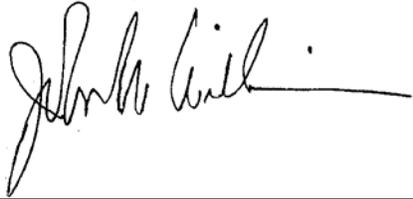


For: FSA Employees

**Non-OCIO-ITS 3rd-Party and Legacy Devices Attached to the
Service Center Agency (SCA) Network**

Approved by: Deputy Administrator, Management



1 Non-OCIO-ITS 3rd-Party and Legacy Devices on SCA Network

A Background

The memorandum in Exhibit 1 notified FSA that:

- **all** 3rd-party desktops, laptops, or non-OCIO-ITS devices **must** be migrated to OCIO-ITS-Common Computing Environment (CCE) image by May 1, 2007
- any 3rd party or legacy systems that **cannot** have the CCE image loaded will be disconnected from the network on **May 2, 2007**.

Exception: Third-party desktops, laptops, or non-OCIO-ITS devices that are documented with an Interconnection Security Agreement (ISA) between FSA and OCIO-ITS are exempt from this requirement.

To ensure a smooth transition, OCIO-ITS:

- requests that FSA document, in writing, **all** desktops, laptops, and legacy applications that require ISA's by May 1, 2007
- Technical Support Division Group Managers will be available to assist users with ISA documentation.

Disposal Date	Distribution
June 1, 2007	All FSA Employees; State Offices relay to County Offices

Notice IRM-389

1 Non-OCIO-ITS 3rd-Party and Legacy Devices on SCA Network (Continued)

B Purpose

This notice:

- informs FSA employees that any computers or devices that do **not** have CCE image loaded will be disconnected from the network on May 2, 2007
- requests that State and Large Office Administrative Officers survey their constituent offices to determine if any ISA's are needed.

Notes: ISA's are **required** for State Office electronic distribution system print shops with Heidelberg 9110's and Xerox Docutechs.

System 36/AS-400's are exempt from the ISA requirement.

C Action

By Thursday, **April 19, 2007**, provide a list of systems requiring ISA's to DAFO, Attn: Ragh Singh by either of the following:

- e-mail to **ragh.singh@wdc.usda.gov**
- FAX at 202-690-3309.

Note: All 3rd party or legacy systems that **cannot** have the CCE image loaded and do **not** have an ISA will be disconnected from the network on **May 2, 2007**.

D Contacts

The following table provides contacts if there are questions.

IF questions are about...	THEN contact...
this notice	Louis Iacoletti, ITSD by: <ul style="list-style-type: none">• e-mail to louis.iacoletti@wdc.usda.gov• telephone at 202-720-4143.
providing the list of systems requiring ISA's to DAFO	DAFO, Attn: Ragh Singh by: <ul style="list-style-type: none">• e-mail to ragh.singh@wdc.usda.gov• telephone at 202-720-7094• FAX at 202-690-3309.



**United States
Department of
Agriculture**

March 20, 2007

**Office of the Chief
Information Officer**

1400 Independence
Avenue SW

Washington, DC
20250

TO: Steve Sanders
CIO, Farm Services Agency

Jack Carlson
CIO, Natural Resources Conservations Service

Christopher Smith
CIO, Rural Development

FROM: Richard K. Roberts 
Associate CIO for Information Technology Services

SUBJECT: Non OCIO/ITS (Third-Party) and legacy devices attached to the
Service Center Agency (SCA) Network

Action Required By: May 1, 2007.

In October 2005, The Office of the Inspector General (OIG) released an issue paper titled "Office of the Chief Information Officer – Management and Security over Information Technology Convergence – Common Computing Environment" (Report No. 50501-3-FM). The audit report disclosed a material weakness concerning 'third-party' devices for failure to meet the required minimum security standards. To remediate this material weakness, OIG recommended that the Office of the Chief Information Officer (OCIO) Information Technology Services (ITS) assume control of legacy devices, and establish policies, procedures, and controls to ensure that the third-party devices (1) meet minimum security standards and (2) are scanned for vulnerabilities and malicious code prior to being connected to the CCE network. "Third-party" devices or non OCIO-ITS devices are identified as all desktops, systems, and devices on the Service Center Agency (SCA) network that are not managed by OCIO-ITS. OCIO-ITS submitted a request to close this recommendation out in June 2006; this request was subsequently denied by OIG and OCFO. This audit recommendation remains a material weakness for USDA and the report remains as there is still 'third-party' devices remaining on OCIO-ITS's network.

In an effort to address this material weakness and close the recommendation, OCIO-ITS has established the following procedures:

1. All "third-party" desktops or laptops or non OCIO-ITS devices must be migrated to the OCIO-ITS CCE image by May 1, 2007. The CCE image includes software to manage the device and to scan for vulnerabilities and malicious code. OCIO-ITS will make resources available to assist in this migration.

2. For “third-party” desktops, laptops, and legacy applications that are not managed by OCIO-ITS, an Interconnect Security Agreements must be signed between ITS and the Service Center Agency before such devices can be connected to any OCIO-ITS system. Federal requirements and Departmental Regulations require all systems to be certified and accredited prior to ITS entering into an Interconnect Security Agreement with any agencies.

The minimum security requirements mandated for USDA’s environment can be found in the following Federal regulations and Departmental policies:

- Federal Information Security Management Act (FISMA);
- National Institute of Standards and Technology (NIST) 800-47 Security Guide for Interconnecting Information Technology Systems;
- NIST 800-53 Recommended Security Controls for Federal Information Systems;
- USDA OCIO Cyber Security Manual specifically DM3575-001 Chapter 15, Part 1 Security Controls in the System Life Cycle / Systems Development Life Cycle;
- DM3530-004 Firewall Technical Security Standards (02/17/05);
- DM3530-006 Malware and Anti-Virus;
- DM 3535-000, Chapter 7, C2 Controlled Access Protection and DM 3535-002, Chapter 7, Part 2, Patch Management and System Updates; and
- OCIO-ITS Security Policy Manual – Chapter Fifteen: Non-OCIO-ITS Owned Devices Security Policy.

To ensure a smooth transition, OCIO-ITS is requesting each Agency CIO to document in writing their non OCIO-ITS laptops and desktops and legacy applications that require Interconnect Security Agreements by May 1, 2007. My security staff will work with your security staff in detecting these devices and establishing these agreements. Any third party or legacy system that cannot meet the minimum security requirements WILL NOT BE ALLOWED TO CONNECT TO ANY OCIO-ITS AFTER MAY 1, 2007.

If there are any non OCIO-ITS devices or legacy applications remaining on the OCIO-ITS network that have not been migrated to the CCE image or have not obtained an ISA, we will assume that agencies will retain control of the ‘third-party’ devices, and will remove these systems from the OCIO-ITS network on May 2, 2007. Any non OCIO-ITS devices or legacy applications or legacy application detected by my staff will be reported as a security incident beginning in May 2007.

These procedures do not apply to third party devices being placed on the SCA network for temporary purposes. OCIO-ITS Security Policy Manual – Chapter Fifteen: Non-OCIO-ITS Owned Devices Security Policy” procedures shall be used for managing these temporary devices on the SCA network.

Please contact Larry Brooks, Technical Support Division Director, if you have any questions on 970-295-5423.

cc: Robert E. Suda, ACIO I&O
Eric Won, DACIO
Greg Gage, ISSPM and SLM
Scott Snover, ITS/IDD
Carol Henson, ITS/IOD
Larry Brooks, ITS/TSD
Greg Montgomery, ITS/IGD
Valarie Burks, ITS/WCTS
Craig Chase, ITS/IGD/SPB
Brian J. Davies, ISSPM/FSA
Brenda Dinges, ISSPM/RD
Elizabeth Pigg, ISSPM/NRCS
Greg Schmitz, ISSPM/NITC