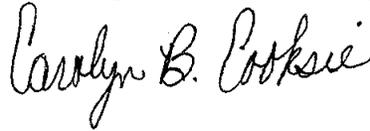


For: FSA Offices

FY 2011 Mandatory Specialized Role-Based Information Technology (IT) Security Training

Approved by: Associate Administrator for Operations and Management



1 Overview

A Background

The Federal Information Security Management Act (FISMA) mandates that better attention be devoted to **specialized** role-based IT security training. Employees, contractors, and partners holding positions with **significant responsibilities for information security** are required to have specialized role-based IT security training before access is granted to any agency information systems and/or sensitive data. For continued access, personnel must complete specialized role-based security training each FY. USDA, OCIO define positions with significant responsibility for information security as the following.

Positions that may impact the mission of the agency through a loss of confidentiality, integrity and/or availability of the USDA information, regardless of media, are to be designated as having significant responsibilities for security. Some of the determining factors are: users requiring advanced rights to a system beyond that of a regular user, which may include database, network, mail and IT system administrators, programmers, security managers, IT system owners, information owners, and IT system program managers, CIO's, Privacy Officers, FOIA Officers. In addition, positions that have programmatic and/or management control over IT system resources are also included.

Note: Users who have administrative access to their own desktops and/or laptops are **not** considered to have significant responsibilities for security.

Disposal Date	Distribution
November 1, 2011	State Offices; State Offices relay to County Offices

1 Overview (Continued)

B Purpose

This notice:

- identifies employees mandated by the Chief Information Security Officer (CISO) to complete specialized role-based IT security training by **COB March 4, 2011**
- directs supervisors to identify and ensure appropriate personnel complete specialized role-based IT security training each FY
- directs supervisors to identify and ensure appropriate personnel complete specialized role-based IT security training whenever a significant change occurs in the IT security environment
- document procedures to complete FY 2011 specialize role-based IT security training using AgLearn.

2 Specialized Role-Based IT Security Training Guidance

A Scope

Supervisors are required to identify and ensure that employees, contractors, and partners designated with significant responsibilities for information security receive specialized training based on the functional responsibilities of the individual user.

B Mandatory Training for Information Security Office (ISO) Personnel and State Office Security Liaison Representatives (SLR's)

ISO employees and contractors and State Office SLR's and alternates are identified by the CISO as having significant security responsibilities. Therefore, these employees are required to complete the FY 2011 Specialized Role-Based IT Security Training using AgLearn by **COB March 4, 2011**.

Note: Newly assigned ISO employees, contractors, SLR's, and SLR alternates shall complete specialized role-based IT security training before starting their security related duties.

2 Specialized Role-Based IT Security Training Guidance (Continued)

C Other Personnel

Supervisors should revisit the USDA definition in subparagraph 1 A and ensure that specialized role-based IT security training is provided for any other personnel position that is relevant to the USDA definition for position with significant security responsibilities.

Employees that should be considered for role-based IT security training include, but are not limited to, the following:

- FSA leaders
- facility managers
- IT support personnel
- operations managers
- human resource representatives
- webpage developers
- end users
- system managers, owners, and administrators.

D Assigning the Specialized Role-Based Training Curriculum

ISO personnel, SLR's, and any additional positions identified by supervisors must complete at least **1** of the 11 course options listed under the Training Curriculum in Exhibit 1. **Do not repeat the same course taken in FY 2010 or previous FY's.** Credit will **not** be given for repeated courses. Check the learning history to view courses completions and select a different course from last year, if applicable.

The online course curriculum must be assigned to the employee by an AgLearn Administrator and will be accessible in the employee's AgLearn "Curricula".

HRD, Leadership and Employee Development Branch will assign the training curriculum to all ISO personnel, contractors, and SLR's initially identified by CISO.

All additional personnel identified by supervisors shall contact the local AgLearn Administrators or the alternates to request the training curriculum.

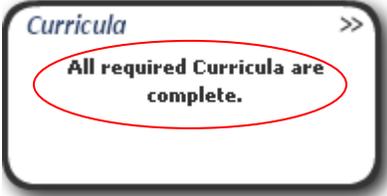
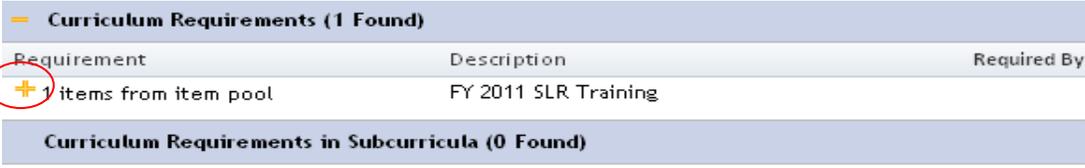
Notice IRM-442

2 Specialized Role-Based IT Security Training Guidance (Continued)

E Accessing the Specialized Role-Based Training Curriculum

Access and complete the training using AgLearn according to the following.

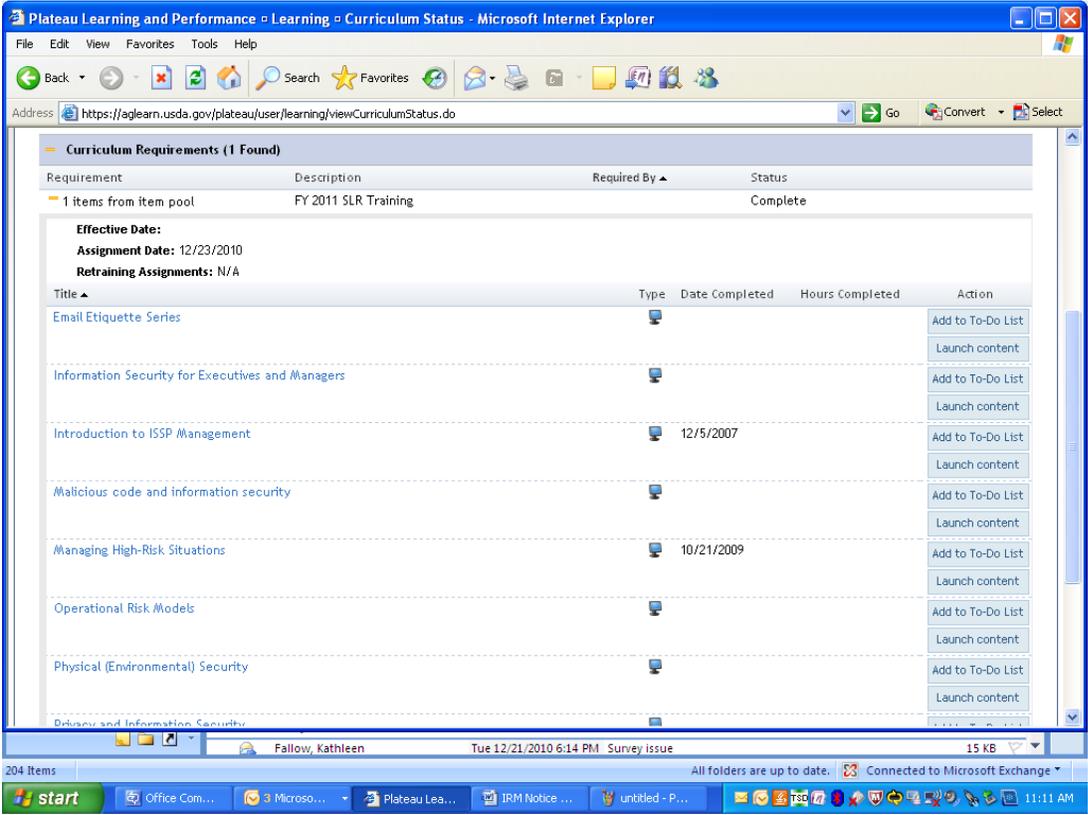
Note: Newly appointed SLR’s shall complete the “Introduction to ISSP Management” course.

Step	Action
1	Review Exhibit 1 and select a course most appropriate for individual specialized security role.
2	Access the AgLearn Home Page at http://www.aglearn.usda.gov .
3	CLICK “Learner Login”.
4	On the eAuthentication Login Warning Screen, CLICK “I Agree”. Enter user ID and password and CLICK “Login”.
5	Under “Curricula”, CLICK “All required Curricula are complete”. 
6	CLICK “FSA FY2011 Role-Based IT Security Training”. 
7	Under “Curriculum Requirements”, CLICK “+” to expand selections. 

Notice IRM-442

2 Specialized Role-Based IT Security Training Guidance (Continued)

E Accessing the Role-Based Training Curriculum (Continued)

Step	Action																																																
8	<p>CLICK on “Launch Content” to begin the course not previously taken.</p>  <p>The screenshot shows a web browser window titled "Plateau Learning and Performance - Learning - Curriculum Status". The address bar shows the URL: https://aglearn.usda.gov/plateau/user/learning/viewCurriculumStatus.do. The main content area displays "Curriculum Requirements (1 Found)" with a table listing requirements. Below this, there are details for the requirement: "Effective Date:", "Assignment Date: 12/23/2010", and "Retraining Assignments: N/A". A table lists several courses with columns for Title, Type, Date Completed, Hours Completed, and Action. The Action column contains "Add to To-Do List" and "Launch content" buttons for each course.</p> <table border="1"> <thead> <tr> <th>Requirement</th> <th>Description</th> <th>Required By</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>1 items from item pool</td> <td>FY 2011 SLR Training</td> <td></td> <td>Complete</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Title</th> <th>Type</th> <th>Date Completed</th> <th>Hours Completed</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td>Email Etiquette Series</td> <td></td> <td></td> <td></td> <td>Add to To-Do List Launch content</td> </tr> <tr> <td>Information Security for Executives and Managers</td> <td></td> <td></td> <td></td> <td>Add to To-Do List Launch content</td> </tr> <tr> <td>Introduction to ISSP Management</td> <td></td> <td>12/5/2007</td> <td></td> <td>Add to To-Do List Launch content</td> </tr> <tr> <td>Malicious code and information security</td> <td></td> <td></td> <td></td> <td>Add to To-Do List Launch content</td> </tr> <tr> <td>Managing High-Risk Situations</td> <td></td> <td>10/21/2009</td> <td></td> <td>Add to To-Do List Launch content</td> </tr> <tr> <td>Operational Risk Models</td> <td></td> <td></td> <td></td> <td>Add to To-Do List Launch content</td> </tr> <tr> <td>Physical (Environmental) Security</td> <td></td> <td></td> <td></td> <td>Add to To-Do List Launch content</td> </tr> </tbody> </table>	Requirement	Description	Required By	Status	1 items from item pool	FY 2011 SLR Training		Complete	Title	Type	Date Completed	Hours Completed	Action	Email Etiquette Series				Add to To-Do List Launch content	Information Security for Executives and Managers				Add to To-Do List Launch content	Introduction to ISSP Management		12/5/2007		Add to To-Do List Launch content	Malicious code and information security				Add to To-Do List Launch content	Managing High-Risk Situations		10/21/2009		Add to To-Do List Launch content	Operational Risk Models				Add to To-Do List Launch content	Physical (Environmental) Security				Add to To-Do List Launch content
Requirement	Description	Required By	Status																																														
1 items from item pool	FY 2011 SLR Training		Complete																																														
Title	Type	Date Completed	Hours Completed	Action																																													
Email Etiquette Series				Add to To-Do List Launch content																																													
Information Security for Executives and Managers				Add to To-Do List Launch content																																													
Introduction to ISSP Management		12/5/2007		Add to To-Do List Launch content																																													
Malicious code and information security				Add to To-Do List Launch content																																													
Managing High-Risk Situations		10/21/2009		Add to To-Do List Launch content																																													
Operational Risk Models				Add to To-Do List Launch content																																													
Physical (Environmental) Security				Add to To-Do List Launch content																																													
9	<p>Ensure that courses show as complete in the learning history.</p> <p>Note: If course number “4”, “Managing High Risk Situations” is selected, the course “Operational Risk Models” shall also be completed to receive full credit.</p>																																																

Notice IRM-442

2 Specialized Role-Based IT Security Training Guidance (Continued)

F Contacts

The following provides a summary of contacts if there are questions.

IF there is a question about...	THEN...
AgLearn	do any of the following: <ul style="list-style-type: none"> • in AgLearn, CLICK “Help” • in AgLearn, CLICK “Contact Us” • call 1-866-633-9394.
new eAuthentication accounts or password resets	Contact ITS National Help Desk at 1-800-255-2434, option 3, or self-register for an account at http://www.eauth.egov.usda.gov/eauthCreateAccount.html .
this notice or Security Awareness Training policy	contact either of the following: <ul style="list-style-type: none"> • Seabelle Ball by: <ul style="list-style-type: none"> • e-mail at seabelle.ball@wdc.usda.gov • telephone at 202-205-7399 • Brian Davies by: <ul style="list-style-type: none"> • e-mail at brian.davies@wdc.usda.gov • telephone at 202-720-2419.
National Office employee training administration	contact Bessy Plaza, HRD, by: <ul style="list-style-type: none"> • e-mail at bessy.plaza@wdc.usda.gov • telephone at 202-401-0365.
Kansas City, St. Louis, or APFO employee training administration	contact either of the following: <ul style="list-style-type: none"> • Mark Nelson by: <ul style="list-style-type: none"> • e-mail at mark.nelson@kcc.usda.gov • telephone at 816-926-3420 • Cindy Witmer by: <ul style="list-style-type: none"> • e-mail at cindy.witmer@kcc.usda.gov • telephone at 816-926-2500.
State and County Office employee training administration	contact State training officer or AgLearn lead.

2 Specialized Role-Based IT Security Training Guidance (Continued)

G Reasonable Accommodations

Persons who require special accommodations to participate in this training should contact their supervisor or local help desk.

H Noncompliance

Employees that do **not** comply with the specialized role-based IT security training mandate risk computer account suspension.

I Continuing Security Training Requirements

To facilitate strengthening FSA's overall IT Security Training Program and expand on the required annual IT Security Awareness, Rules of Behavior, and Role-Based IT Security Training, FSA offices shall:

- employ subsequent methods, (office posters, booklets, newsletters, handouts, checklists, videos, brown bag lunch series, etc.), to make personnel aware of information security and changes in the security environment of the individual office
- provide additional or refresher training when personnel enters a new position which deals with sensitive information or has different information security requirements. The additional training should be on the level of responsibility and the sensitivity of the information the employee handles.

Use the National Institute of Standards and Technology (NIST) Special Publications 800-16, Information Technology Security Training Requirements: A Role-and Performance-Based Model, and 800-50, Building an Information Technology Security Awareness and Training Program to help plan, implement, maintain, and periodically evaluate ongoing IT security training plans and actions. NIST Special Publications are located on the NIST website at <http://csrc.nist.gov/publications/PubsSPs.html>.

FY 2011 Specialized Role-Based IT Security Training Curriculum

FY 2011 Role-Based IT Security Training Curriculum				
Course Number	Course Name	Course Description	Target Audience	Duration
1	Introduction to ISSP Management	Introduction to ISSP Management.	New SLR's	60 minutes
2	Information Security for Executives and Managers (Briefing USDA-OCIO-EXECSUMM-PII-V1)	This training will provide an overview of the key information security practices to consider as organization leaders within USDA.	Executive and managers, but all employees could benefit	40 minutes
3	Malicious Code and Information Security	How malicious code works and the ways to defeat it in a wired and wireless environment. An introduction to information security best practices.	All users	100 minutes
4	A. Managing High-Risk Situations (30 min) and B. Operational Risk Models (10 min)	Presents 9 scenarios in which employees face volatile and potentially violent situations in the workplace and gives participants an opportunity to discuss appropriate resolutions. Involves understanding the negative events associated with people, process technology, and external events.	GS-15 and Schedule C (all managers and supervisors can benefit)	Total of 40 minutes for both courses. Both courses must be completed to get credit.
5	Email Etiquette Series	The 12 Immutable Laws of Email Etiquette.	All users	45 minutes
6	Privacy and Information Security	The protection of an individual's personal information has business implications that extend beyond the privacy of any 1 individual. Various laws protect private information relative to certain businesses and industries. Example: The Health Insurance Portability and Accountability Act (HIPAA) laws protect private medical information.	All employees, especially those who have access to private information	60 minutes

FY 2011 Specialized Role-Based IT Security Training Curriculum (Continued)

FY 2011 Role-Based IT Security Training Curriculum				
Course Number	Course Name	Course Description	Target Audience	Duration
7	Security, Safety, and Communication	To understand the role of security in an organization, (data, physical, incident reporting, etc.). The importance of following safety and environmental guidelines, and how to communicate with customers in a professional manner.	Entry level computer technician and security personnel	125 minutes
8	Physical (Environmental) Security	To understand the considerations and mechanisms involved in implementing the physical security of an enterprise.	Mid-level and senior-level managers	120 minutes
9	Security and the Wireless Environment	Describes security in the wireless environment.	Technical and security professionals; IT and business managers	120 minutes
10	Securing Storage	Recognize the importance of storage security, identify the tasks involved in ensuring storage security, identify the threats to storage security, and how they are mitigated.	IT professionals with little or no knowledge of storage concepts but who need to support storage products now or in the future and make storage related decisions	140 minutes
11	Workplace Security Awareness	Provides an awareness-level orientation of basic workplace security fundamentals and appropriate actions for workers to take in the event of potential threat situations that may be encountered in the workplace, including encountering trespassers, receiving phone threats, dealing with workplace violence incidents, evacuating during an emergency, and protecting against various types of terrorist acts.	All new employees (especially those new to security)	60 minutes