



**Department of Energy
Acquisition Regulation**

**No. AL-2005-16
Date 10/04/05**

ACQUISITION LETTER

This Acquisition Letter is issued under the authority of the DOE and NNSA Procurement Executives.

Subject: Implementation of HSPD-12

References: Homeland Security Presidential Directive 12 (HSPD-12)

Federal Information Processing Standard Publication 201 (FIPS Pub 201)

DOE Notice 206.2 Identity Proofing

Acquisition Letter 2005-10 dated July 7, 2005

When is this Acquisition Letter (AL) Effective?

This AL is effective upon issuance.

When does this AL Expire?

This AL remains in effect until superseded or canceled.

Who is the Point of Contact?

Contact Robert M. Webb of the Office of Procurement and Assistance Policy at (202) 287-1338 or Robert.Webb@hq.doe.gov.

Visit our website at www.pr.doe.gov for information on Acquisition Letters and other policy issues.

What is the Purpose of this Acquisition Letter?

This is the second Acquisition Letter implementing HSPD-12 and FIPS Pub 201 in the solicitation and award of contracts involving physical access to agency premises and electronic authentication and access control to Federal agency's computer systems and electronic infrastructure. DOE has promulgated the requirements for identity proofing covered by this AL as they affect Federal employees and DOE's M&O and other major facilities contractors in DOE Notice 206.2, dated September 14, 2005, and its associated Contractor Requirements Document, respectively. This AL provides guidance on implementation of the identity proofing requirements of HSPD-12 and FIPS Pub 201 for all other DOE contracts. As used in this AL, reference to DOE includes both NNSA and non-NNSA sites.

What is the Background?

On August 27, 2004, President Bush issued HSPD-12, entitled, "Policy for a Common Identification Standard for Federal Employees and Contractors." See, <http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html>. The Directive states that it is the "policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees)."

This policy requires agencies to interconnect badging, physical access, and logical authentication and subsequent access control systems, that is, systems for electronic access to agency electronic infrastructure. When fully implemented, an enhanced employee's or contractor's badge or access authorization, will be necessary for physical access to agency premises and electronic authentication and access control to the agency's computer systems and electronic infrastructure. In the latter case, under normal circumstances, the enhanced employee and contractor badge will take the place of ID/password based authentications for access to the agency's infrastructure, but not necessarily to individual applications, such as Corporate Human Resource Information System (CHRIS), Industry Interactive Procurement System (IIPS), etc. Additionally, when all components of FIPS PUB 201 are fully implemented, one agency's badge or access authorization will be interoperable among Federal agencies, with the host agency retaining responsibility for granting access.

In pursuit of this policy, the Department of Commerce has developed FIPS Pub 201, entitled, "Personal Identification Verification for Federal Employees and Contractors." FIPS Pub 201 is available at <http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf>. All Federal agencies are required to implement the identity verification and management and badge issuance objectives of FIPS Pub 201 by October 27, 2005. Full implementation of FIPS PUB 201 is required by October 2008. The DOE CIO is leading the intra-agency project team, which includes representatives of the Office of Security and Safety Performance Assurance (SSA), the Office of Management Budget and Evaluation, DOE program offices, NNSA, the Defense Nuclear Facilities Safety Board, the power marketing

AL 2005-16 (10/04/05)

administrations, and the Federal Energy Regulatory Commission, responsible for DOE-wide implementation.

AL 2005-10, dated July 7, 2005, provided guidance on the planning, solicitation, evaluation, and award of all procurements for hardware and software components of DOE's physical access and electronic infrastructures. See <http://professionals.pr.doe.gov/ma5/MA-5Web.nsf/Procurement/Acquisition+Letters?OpenDocument>.

Implementation of HSPD-12 and FIPS Pub 201 requires a more rigorous process for identity proofing of Federal and contractor employees prior to their receiving a credential that allows physical access to a DOE-owned or -leased facility. The identity proofing process does not affect the process for applying for a security clearance, only applying for a security badge allowing physical access. This AL implements HSPD-12 and FIPS Pub 201, as they relate to contractor employee physical access to a DOE-owned or leased facility. One should note that no monies are available specifically to implement HSPD-12 or FIPS Pub 201.

What is the Effect on DOE Procurements and Contracts?

Contracting Officers shall insert the clause in Attachment 1 in solicitations and contracts, other than for DOE Management and Operating (M&O) or other major facilities solicitations and contracts, under which an employee(s) of the contractor will require a security badge, allowing physical access to a DOE-owned or leased facility, for a period of more than six (6) months or such lesser period as may be determined by the program official, in coordination with the cognizant security office.

Contracting Officers may negotiate this clause into active contracts, other than for DOE M&O or other major facilities solicitations and contracts, in effect on October 27, 2005, under which new employee(s) of the contractor will require a security badge, allowing physical access to a DOE-owned or leased facility, for a period of more than six (6) months or such lesser period as may be determined by the program official, in coordination with the cognizant security office as necessary to assure compliance with the identity proofing requirements of the clause.

DOE has implemented the requirements for identity proofing covered by this AL as they affect Federal employees and DOE's M&O and other major facilities contractors in DOE Notice 206.2, dated September 14, 2005, and its associated Contractor Requirements Document, respectively.

ATTACHMENT I- MODEL CONTRACT CLAUSE TO IMPLEMENT IDENTITY PROOFING REQUIREMENTS OF HSPD-12 AND FIPS PUB 201

ARTICLE XXX-ACCESS TO DOE –OWNED OR LEASED FACILITIES

(a) The performance of this contract requires that employees of the Contractor have physical access to DOE-owned or leased facilities; however, this clause does not control requirements for an employee's obtaining a security clearance. The Contractor understands and agrees that DOE has a prescribed process with which the Contractor and its employees must comply in order to receive a security badge that allows such physical access. The Contractor further understands that it must propose employees whose background offers the best prospect of obtaining a security badge approval for access, considering the following criteria, which are not all inclusive and may vary depending on access requirements:

- (1) is, or is suspected of being, a terrorist;
- (2) is the subject of an outstanding warrant;
- (3) has deliberately omitted, concealed, or falsified relevant and material facts from any Questionnaire for National Security Positions (SF-86), Questionnaire for Non-Sensitive Positions (SF-85), or similar form;
- (4) has presented false or forged identity source documents;
- (5) has been barred from Federal employment;
- (6) is currently awaiting a hearing or trial or has been convicted of a crime punishable by imprisonment of six (6) months or longer; or
- (7) is awaiting or serving a form of pre-prosecution probation, suspended or deferred sentencing, probation or parole in conjunction with an arrest or criminal charges against the individual for a crime that is punishable by imprisonment of six (6) months or longer.

(b) The Contractor shall assure:

(1) In initiating the process for gaining physical access, (i) compliance with procedures established by DOE in providing its employee(s) with any forms directed by DOE, (ii) that the employee properly completes any forms, and (iii) that the employee(s) submits the forms to the person designated by the Contracting Officer.

(2) In completing the process for gaining physical access, that its employee (i) cooperates with DOE officials responsible for granting access to DOE –owned or leased facilities and (ii) provides additional information, requested by those DOE officials.

(c) The Contractor understands and agrees that DOE may unilaterally deny a security badge to an employee and that the denial remains effective for that employee unless DOE subsequently determines that access may be granted. Upon notice from DOE that an employee's application for a security badge is or will be denied, the Contractor shall promptly identify and submit the forms referred to in subparagraph (b)(1) of this clause for the substitute employee. The denial of a security badge to individual employees by DOE shall not be cause for extension of the period of performance of this Contract or any contractor claim against DOE.

AL 2005-16 (10/04/05)

(d) The Contractor shall return to the Contracting Officer or designee the badge(s) or other credential(s) provided by DOE pursuant to this clause, granting physical access to DOE -owned or leased facilities by the Contractor's employee(s), upon (1) the termination of this Contract; (2) the expiration of this Contract; (3) the termination of employment on this Contract by an individual employee; or (4) demand by DOE for return of the badge.

(e) The Contractor shall include this clause, including this paragraph (e), in any subcontract, awarded in the performance of this Contract, in which an employee(s) of the subcontractor will require physical access to DOE -owned or leased facilities.