states that an agency must meet the security requirements in DR 3140-2 and subsequently DR 3140-1 before a waiver is granted. Both of these DR's require the agency to ensure that adequate security is in place for sites accessing the internet.

On March 21, 2001, ARS requested approval from the USDA OCIO for 58 ARS units to acquire Internet access services from providers other than the USDA Internet Access Network. Generally, these waiver requests were supported on a cost and performance basis and the need was identified as necessary to support the ARS research mission. The request also stated that "…all 58 of the units included in the request meet the requirements outlined in DR-3300-I and have the required security plans on file with the OCIO."

Our review of five security plans for six of the 58 units (one security plan included two units) which were requesting waivers disclosed that many of the sections of the security plans were inadequately completed because the ARS "User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems," directed the sites to incorporate planned future dates rather than address the required sections currently. For example: four of the five security plans did not address "Risk Assessment and Management" since ARS had not yet adopted and implemented a standard risk assessment methodology; none of the five plans addressed "Authorize Processing" (a formal process for testing components or systems against a specified set of security

requirements) as the ARS OCIO was still evaluating various certification and accreditation processes for use throughout ARS; and none of the five plans adequately addressed "Contingency Planning" as no formal emergency, disaster or contingency plans had been formally developed and tested. Other security plans sections which were incomplete or which indicated future dates for compliance included the sections on "Rules," "Acquisition Specifications," "Design Review and Testing," "Production," Input/Output Controls," "Audit and Variance Detection, and "Integrity Controls."

We also found, at the sites visited, that the ARS does not have any service level agreements, which address ARS security requirements, in place with its non-USDA ISPs.

RECOMMENDATION NO. 5

Ensure that departmental requirements regarding security are met for any Internet access waiver requests submitted.

Agency Response

The ARS agreed with the recommendation and plans to work with the USDA Office of Cyber Security and ARS telecommunication specialists as well as its field locations to review all 60 ARS ISP waivers and determine an action plan for each. The corrective actions are planned to be completed by December 1, 2001.

OIG Position

We concur with the management decision.

RECOMMENDATION NO. 6

Ensure that service level agreements are timely prepared which address, at least, the minimum level of security required at each ARS site, and that the service level agreements are entered into with and agreed to by each non-USDA ISP.

Agency Response

The ARS agreed with the recommendation and plans to work with all non-USDA ISPs to develop timely service level agreements which address minimum security levels.

OIG Position

We concur with the agency response, but are unable to reach management decision until the ARS provides us the timeframes for completing the cited actions.

RECOMMENDATION NO. 7

Discontinue using any non-USDA ISP if service level agreements can not be obtained. Ensure agreements are timely updated when required due to changes in ARS operations or security needs.

Agency Response

The ARS generally concurred with the recommendation but offered an alternative to discontinuing the use of non-USDA ISPs if adequate and timely service level agreements cannot be obtained. The ARS proposed the deployment of network and host-based firewalls between non-USDA ISPs and ARS systems as one alternative to discontinued use on non-USDA ISPs when timely service level agreements cannot be developed. The ARS also plans to work with the Department to develop other technical solutions.

OIG Position

We concur with the agency response, but are unable to reach management decision until the ARS provides us the timeframes for completing the cited actions.

EXHIBIT A – AGENCY'S RESPONSE

USDA

United States Department of Agriculture

Research, Education, and Economics
Agricultural Research Service

OCT 17 2001

SUBJECT: Security Over the Agricultural Resource Service's Information Technology Resources Audit No. 02099-1-FM

TO: Richard J. Davis
Director, Administration and Finance Division
Office of Inspector General

FROM: Floyd P. Horn
for Administrator Edward B. Knipling

The purpose of this memorandum is to respond to recommendations in the official draft report for the subject audit, and, in addition, to identify text in the report that could facilitate unauthorized access to Agricultural Research Service (ARS) systems.

Attached is a copy of Report No. 02099-1-FM Official Draft with highlighted text that, for security purposes, should be deleted from the final published report. Given the events of September 11, 2001, publication of the document in its current form; e.g., with references to the specific Agency and specific operating systems is not in the best security interests of ARS nor the United States Department of Agriculture (USDA).

The following is the ARS response to the seven recommendations in the official draft report.

- *Ensure all necessary corrective actions are completed on all high and medium risk vulnerabilities identified during our audit, including the vulnerabilities identified for the Novell Netware servers.*

  As outlined in my December 6, 2000, and May 3, 2001, memoranda to James R. Ebbitt, systems administrators have taken action to correct all high and medium vulnerabilities.

ars

Office of the Administrator
1400 Independence Avenue, SW • Room 302-A • Jamie L. Whitten Federal Building
Washington, DC 20250-0300
An Equal Opportunity Employer

- *Revise the ARS internal security standards to bring them in line with industry "best practices," or document why these practices do not apply to ARS. Establish and document a minimum set of security standards for all ARS field sites using the Novell Netware servers and software and require them to follow them.*

As outlined in my May 3, 2001, memorandum to James R. Ebbitt, ARS had planned to develop and implement an Agency configuration management policy, which would expand on a Department-wide configuration management framework and policy, no later than December 31, 2001. The planned policy date has been moved back to June 30, 2002, due to limited security resources, and other competing security program deliverables that are in response to other Office of Inspector General (OIG) recommendations. However, a component of the configuration management policy will be the development of hardening guides for all major network operating systems including Novell, which we expect to begin issuing in second quarter FY 2002.

- *Conduct periodic assessments to ensure field office compliance with ARS internal security requirements.*

As outlined in my May 3, 2001, memorandum to James R. Ebbitt, ARS had planned to develop and implement an Agency security assessment policy identifying responsibilities, procedures, schedules, and controls for conducting internal security reviews, security plan reviews, and vulnerability scans no later than December 31, 2001. ARS has purchased the Network Associates Incorporated (NAI) Cyber Cop suite, conducted training for fifteen Agency administrators, and is actively using the Cyber Cop scanning tool. In addition, two security specialists in the ARS Office of the Chief Information Officer (OCIO) will attend training on Internet Security Systems (ISS) security tools in November 2001 and will implement periodic scanning of Agency systems to ensure field compliance with ARS internal security requirements. However, the planned full policy implementation date has been moved back to June 30, 2002, due to limited security resources, and other competing security program deliverables that are in response to other OIG recommendations.

- *Prepare comprehensive and system specific contingency plans that address protection of information resources and recovery procedures, including the offsite storage requirements, in the event of service disruptions. Include a description of these plans in each site's security plans.*

As outlined in my July 24, 2001, memorandum to Richard D. Long, ARS anticipates development and implementation of continuity and contingency policy and procedures by June 1, 2002. Subsequently, Agency systems will be prioritized and a timetable will be established to ensure that continuity and contingency plans for the most critical Agency systems are developed and tested as soon as possible.

- *Ensure that Departmental Requirements regarding security are met for any Internet access waiver requests submitted.*

As outlined in my July 24, 2001, memorandum to Richard D. Long, William Hadesty, Associate Chief Information Officer for Cyber Security, directed a review of all ARS Internet access waivers to ensure compliance with Departmental requirements. On June 4, 2001, Mr. Hadesty extended ARS date for compliance to December 1, 2001. We will be working with the USDA Office of Cyber Security, ARS telecommunications specialists and field locations to review all 60 ARS Internet Service Providers (ISP) waivers and determine an action plan for each.

- *Ensure that service level agreements are timely prepared which address, at least, the minimum level of security required at each ARS site, and that the service level agreements are entered into with and agreed to by each non-USDA ISP.*

To the maximum extent possible given current resource constraints and cooperative agreements with major universities, ARS will be working with all non-USDA ISPs to develop timely service level agreements (SLAs) which address minimum security levels.

- *Discontinue using any non-USDA ISP if service level agreements cannot be obtained. Ensure agreements are timely updated when required due to changes in ARS operations or security needs.*

As stated above, ARS will be working with all non-USDA ISPs to develop timely service level agreements which address minimum security levels. ARS has long-standing relationships with the majority of its non-USDA ISPs whose services are integral components of the ARS mission delivery. Discontinued usage of the services or breaking existing agreements with major universities is not a reasonable alternative in many of the environments. We recommend deployment of network and host-based firewalls between non-USDA ISPs and ARS systems as one alternative to discontinued use of non-USDA ISPs when timely SLAs cannot be developed. In addition, we plan to work with the Department to develop other technical solutions.

Enclosure

cc:
Y. King, OCIO

ABBREVIATIONS

ARS	Agricultural Research Service
CDE	Common Desktop Environment
CIO	Chief Information Officer
DR	Departmental Regulation
FY	Fiscal Year
ISP	Internet Service Provider
IT	Information Technology
OCIO	Office of Chief Information Office
OMB	Office of Management and Budget
PAN	Public Access Network
TCP/IP	Transmission Control Protocol/Information Protocol
USDA	United States Department of Agriculture