



United States  
Department of  
Agriculture

Office of the Chief  
Information Officer

1400 Independence  
Avenue SW

Washington, DC  
20250

**TO:** Douglas C. Nash  
Chief Information Officer  
Forest Service

**FROM:** Cheryl Cook *Cheryl L. Cook*  
Acting, Chief Information Officer

**SUBJECT:** Guidance for Short-Term State and Local Emergency Response  
Personnel Regarding Logical Access to Department Networks and  
Resource

MAY 1 - 2012

On February 17, 2012, the United States Department of Agriculture (USDA) and the United States Department of Interior (DOI) Chief Information Officers approved a request to accept risk for granting short-term state and local emergency response personnel without full background investigations access to USDA and DOI general support systems (GSS). As a result, I am issuing the following guidance for granting such access for the 2012 fire season. Interior is issuing similar guidance to ensure that common policies and practices are followed throughout our respective organizations.

This memorandum applies to wildfire program activities for the 2012 fire season only in the Forest Service. This pilot will function as a proof of concept and the activities will be evaluated in November 2012. This memorandum does not change the current procedures for controlling physical access at local facilities.

This memorandum grants qualifying short-term state and local emergency response support personnel access to federal networks and resources without possessing HSPD-12 identity credentials, including fingerprint checks and/or background investigations. Each of the affected organizations will adhere to the 25 mitigating controls described in the February 17, 2012 memorandum (Attachment D). Any permanent or temporary entity (for example, a dispatch center or an incident organization) that grants short-term state and local emergency response personnel access to USDA networks without full background investigations will follow these procedures:

- Establish an appropriate number of short-term computer user accounts consisting of predefined login names and passwords to be assigned to these short-term emergency response personnel. Each issuing office shall document the granting of these short-term accounts.
- Provide all short-term non-federal emergency employees with Rules of Behavior for use of information technology systems for review and signature.
- Conduct and track Information Technology Security Awareness Training as outlined in Attachment A.
- Provide short-term emergency response personnel with Information Technology Security Awareness training as found in Attachment B.

- Establish a Service Level Agreement (SLA) between each dispatch center and the servicing Information Technology organization using the template found in Attachment C. The SLA must be in place prior to establishing the user accounts for short-term emergency response personnel.
- Document any security violations involving these personnel, and immediately report them to the appropriate authority.

Each affected organization is responsible for transmitting this guidance to all affected elements of the organization, for implementing the guidance in coordination and collaboration with interagency partners, and for providing appropriate monitoring and oversight.

cc: Chief, Forest Service

**Attachments:**

- A. Information Technology Security Awareness Training Procedures
- B. Information Technology Security Awareness Training
- C. Service Level Agreement Template
- D. Memorandum, February 17, 2012, *Risk Acceptance Details for Granting Short-Term State & Local Emergency Response Personnel without Full Background Investigations Access to USDA and DOI General Support Systems*