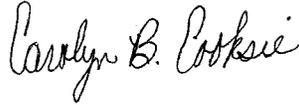


For: State and County Offices

**Annual Information Technology (IT) Security Program Review and
Security Controls Risk Assessment for State and County Offices**

Approved by: Associate Administrator for Operations and Management



1 Overview

A Background

FSA-774 and FSA-774A have been consolidated into a revised FSA-774, “IT Security Program Review and Security Controls Risk Assessment Checklist” and related policy in 6-IRM is being updated to better support security program objectives and mission requirements. The updated policy incorporates security standards documented in the following:

- FISMA Act of 2002
- USDA DM 3570
- NIST SP-800-53 guidance.

This improved series of actions alleviates redundancy, clarifies the reporting process for State and County Offices, and incorporates new minimum required physical security control objectives.

Until the release of the revised 6-IRM, this notice and the revised FSA-774 supersede the existing FSA-774, FSA-774A, and related policies.

| Disposal Date | Distribution |
|----------------------|--|
| February 1, 2011 | State Offices; State Offices relay to County Offices |

Notice IRM-427

1 Overview (Continued)

B Purpose

This notice:

- communicates the updated policy and procedure to State and County Offices on the requirement for an annual IT security program review and security controls risk assessment
- provides the revised FSA-774 and reporting process
- instructs State and County Offices on how to complete and submit the revised FSA-774
- communicates a new requirement for a physical review of State Offices by the Security Liaison Representative (SLR)
- explains the program review, risk assessment, and certification process
- explains the requirement for a corrective action plan to address security vulnerabilities
- identifies responsibilities
- obsoletes FSA-774A.

C Contact

If additional information is needed:

- County Offices shall contact the State SLR
- State SLR shall contact either of the following by e-mail:
 - Seabelle Ball at seabelle.ball@wdc.usda.gov
 - Marcia McCarty at marcia.mccarty@kcc.usda.gov.

2 Policy

A FSA-774 and Plans of Action and Milestones (POA&M's)

State and County Offices shall:

- conduct an annual IT security program review and risk assessment using the revised FSA-774
- include a corrective POA&M's to address security weaknesses identified during the program review and risk assessment.

2 Policy (Continued)

A FSA-774 and Plans of Action and Milestones (POA&M's) (Continued)

POA&M's define tasks that need to be accomplished to correct weak or vulnerable security controls. The process details required resources, schedule completions dates for task closure, and documents accomplished milestones along the way. It is a critical management process to help mitigate weak security controls at individual offices. It will also improve FSA's overall security posture. State and County Offices should work diligently to implement, document, and resolve POA&M's.

State and County Offices shall follow current OCIO, International Technology Services (ITS) minimum security requirements for Service Center Agencies (SCA's), including security standards documented in the current FSA and OCIO, ITS Service Level Agreement.

The FY 2010 annual security program review is currently in progress and State and County Offices may have already submitted FSA-774 and FSA-774A. **The revised FSA-774 or FSA-774, dated "4-17-97" and FSA-774A are admissible for the FY 2010 review in progress.** County Offices shall submit reports to the State Office, and the State Office will submit reports to the National Information Security Office (ISO) by the following dates.

| Due Date | Office Location | Remarks |
|----------|--------------------------------------|--|
| May 30 | SLR County Office reviews completed. | Optional for FY 2010. Mandatory for future years. |
| June 15 | State Office submission to ISO. | No exceptions. |

B Local Security Policy and Procedures

Examination of FSA's security program controls calls for a systematic approach and application to improve some physical security control. In addition to the revised FSA-774, which includes current minimum physical security controls for ADP server rooms in all SCA's managed space according to DR 3901-001 and 33-AS; effective immediately State Offices should also develop, distribute, and communicate to FSA County Offices **local level physical access policy and/or procedure to protect the System 36/AS400 system and data.**

Facility physical security for SCA offices may vary depending on the office size and physical location issues commensurate with the local environment. Some SCA offices may choose to implement more extensive security controls, for instance if the facility has extensive public access.

2 Policy (Continued)

B Local Security Policy and Procedures (Continued)

Information processed within any SCA office is sensitive in nature and must be adequately protected. One approach to the policy development requirement is to closely examine the data on the incoming FY 2010 FSA-774's and write a local notice to address areas that may need strengthening or additional oversight. See Exhibit 1.

3 Action

A SLR Action

SLR's will conduct physical program reviews within the State under the following general guidelines. SLR's will:

- review and verify that all security areas on the State Office FSA-774 are assessed and analyzed for risks and vulnerabilities
- document and track needed corrective actions
- submit the State Office FSA-774 to ISO by June 15
- schedule and conduct physical reviews for a minimum 1 percent of the County Offices each year between February 15 and May 30
- monitor progress of the State Offices POA&M corrective plan and report the progress to SED
- report completion or updates of the State Office POA&M's to ISO by the identified completion date.

B SED Action

SED's will:

- relay guidance to the County Offices
- review and certify the State Office FSA-774 before the State submission to ISO
- identify resources to support POA&M's corrective actions
- work with appropriate sources to ensure ADP space requirements are being addressed and/or document issues in the appropriate section of FSA-774
- ensure local policy is developed and distributed of improve physical protection of the Systems 36/AS400.

Notice IRM-427

3 FSA-774, Annual Information Technology (IT) Security Program Review and Security Controls Risk Assessment Checklist

A Instructions

FSA-774:

- is prepared to verify that IT security and physical controls have been assessed and analyzed for security risks and vulnerabilities
- **represents the minimum requirements that all State and County Offices must have in place.**

State and County Offices shall:

- review each question or statement on FSA-774
- check (✓) “YES” or “NO” to document the current security posture for the local office being reviewed.

SED or SLR must:

- define POA&M for all “No” answers
- explain all “N/A” answers and submit supporting documents when appropriate.

Notice IRM-427

3 FSA-774, Annual Information Technology (IT) Security Program Review and Security Controls Risk Assessment Checklist

B Required Certifications for FSA-774 Submission

The following are required certifications for submitting FSA-774.

| Items | Action |
|---------------------|---|
| 2A through 2D | <p>For:</p> <ul style="list-style-type: none"> • County Offices, enter the following: <ul style="list-style-type: none"> • name, title, and telephone number of preparing official • date FSA-774 is prepared <p>Note: County Offices may have up to 2 people preparing FSA-774. The second preparer shall use items 3A through 3D.</p> <ul style="list-style-type: none"> • State Offices, SLR: <ul style="list-style-type: none"> • shall prepare FSA-774 • is the preparing official and shall enter their name, title, and telephone number • shall enter date FSA-774 is prepared. |
| 4A through 4D | <p>For:</p> <ul style="list-style-type: none"> • County Offices, CED is the certifying official and shall enter name, title, telephone number, and date • State Offices, SED is the certified official and shall enter name, title, telephone number and date. |
| 5A through 5D | <p>For:</p> <ul style="list-style-type: none"> • County Offices, SLR is the reviewing official and shall enter name, title, telephone number, and date FSA-774 is reviewed and verified • State Offices, ISO is the reviewing official and shall enter name, title, telephone number, and date FSA-774 is reviewed and verified. |

Sample Local Physical Access Policy**System 36/AS400 Physical Access Policy****I. Purpose**

The purpose of this policy is to establish local standards for securing _____ State Office System 36/AS400, data, and server rooms. Effective implementation of this policy will minimize unauthorized access and provide more effective auditing of physical access controls.

II. Scope

The policy applies to all _____ State and County local facilities containing System 36/AS400 operated equipment _____.

III. Policy**A. Ownership and Responsibilities**

The local _____ offices are responsible for the safety and security of the System 36/AS400 data enter, processed or on stored and the equipment used to run the network infrastructure.

B. Physical Access

All local facility and physical access security controls must comply with applicable regulations such as, but not limited to those noted in **FSA-774, Annual Information Technology (IT) Security Program Review and Security Controls Risk Assessment Checklist for State and County Offices**.

- Physical access to the facility must be restricted and must be documented and managed.
- The System 36/AS400 sever room facilities must be physically protected in proportion to the _____.
- Access to the System 36/AS400 facilities will be granted only to support personnel and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to the sever room must include the approval of the _____.
- Access cards and/or keys must not be shared or loaned to others at any time.
- Access cards and/or keys that are no longer required must be returned to the _____.
- Cards or keys must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the _____.
- Card access records and keys logs for IT facilities must be kept for routine review.
- _____ will remove the card and/or key access rights of individuals that change roles or are separated from their relationship with the local office.
- Visitors must be escorted in access controlled areas of server room facilities.
- Signage for restricted access.
- must be practical, yet minimal evidence of the importance of the location should be displayed.
- Etc.

C. Authorized Personnel**IV. Enforcement**

Anyone found to have violated this policy may be subject to appropriate disciplinary action.