



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

DEC 03 2009



Department of the Interior Acquisition Policy Release (DIAPR) 2010-04

SUBJECT: Implementation of Homeland Security Presidential Directive-12 (HSPD-12) Part 2, DOI Access Program Implementation

- 1. Policy:** This policy release establishes procedures for implementation of the DOI Access Program in DOI contracts. This DIAPR supersedes DIAPR 2006-03, Implementation of Homeland Security Presidential Directive-12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors.
- 2. Effective Date:** Upon signature.
- 3. Expiration Date:** Upon revision of the DIAR to incorporate these requirements.
- 4. Background and Explanation:** HSPD-12, issued on August 12, 2004, directed the creation of a new Federal standard for secure and reliable identification issued by Federal agencies to their employees and contractors, including all tiers of subcontractors. Implementation of HSPD-12 is being carried out in two stages. DIAPR 2006-03 addressed implementation of the first stage, known as Personal Identity Verification (PIV)-I. This DIAPR addresses implementation of PIV-II, known in the Department as the DOI Access Program. This program implements a standard process for personal identity verification and issuance of DOI Access Cards to DOI employees and contractors, as outlined in Personnel Bulletin 09-06 dated June 1, 2009. The DOI Access Card is the only authorized access card and replaces all bureau-issued access cards.

Which Contractor Employees Need DOI Access Cards?

Contractor employees, including subcontractors, requiring routine physical access for more than 180 calendar days, or unsupervised logical access, will need DOI Access Cards. See below for descriptions of *physical access* and *logical access*. See "Guidance on Who Should Receive DOI Access Cards," which will be posted to the DOI Access Web site at <https://portal.doi.net/doiaccess>, for a decision tree that will assist in determining which contractor employees will need PIV credentials.

Physical Access means routine, unescorted or unmonitored access to non-public areas of a Federally controlled facility. A "Federally controlled facility" is Federally owned or leased space, whether for single or multi-tenant occupancy, all or any portion of which is under the jurisdiction, custody or control of DOI. If a building is shared with non-government tenants, only access to the Federal area

is controlled. The requirements for contractor credentialing apply even if there is no guard, card reader, or other physical control at the entrance to the office.

Logical Access means routine, unsupervised access to a Level 3 or 4 Federally controlled information system. An “information system” is defined in the Federal Information Security Management Act of 2002 (44 U.S.C. §3503(8)). Use of an information system by a contractor on behalf of an agency is described in 44 U.S.C. §3544(a)(1)(A). If a contractor employee needs any amount of unsupervised access to a DOI information system, the employee must be issued a DOI Access Card. The credentialing requirements apply whether the contractor accesses the information system from the premises of a DOI facility, from their own facility, through the Internet, or by any other means. Credentialed contractor employees are also required to comply with OCIO policies for network access, including periodic information technology (IT) security training.

What About Contractor Employees Needing Only Temporary and/or Intermittent Access to DOI Facilities?

Contractors who do not need physical or logical access as described above, but need temporary and/or intermittent access to DOI facilities or information systems will be treated as visitors and issued alternate credentials. This group includes temporary and seasonal workers, and those needing intermittent physical access such as delivery services. These persons must access the facility via a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times. Normally, persons working exclusively outside on the grounds of Federally controlled facilities, such as grounds maintenance workers, parking attendants, and some construction workers, need not receive DOI Access Cards.

Special Cases

Risk. The preceding paragraphs describe the minimum requirements. Depending on risk, increased application of DOI Access credentialing requirements will be appropriate in some cases. Workers at construction sites may or may not need DOI Access Cards depending on the nature of what is being built. For example, it may be appropriate to credential workers on a critically sensitive dam. Similarly, grounds workers at a sensitive site, such as the White House, should be credentialed.

Failure to Obtain DOI Access Card. Should a contractor’s DOI Access Card be declined or revoked, the contract administration team must take some action to accommodate this in the contract. For example, the contract may have to be terminated if there is no alternative to on-site performance by the individual in question. On the other hand, it may be possible to arrange off-site performance or some other accommodation. In any case, the contracting officer must work together with the COR/COTR, security personnel, and the contractor to address this situation promptly.

Contractor Employees with Existing Clearances. If contractor personnel have already been investigated by another agency through OPM, the results of a prior National Criminal History Check (or higher) clearance will be accepted by DOI upon receipt of appropriate verification. These contractor employees will not be required to complete a new investigation before being issued the DOI Access Card.

5. **Action Required:** *Bureau Head of the Contracting Activity (HCA).* Per the DOI Access Implementation and Operations Plan memorandum, dated November 23, 2009, HCAs are required to coordinate with their DOI Access Bureau Leads to identify the DOI Access Card Sponsor, Adjudicator and Security Officer who will be responsible for processing of contractor employees, and to assign duties to each. A list of the DOI Access Bureau Leads will be posted to the DOI Access Web site at <https://portal.doi.net/doiaccess> . See “DOI Access Card Management Process,” also available on the DOI Access Web site, for a flow chart that shows the responsibilities of each role involved in the process.

Bureau Procurement Chief (BPC). BPCs should distribute this DIAPR as widely as possible, including to requisitioners. Coordinate with program offices and other requisitioners to ensure that the new procedures are followed and that contract work is not delayed. In conjunction with the bureau DOI Access Card Sponsor, tailor the Model Statement of Work/Performance Work Statement Language shown below as necessary to implement the bureau DOI Access Program in accordance with the DOI Access Implementation and Operations Plan memorandum.

Contracting Officer (CO). COs must inform existing contractors subject to contract PIV requirements of the new requirement to have DOI Access Cards issued to their affected employees. COs must insert the Model Statement of Work/Performance Work Statement Language shown below, or language substantially similar to the model language as tailored by the BPC, in the work statement of new solicitations and contracts that require contractor personnel to have physical or logical access as described above. COs must work with their COR/COTRs to determine whether PIV requirements are applicable to existing contracts, and at the earliest opportunity, but no later than exercise of an option, modify these applicable contracts to include the model language. COs must also include the Federal Acquisition Regulation clause 52.204-9, Personal Identity Verification of Contractor Personnel, in applicable contracts.

Contracting Officer's Representative (COR)/Contracting Officer's Technical Representative (COTR). COR/COTRs will have duties related to the DOI Access Program, and these should be reflected in the COR/COTR appointment letter. COR/COTRs will act as Requestors for contractor personnel in accordance with the DOI Access Requestor's Guide, which may be found at <https://portal.doi.net/doiaccess> . In this capacity, they will be responsible for determining the need for a contractor employee to obtain a PIV credential, and then initiating the DOI Access Card request in the DOI Access System at

<https://portal.doi.net/doiaccess> . The COR must also ensure that credentials are renewed and rescinded in a timely manner in the case of a change in contractor personnel, termination of the contract, etc. It is the COR's responsibility to make sure that contractors' credentials are returned to the DOI Access Card Sponsor (Sponsor) at the end of the contract or whenever a contractor employee's affiliation with DOI ends, and that lost cards are reported promptly to the Sponsor. The COR may delegate physical control of DOI Access Cards to another DOI employee in cases where contractor employees are not located within reasonable travel time of the COR. The COR may initiate alternate credentialing procedures (use PIV-I procedures) for a contractor employee not located within reasonable travel time of a USAccess Credentialing Center.

Model Statement of Work/Performance Work Statement Language

Contractor Personnel Security and Suitability Requirements

Performance of this contract requires contractor personnel to have a Federal government-issued Personal Identity Verification (PIV) credential before being allowed unsupervised access to a DOI [facility and/or information system]. The Contracting Officer's Representative (COR) or Contracting Officer's Technical Representative (COTR) will be the requesting official, and will make arrangements through a DOI Access Card Sponsor for personal identity verification and DOI Access Card issuance.

At least two weeks before start of contract performance, the Contractor must identify all contractor and subcontractor personnel who will require [physical and/or logical] access for performance of work under this contract. *Physical Access* means routine, unescorted or unmonitored access to non-public areas of a Federally-controlled facility. *Logical Access* means routine, unsupervised access to a Level 3 or 4 Federally controlled information system. The Contractor must make their personnel available at the place and time specified by the COR/COTR or DOI Access Card Sponsor in order to initiate screening and background investigations. The following forms and inquiries, or their equivalent, will be used to initiate the credentialing process:

- OPM Standard Form 85 or 85P
- OF 306
- National Criminal History Check (NCHC) (local procedures may require the fingerprinting to done at a police station; in this case, any charges are to be borne by the contractor)
- Release to Obtain Credit Information
- PIV card application (web-based)

Before starting work under this contract, a National Criminal History Check (NCHC) will be initiated to verify the identity of the individual applying for clearance and to determine the individual's suitability for the position. If the NCHC adjudication is favorable, a DOI Access Card will be issued for that individual. If the adjudication is unfavorable, the credentials will not be issued and the contractor must make other arrangements for performance of the work. In the event of a disagreement between the Contractor and the

Government concerning the suitability of an individual to perform work under this contract, DOI shall have the right of final determination.

Contractor employees must give, and authorize others to give, full, frank, and truthful answers to relevant and material questions needed to reach a suitability determination. Refusal or failure to furnish or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the contractor personnel being screened or investigated in person, by telephone or in writing, and the Contractor must ensure they are available for such contact.

Alternatively, if an individual has already been credentialed by another agency through OPM, and that credential has not yet expired, further investigation may not be necessary. In that case, the contractor must provide the COR/COTR with documentation that supports the individual's credentialed status.

Contractor employees who have been successfully adjudicated will be issued DOI Access Cards, which must be activated at a USAccess Credentialing Center. Those Contractor employees not located within a reasonable travel time of a USAccess Credentialing Center will be screened and issued alternate credentials, such as temporary access badges.

During performance of the contract, the Contractor must keep the COR/COTR apprised of changes in personnel to ensure that performance is not delayed by compliance with credentialing processes. Cards that have been lost, damaged, or stolen must be reported to the COR/COTR and Issuing Office within 24 hours. If reissuance of expired credentials is needed, it must be coordinated through the COR/COTR.

At the end of contract performance, or when a contractor employee is no longer working under this contract, the Contractor must ensure that all identification cards are returned to the COR/COTR.

This requirement must be incorporated into any subcontracts that require subcontractor personnel to have routine unsupervised access to a Federally controlled facility for more than 180 calendar days or any unsupervised access to a Federally controlled Level 3 or 4 information system.

6. **Additional Information:** If you have questions about this matter, please contact Tiffany Schermerhorn at (202) 513-0747 or Tiffany_Schermerhorn@ios.doi.gov.



Debra E. Sonderman, Director
Office of Acquisition and Property Management