

Financial Assistance Policy And Oversight Division DOT Dash 2010-05

Date: July 30th, 2010

To: Financial Assistance Points of Contact

From: Financial Assistance Policy and Oversight Division

Subject: Homeland Security Presidential Directive Number 12 (HSPD-12)

Summary: The purpose of this memorandum is to accomplish the following:

- a. Provide information concerning implementation of Homeland Security Presidential Directive-12 (HSPD-12) and its requirement for personal identity verification (PIV); and
- b. Require contracting/procurement officers to include applicable HSPD-12 clauses in those Request for Applications (RFAs), grants, and cooperative agreement that require contractors or recipients to have routine physical access to DOT-controlled facilities or logical access (e.g., DOT Network, PRISM, Grants Management Systems, etc.) to DOT's information systems.

Background

Increasingly, contractors are required to have physical access to federally controlled facilities and information systems in the performance of government contracts. On August 27, 2004, in response to the general threat of unauthorized access to Federal government physical facilities and its information systems, the President issued Homeland Security Presidential Directive (HSPD12 (<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>)).

The primary objectives of HSPD-12 are to establish a process to enhance security, increase government efficiency, reduce identity fraud, and support the fight against global terrorism by establishing a mandatory, government-wide standard for verifying identity and providing badge credentials to its employees and contractors that routinely work in federally-controlled facilities and/or have physical access to federal information systems. In accordance with HSPD-12, this government-wide identification standard was issued in February, 2005, by the Secretary of Commerce's National Institute of Standards and Technology (NIST), and is referred to as FIPS 201, "Personal Identity Verification" (PIV) of Federal Employees and Contractors. Federal government agencies are required to use the FIPS 201 PIV standard for identifying and issuing new "smart card" ID to all individuals that routinely work in federally controlled facilities, or require access to federal information systems. The ID contains a computer chip of agency specific information. When HSPD-12 and FIPS 201 are fully implemented, there will be interoperability among federal agencies with respect to these new "smart card" IDs, allowing them to be accepted by fellow agencies as reliable identification.

Although HSPD-12 and FIPS 201 only mention employees and contractors, DOT is aware that there may be situations that require assistance recipients to work in DOT controlled space and/or use DOT information systems. As a result, DOT will apply the requirements of HSPD-12 policy to those applicable assistance awards. This DOT DASH addresses the impact of HSPD-12 on recipients that routinely access DOT space and/or require logical access to DOT information systems (e.g., DOT Network, PRISM, Grants Management Systems, etc.)

Required Actions

With regard to RFA solicitations and assistance awards that require the recipient (or recipient employees) to have routine physical access to DOT-controlled facilities (i.e. will be needing an ID for regular entry to DOT space), or have logical access (e.g., DOT Network, PRISM, Grants Management Systems, etc.) to DOT's information systems. Operating Administrations awarding financial assistance may need to include the acquisition clause (FAR 52.204-9) that appears in Attachment 1, in the memorandum. Further implementation guidance on this issue will be forthcoming.

Please direct questions to Ellen Shields at ellen.shields@dot.gov


Ellen Shields, Associate Director
Financial Assistance Management Division

Attachment



U.S. Department of
Transportation
Office of the Secretary
of Transportation

Memorandum

Subject: Contract Requirements – Homeland Security Presidential
Directive 12 (HSPD-12)

JUN 22 2010

From: Michael Lessrd, Director
Office of Security

George Fields, Acting Director
Acquisition and Financial Assistance Management

To: All Contracting Officers and Contracting Officer
Technical Representatives

PURPOSE: The purpose of this memorandum is to accomplish the following:

- a. Provide information concerning implementation of Homeland Security Presidential Directive-12 (HSPD-12) and its requirement for personal identity verification (PIV), and
- b. Require contracting/procurement officers to include applicable HSPD-12 clauses in those RFP/RFAs, contracts, grants, and cooperative procurements that require contractors or recipients to have routine physical access to DOT-controlled facilities or logical access (e.g., DOT Network, PRISM, CSAM, Delphi, etc.) to DOT's information systems.

BACKGROUND: Increasingly, contractors are required to have physical access to federally controlled facilities and logical access to information systems in the performance of government contracts. On August 27, 2004, in response to the general threat of unauthorized access to Federal Government physical facilities and information systems, the President issued Homeland Security Presidential Directive Number 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors. The primary objectives of HSPD-12 are to establish a process to enhance security, increase government efficiency, reduce identity fraud, and support the fight against global terrorism by establishing a mandatory, government-wide standard for verifying identity and providing access credentials to government employees and contractors who routinely work in federally-controlled facilities and/or have physical access to federal information systems.

In accordance with HSPD-12, a government-wide identification standard was issued in February 2005 by the Department of Commerce's National Institute of Standards and

Technology (NIST), and is referred to as FIPS 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors." Federal Government agencies are required to use the FIPS 201 standard for issuing new "smart card" identification cards to all individuals who routinely work in federally controlled facilities or who require access to federal information systems. The new identification card incorporates a computer chip containing information on the individual and agency specific information. When HSPD-12 and FIPS 201 are fully implemented, there will be interoperability among federal agencies with respect to these "smart card" identification cards, allowing them to be accepted by fellow agencies as reliable identification.

This memorandum addresses the impact of HSPD-12 on all non-federal individuals who routinely access DOT space and/or require logical access to our information systems.

In 2006 the Civilian Agency Acquisition Council and the Defense Acquisition Regulation Council issued rules that amended the Federal Acquisition Regulation (FAR) to reflect HSPD-12. These rules amended the FAR as follows:

- Added definitions of "federal information system" and "federally-controlled facilities" at FAR 2.101;

- Added Subpart 4.13, Personal Identity Verification of Contractor Personnel, to implement FIPS 201 and associated Office of Management and Budget (OMB) guidance. This section also requires all agencies to include language implementing the HSPD-12 Standard in applicable solicitations and contracts that require contractors to have access to a Federally-controlled facility or access to a Federal information system;

- Modified the security considerations in FAR 7.105(b)(17) to require the acquisition plan to address the agency's PIV requirements for contractors when applicable; and

- Added FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel, to require the contractor to comply with the PIV process for all affected employees in accordance with agency procedures identified in the contract. This new FAR clause 52.204-9, must be included in any solicitation or contract that requires contractors to have routine access to federally controlled space and/or access to federal information systems.

GUIDANCE: Attachment 1 to this memorandum contains mandatory language for all DOT solicitations and contracts where contractor employees must have routine access to federally controlled space and/or access to federal information systems. The language addresses the PIV requirements of HSPD-12. It alerts contractors and recipients about the two different personal identification documents they will be required to submit before they will be able to obtain a DOT identification card or be granted access to DOT information systems. The identity source documents must come from the list of acceptable documents that is available from the applicable DOT servicing security organization.¹ FAR clause 52.204-9 is included in Attachment 1.

¹ The DOT Security Office, M-40, is the servicing security organization for all DOT organizations except the FAA. For FAA, the servicing security organization is AIN-100.

REQUIRED ACTION:

RFP solicitations and contracts that require contractor employees to have routine physical access to DOT-controlled facilities (i.e. will be needing an identification card for regular entry to DOT space), or have logical access to DOT's information systems, must contain both the FAR clause 52.204-9 and the DOT HSPD-12 Personal Identity Verification clause that appear in Attachment 1.

Existing contracts, task orders (if applicable), and option extensions must be modified to include the clauses by July 1, 2010.

Attachment

ATTACHMENT 1

Mandatory contract language for all contracts requiring access to DOT facilities or information technology systems

(FAR Clause 52.204-9)

52.204-9 Personal Identity Verification of Contractor Personnel.

As prescribed in 4.1303, insert the following clause:

Personal Identity Verification of Contractor Personnel (Sept 2007)

(a) The Contractor shall comply with agency personal identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24 and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system.

Homeland Security Presidential Directive-12 (HSPD-12) (August 2004)

DOT HSPD-12 Personal Identity Verification clause:

Homeland Security Presidential Directive-12 was issued in response to the general threat of unauthorized persons gaining access to federal facilities and information systems. HSPD-12 requires all Federal agencies to use a common Personal Identity Verification (PIV) standard when identifying and issuing access rights to users of Federally-controlled facilities and/or Federal Information Systems.

To perform the work specified herein, contractor personnel will require access to sensitive data, regular access to DOT-controlled facilities and/or access to DOT information systems. The Government has determined the position risk/sensitivity level under this effort to be _____¹.

Accordingly, before any individual may obtain a DOT identification card (new or replacement) authorizing him/her routine access to DOT facilities, or logical access to DOT's information systems, the individual must provide two forms of identity source documents in original form. One identity source document must be a valid Federal or state government-issued picture identification card. DOT contractors must contact the DOT servicing security organization to obtain the list of acceptable forms of documentation. Submission of these documents, and related background checks, are mandatory in order for the contractor to receive a building access identification card, and before access will be granted to any of

¹ The following sentence may be substituted when multiple risk/sensitivity levels apply: "The Government estimates that this effort will entail multiple levels of risk/sensitivity, ranging from _____ to _____; but risk/sensitivity levels cannot be ascertained definitively until after contract award."

DOT's information systems. Identification documents must be presented again in order to receive the card after it is manufactured. DOT identification cards are government property and must be returned when access to government facilities or information systems is no longer authorized, e.g., upon termination of employment, upon the contractor's reassignment of the employee to a non-DOT project, upon termination of the contract, or upon demand by DOT.

The minimum Government investigation for a low risk or non-sensitive position is a National Agency Check and Inquiries (with fingerprinting), which consists of searches of records covering specific areas of a person's background during the past five years. Those inquiries are sent to current and past employers, schools attended, references, and local law enforcement authorities. Higher level positions, above low risk/non-sensitive, require more extensive documentation and investigation.

Contractors should ensure that the employees whose names they submit have a reasonable chance for access approval. Delays associated with rejections and consequent reinvestigations may not be excusable.²

The contractor must comply with all applicable HSPD-12 and PIV procedures, as described above, and any subsequent DOT or government-wide HSPD-12 and PIV procedures/policies, including any subsequent related DOT directives and required procedures.

In the event of inconsistencies between this clause and later issued agency or government wide HSPD-12 guidance, the most recently issued guidance shall take precedence, unless otherwise instructed by the Contracting Officer.

The contractor is required to include this clause in any subcontracts that require the subcontractor or subcontractor employee to have routine physical access to DOT space or logical access to a DOT information system.

² Investigations may delay performance, regardless of the outcome of the investigation. The facts surrounding individual cases will determine whether a delay is excusable.