



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

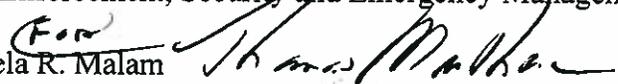


MAY 16 2012

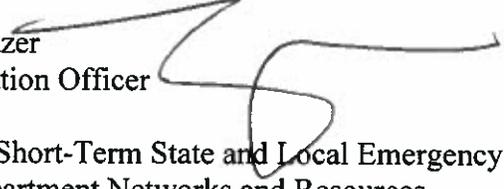
OCIO Directive 2012-007

To: Assistant Directors for Information Resources

Through: Kimberly A. Thorsen 
Deputy Assistant Secretary
Law Enforcement, Security and Emergency Management


Pamela R. Malam
Deputy Assistant Secretary
Human Capital and Diversity


Andrew Jackson
Deputy Assistant Secretary
Technology, Information and Business Services

From: Bernard J. Mazer 
Chief Information Officer

Subject: Guidance for Short-Term State and Local Emergency Response Personnel Regarding Access to Department Networks and Resources

On February 17, 2012, the United States Department of Agriculture's (USDA) Chief Information Officer (CIO) and I approved a request to accept risk for granting short-term state and local emergency response personnel without full background investigations access to USDA and the Department of the Interior's (DOI) General Support Systems (GSS). As a result, I am rescinding DOI's Office of the Chief Information Officer (OCIO) Directive 2011-005, and issuing the following guidance for granting such access. USDA is issuing similar guidance to ensure that common policies and practices are followed throughout the respective organizations.

This directive applies to the Wildland Fire program activities in the following DOI organizations:

- Office of the Secretary;
- Bureau of Land Management;
- Bureau of Indian Affairs;
- National Park Service; and
- Fish and Wildlife Service.

This directive 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 A). 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 DOI 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 (IT) systems for review and signature.
- Conduct and track IT Security Awareness Training as outlined in Attachment A.
- Provide short-term emergency response personnel with IT Security Awareness training as found in Attachment B.
- Establish a Service Level Agreement (SLA) between each dispatch center and the servicing IT 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. If you have questions regarding this policy, please contact, Chris Rutherford at Christopher_Rutherford@ios.doi.gov or 202-208-5433.

cc: Kirk Rowdabaugh, Director, Office of Wildland Fire

Attachments:

Attachment A - Memorandum of February 17, 2012
Attachment B - Information Technology Security Awareness Training Procedures
Attachment C - Information Technology Security Awareness Training
Attachment D - Service Level Agreement Template