

## Information Technology Security Awareness Training Procedures for Short-Term Non-Federal Emergency Response Personnel

### Background

Department of the Interior (DOI) and Department of Agriculture (USDA) employees are required to read and acknowledge their understanding of their respective Department's information technology (IT) security awareness and individual user responsibilities prior to accessing IT systems or sensitive information.

Non-Federal employees (e.g., State and county fire team workers), specifically those that are assigned on-site for two weeks or less during the fire season, need to be rapidly trained and provisioned for their assignments. After discussion and review, DOI and USDA acknowledged the need for a streamlined security awareness training process that would meet the rapid deployment need and comply with federal security training requirements for this group of employees.

The following minimum requirements needed to be met to be accepted by both Departments:

1. Training must be consistent between the two Departments;
2. Accomplishment of training must be trackable;
3. Evidence of training must be readily available for review in the event of an audit; and
4. Training must meet the minimum security awareness training requirements for access to Federal IT systems and other sensitive information.

As part of the DOI/USDA training pilot, rapid deployment of training was determined to best be accomplished by using a combination of a DOI/USDA IT Security Awareness and Best Practices handout and managed via a user log (reference Short-Term Emergency Response Personnel User Log) that tracks individual user's acknowledgement to adhere to the identified IT security best practices.

### Scope

The process defined in this document is applicable to all short-term, non-Federal emergency response personnel who use DOI or USDA computer systems or have access to sensitive information, regardless of its form.

### Oversight Responsibility

The benefiting activity manager or Office Coordinator is responsible for ensuring that all short-term non-Federal emergency response personnel under their purview follow these procedures. The manager or Office Coordinator may designate IT support personnel to distribute user accounts and coordinate with the Help Desk to reset accounts when they are no longer needed. The manager or Office Coordinator shall make the user log available upon request for designated IT support personnel to review as needed. IT support personnel shall distribute user IDs and initial logon passwords in a sealed envelope.

If the non-Federal employee is deployed at multiple sites, the employee will be required to accomplish this training and acknowledge receipt of training at each site. The activity managers or Office Coordinators at each site are required to log and track the training information as noted above.

### Process

1. Short-term, non-Federal emergency response personnel shall be provided a copy of the *Information Technology Security Awareness and Best Practices* handout **before** they are granted initial access to their account.
2. The user shall read the *Information Technology Security Awareness and Best Practices* handout and contact their incident supervisor or the IT Security Manager if they have any questions. This is important in order to ensure that the user is aware of their responsibilities and to provide Department/office accountability.
3. The user fills out the *Short-Term Emergency Response Personnel User Log* and signs it to acknowledge their agreement to follow Department IT security best practices. The manager or Office Coordinator initials the log signifying that the individual signed this acknowledgement.
4. The user receives the sealed envelope with their account access information.

