UNITED STATES DEPARTMENT OF COMMERCE
Chief Financial Officer and
Assistant Secretary for Administration
Washington, D.C. 20230

NOV - 2 2005

PROCUREMENT MEMORANDUM 2006-01

ACTION

MEMORANDUM FOR: HEADS OF CONTRACTING OFFICES

FROM: Michael S. Sade
Director of Acquisition Management
And Procurement Executive

SUBJECT: Guidance for Implementation of Homeland Security Presidential Directive 12 (HSPD-12) in Contracts

Background

On August 27, 2004, President Bush issued Homeland Security Presidential Directive 12 (HSPD-12), entitled "Policy for a Common Identification Standard for Federal Employees and Contractors". The directive requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. As required by the directive, the Department of Commerce (DOC) issued Federal Information Processing Standards Publication Number 201 (FIPS PUB 201), "Personal Identity Verification (PIV) of Federal Employees and Contractors". FIPS PUB 201 provides detailed specifications for identification issued by Federal departments and agencies to Federal employees and contractors for gaining physical access to Federally controlled facilities and logical access to Federal information systems. FIPS PUB 201 is available at http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201-022505.pdf.

In accordance with the directive, all Federal agencies are required to implement the minimum requirements for a Federal personal identification system that meets the control and security objectives of the directive, including the personal identity proofing, registration, and issuance process for employees and contractors by October 27, 2005. Full implementation of FIPS PUB 201 is required by October 2008. In order to facilitate implementation of the directive throughout the Department, DOC has established the Credential Management Program Office (CMPO) within the Office of the Secretary, Director for Security. The CMPO will make policy recommendations and develop the Department's Credential Reliability Program to include associated services (i.e., identity proofing, credential management, etc.) for the Department.

Purpose and Scope

The purpose of this procurement memorandum is to implement HSPD-12 and direct the use of FIPS PUB 201 in the solicitation and award of contracts involving physical access

to agency premises and electronic authentication and access control to agency computer systems and electronic infrastructure.

Acquisition Policy

PIV Sponsors: Contracting Officer Representatives (CORs) will serve as PIV sponsors for contractor personnel. Contracting Officers shall ensure the COR Delegation and Appointment Memorandum outlines duties for PIV sponsors. In order to facilitate the PIV credential process, a copy of applicable HSPD-12 award documents should be submitted to the CMPO within 5 days after award.

As PIV sponsors, CORs will be responsible for ascertaining the risk level for the contract and the positions required to complete the work, including credentialing requirements, facilitating the vetting process, and ensuring that credentials are renewed and rescinded in a timely manner. Procedures for sponsorship are specified at Office of Security (OSY) website http://www.osec.doc.gov/osy/HSPD12/HSPD-12Information.htm. CORs shall refer to NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems* (http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf), and the Commerce IT Security Program Policy, Section 7.4 (http://www.osec.doc.gov/cio/ITSIT/DOC-ITSecuirty-Program-Policy.htm), for assistance in determining the risk designation of positions that involve access to Commerce IT systems.

Physical Access: When a contract requires contractor personnel to have unsupervised physical access to a Federally controlled facility for more than 180 days; HSPD-12 compliant credentials must be issued. The 180 day period begins on the date contract performance begins and ends exactly 180 days later. Contractor personnel that require only intermittent access to federally controlled facilities are not required to undergo the PIV credential process. This group includes delivery service, vending machine service, and other transient service personnel. A "Federally controlled facility" is any 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 DOC. If a building is shared with non-government tenants, only access to the Federal area is controlled.

Logical Access: When Commerce authorizes contractor personnel an account to access a Commerce IT system (either for log-in locally or remotely), then the person must be in possession of the PIV credential for identification and authentication before access is permitted. The COR must document in the Statement of Work the maximum level of access required for the contractor to perform their duties (such as full access for system administration, read/write only access for basic user functions, etc.).

Electronic Infrastructure: Procurements for hardware, software, or services that involve the purchase of hardware or software associated with physical access to DOC facilities or logical access to DOC IT hardware or software (i.e., computer components, servers, local area network components, and other related hardware and software) must be reviewed for compliance with HSPD-12 and FIPS PUB 201. CORs shall coordinate with designated representatives of the Office of Security (OSY) for compliance with physical access

requirements and the Office of the Chief Information Officer (OCIO) for compliance with logical access requirements.

Action Required

Physical and Logical Access: Contracting Officers shall insert language to comply with the HSPD-12, FIPS PUB 201, and OMB Memorandum M-05-24 in solicitations and contracts when performance requires contractors to have physical access to a Federally controlled facility for more than 180 days or access to a Federal information system. Current contracts that require contractor personnel to have physical or logical access as described above must be modified to include the PIV requirements when an option is exercised, or when the contract term will extend past October 27, 2007. Attachment A contains a model contract language for use in affected solicitations and resulting contracts.

Electronic Infrastructure: For solicitations for the acquisition of hardware, software, or services that involve electronic infrastructure, Contracting Officers shall require the COR to submit the Statement of Work or Specifications to a designated representative of the OCIO and/or OSY, as appropriate, to address logical and/or physical access issues, for compliance with HSPD-12 and FIPS PUB 201. The Contracting Officer shall take appropriate action pursuant to the guidance received from the designated representative of the OCIO and/or OSY.

For current contracts with pending deliveries of hardware software, and services that involve electronic infrastructure, Contracting Officers must, in consultation with the COR, notify the designated representative of the OCIO and/or OSY, as appropriate, to address logical and/or physical access issues, of any items on the contract not yet delivered and accepted. The Contracting Officer shall take appropriate action pursuant to the guidance received from the designated representative of the OCIO and/or OSY.

Additional Information

For questions regarding the PIV credential process, the Credential Management Program Office (CMPO) point of contact is Ron Martin at (202) 482-4637 or rmartin@doc.gov. For questions regarding logical access requirements, contact Nancy DeFrancesco at (202) 482-3490 or NdeFrancesco@doc.gov. For questions regarding this memorandum, contact Dao Vissering at (202) 482-4185 or dvissering@doc.gov.

ATTACHMENT A

MODEL CONTRACT LANGUAGE TO IMPLEMENT HSPD-12

The performance of this contract requires contractors to have physical access to Federal premises for more than 180 days or access to a Federal information system. Any items or services delivered under this contract shall comply with the Department of Commerce personal identity verification procedures that implement HSPD-12, FIPS PUB 201, and OMB Memorandum M-05-24. The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a Federally controlled facility or access to a Federal information system.