



# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, DC 20240

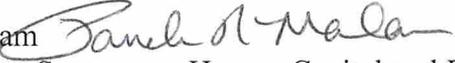


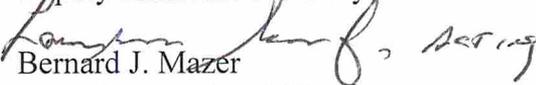
APR 4 2011

OCIO Directive 2011-005

To: Assistant Directors for Information Resources

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

Pamela R. Malam   
Deputy Assistant Secretary – Human Capital and Diversity

From: Bernard J. Mazer   
Chief Information Officer

Subject: Granting Limited/Controlled Access to DOI Information Systems for Short-term Emergency Response Personnel

This directive establishes risk-mitigation procedures to allow short-term emergency response personnel limited/controlled access to DOI computer systems and supersedes and replaces OCIO Directive 2011-001, “Incident Dispatch Centers, Short-Term Incident Personnel.” This directive is in compliance with the Office of Management and Budget (OMB) Memorandum M-05-24<sup>1</sup>, “Policy for a Common Identification Standard for Federal Employees and Contractors,” that allows agencies to exclude specific categories of individuals based on risk-mitigation practices. DOI Personnel Bulletin 09-06, “Policy for the Issuance and Management of DOI Access Cards,” and the “Policy for the Issuance, Management and Use of Federal Personal Identity Verification (PIV) Cards (DOI Access Cards)” memorandum dated March 31, 2011, remain in effect for all other short-term personnel not specified within this directive.

This directive applies to the following four DOI bureaus who hire short-term emergency response personnel for emergency response:

- Bureau of Indian Affairs (BIA)
- Bureau of Land Management (BLM)
- National Park Service (NPS)
- United States Fish and Wildlife Service (USFWS).

Examples of emergency response include providing support to or directly responding to wildfire or all hazardous incidents such as floods, hurricanes, tornadoes or oil spills.

<sup>1</sup> A copy of OMB M-05-24 is available at:

<http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf>

Unless the term of employment exceeds an aggregate of 6 months in either a single continuous appointment or series of appointments, this directive temporarily removes the requirement for a full National Agency Check with Inquiries (NACI) and issuance of a DOI Access Card for short-term federal and non-federal emergency response personnel until:

- a corrective action plan can be fully implemented to quickly process this category of individuals; and
- DOI has developed and implemented a plan for accepting and electronically verifying PIV credentials issued by other federal agencies and state or locally issued PIV Interoperable credentials.

If an individual is expected to work beyond 180 calendar days, a NACI and DOI Access Card must be issued in accordance with Personnel Bulletin 09-06 and the "Policy for the Issuance, Management and Use of Federal Personal Identity Verification (PIV) Cards (DOI Access Cards)."

To comply with this directive, bureaus/offices employing short-term emergency response personnel shall:

- A. Apply adequate controls to systems and facilities.
- B. Ensure that short-term emergency response personnel report to the Incident Command Post (ICP) or local office and complete the identity proofing process:
  1. The short-term emergency response personnel are required to appear in person and provide two forms of identification in original form to the local official. The list of acceptable identity documents are identified in List A or List B from the Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal government-issued picture identification (ID). The second document could be an incident qualifications card (Red Card).
  2. The local official shall visually inspect the identification documents and authenticate them as being genuine and unaltered, and subsequently compare the picture on the source document with the Applicant.
  3. If all of the above checks are deemed to be successful, the local official shall make a record of the two identity documents presented, sign the record, and keep it on file.
- C. Successfully adjudicate a National Criminal History Check (NCHC fingerprint check) prior to granting logical access to information systems.

- D. Provide short-term emergency response personnel with clear documentation on the rules of behavior and consequences for violation before granting access to facilities and/or systems.
- E. Document any security violations involving these personnel, and immediately report them to the appropriate authority.

Standardized policies and procedures for DOI emergency responders to accomplish this will be jointly developed by the Department's Office of the Chief Information Officer (OCIO), Office of Human Resources, DOI Access Program Management Office; and the Office of Emergency Management (OEM). These policies and procedures will be implemented by the end of calendar year 2011. The Plan of Action and Milestone (POA&M) process shall be utilized to document the corrective action plans to mitigate the risk due to the lack of interagency agreements and capability to quickly process this category of individuals. DOI will accept this risk until the corrective action plans are completed.

As an interim measure for CY 2011, to help mitigate risks to an acceptable level, this directive requires execution of the following steps:

- A. Offices shall 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. Offices shall follow local procedures and protocols in documenting the granting of these short-term accounts.
- B. The local office must complete the identity proofing process, defined in section B. above, before granting logical access.

And...

- C. Short-term emergency response personnel are instructed to follow all Information Management and/or Information Technology (IT) security policies, regulations, and practices of the Department.
  - 1. Regarding the use of IT, this includes protection of the Government's investment in computers and network components, not sharing passwords, not allowing unauthorized use of computers, adhering to proper use of the Internet, and following all current IT security practices and procedures.
  - 2. Regarding Information Management, it includes following all DOI policies and procedures with respect to privacy, Freedom of Information Act (FOIA), and records management. Such procedures include maintaining confidentiality and otherwise protecting privacy information, maintaining the confidentiality of all agency sensitive information, and protecting records of the Department. It also involves preserving all records associated with records retention orders.
- D. Each bureau shall also provide these short-term emergency response personnel and Information Technology Security Awareness and Best Practices handouts and provide

an Information Management Awareness and Best Practices Guide handout such as those contained in Attachments B and D, respectively. A procedure for tracking Information Technology Security Awareness is provided in Attachment A.

- E. Each Bureau must establish a Service Level Agreement (SLA) with the jurisdictional Assistant Director for Information Resources. The SLA shall document the purpose and responsibility of all involved parties. The SLA must be in place prior to establishing the user accounts for short-term emergency response personnel. A sample template is provided for the SLA as Attachment C.
- F. All short-term emergency response personnel covered under this policy shall display short-term access badges or a credential recognized by the federal government at all times. Identity credentials issued to short-term emergency response personnel by states or other federal agencies must be visually and electronically distinguishable from a standard PIV credential (i.e., DOI Access Card). Questions regarding this policy shall be directed to the applicable Bureau's Chief Information Security Officer or HSPD-12 lead designee.

cc: Bureau and Office Deputy Chief Information Officers  
Bureau and Office Chief Information Security Officers

Attachments:

- A. Sample Procedures for Tracking Information Technology Security Awareness for Short-Term Emergency Response Personnel
- B. Sample Information Technology Security Awareness and Best Practices Handout
- C. Service Level Agreement (SLA) Template Example
- D. Information Management Awareness and Best Practices Guide