# United States Department of the Interior

## Homeland Security Presidential Directive-12 (HSPD-12)

## Who Needs a Card?

**(Minimum Departmental Guidance)**

**5/22/07**

# Identity Control

# HSPD-12 Objective

- The overall goal of HSPD-12 is to achieve appropriate security assurance for **multiple applications** (primarily electronic access to government information systems and physical access to federally controlled facilities) by efficiently verifying an individual's claimed identity.
- This objective will be achieved by:
  - Developing a **common** reliable and verifiable identification system.
  - Assuring Government-wide interoperability and **reciprocity**.
  - **Mandated use** by all Government employees, contractors, and other classes of individuals (i.e. temporary employees, volunteers, tribal users, etc.) who are granted unsupervised access to federal computer systems and unsupervised physical access to federally controlled facilities.

# Individuals who will receive HSPD-12 compliant identification cards are (except as noted on the next slide)

1) **Federal employees**, as defined in title 5 U.S.C §2105 "Employee," within a department or agency.
2) DOI **specific categories of individuals** (e.g., contractors, guest researchers, tribal users, volunteers or intermittent, temporary or seasonal employees, etc.) who are affiliated with DOI for **more than 180 days** and require access to Federally controlled facilities (level 1-4) as defined on slide 7.
3) Individuals affiliated with DOI for more than 180 days who are granted unsupervised access to Federally controlled **information systems** (as defined on slide 6).
4) Individuals affiliated with DOI for more than 180 days who are granted unsupervised access to sensitive (but unclassified) information (i.e. FOUO, LE Sensitive, etc.)

# Supervised physical and logical access may be granted to certain individuals without the use of HSPD-12 compliant identification under the following conditions:

1) Individuals described as contractors, visitors, cooperatives, partners, guest researchers, volunteers, interns, and intermittent, temporary or seasonal employees, etc. who are affiliated with DOI less than 180 days. Please note: the 180 day period begins the first day the individual is affiliated with DOI and ends exactly 180 days later no matter the frequency or duration of the activity (ex: one or five days a week).

2) All of these individuals must be controlled when entering facilities using or operating federally controlled information systems. At a minimum, individuals must access the facility via a screening system, display a daily visitor badge at all times and be escorted or obtain an official Bureau temporary access badge (TAB).

3) Non-HSPD-12 (or TAB) compliant individuals who require access to Federally controlled information systems (because of contracts and/or agreements) must be directly supervised by an individual with an active HSPD-12 identification card.

4) Vendors, delivery services, recurring services contracts, or other individuals (e.g. volunteers) who do not access Federally controlled information systems but require sporadic physical access in excess of 180 days must access the facility via a screening system, display a daily visitor badge at all times, and be escorted.

5) If at any time a risk based analysis determines HSPD-12 compliant identification is warranted for a particular individual or facility, all exceptions listed in this section will be immediately rescinded.

6) Waiver of HSPD-12 compliant identification does not modify Federal investigative requirements, application of statutory standards of character, or implementation of national security systems requirements, e.g., 44 U.S.C. § 3542(2)(A), 18 U.S.C. § 921, 5 CFR Part 731, 5 CFR Part 732, 441 DM 5, 446 DM 2.

# Federally Controlled Information Systems

1) Information technology system (or information system), as defined by the Federal Information Security Management Act of 2002, (44 U.S.C. §3502(8)).
2) Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, (44 U.S.C. §3544(a)(1)(A).
3) Applicability for employee, contractor, or “other” class of individual’s access to Federal systems from a non-Federally controlled facility (e.g. researchers’ up-loading data through a secure website or a contractor accessing a government system from their own facility).
4) This Directive does not alter requirements for national security systems as defined by the Federal Information Security Management Act of 2002, (44 U.S.C. §3542(2)(A)).

# Federally Controlled Facilities:

1) Federally-owned buildings or leased space, whether for single or multi-tenant occupancy, and its grounds and approaches, all or any portion of which is under the jurisdiction, custody or control of the Department, its Bureaus or Offices (exceptions are maintenance or storage sheds that do not contain Federal information systems).
2) Federally controlled space located in non-government facilities. Example: DOI leased space on the 10th floor of a commercial building, the Directive applies only to the 10th floor.
3) DOI-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.
4) Educational institutions that meet the definition of federally controlled facility and/or enjoy privileged access to Federally-controlled information systems. Unless specifically designated by DOI, this Directive does not apply to Educational institutions that conduct activities on behalf of DOI, its Bureaus or Offices, or at which Federal employees are hosted.
5) Basically: DOI controls the access to a facility or space within a facility.

# Questions to Determine Who Needs a Card

**If you answer yes to any of the following questions, the individual will require a smart card or temporary access badge.**

1) **Is the individual a full time federal employee? (smart card)**
2) **Will the individual be granted un-supervised* access to a federal facility? (smart card or temporary access badge)**
3) **Will the individual be granted un-supervised access to a DOI IT System? (smart card or temporary access badge)**
4) **Will the individual (including specific category or other class of individuals, but not a "vendor") be accessing DOI controlled facilities or DOI controlled space within a facility for more than 180 days on a regular basis? (smart card)**

*** For the purposes of HSPD-12, "supervised" is defined as being with and/or escorting the individual at all times.**

# Could This Have Been Prevented?

A16 SUNDAY, APRIL 22, 2007 THE WASHINGTON POST

NATION

## Engineer Jailed on Iran Trade Charges

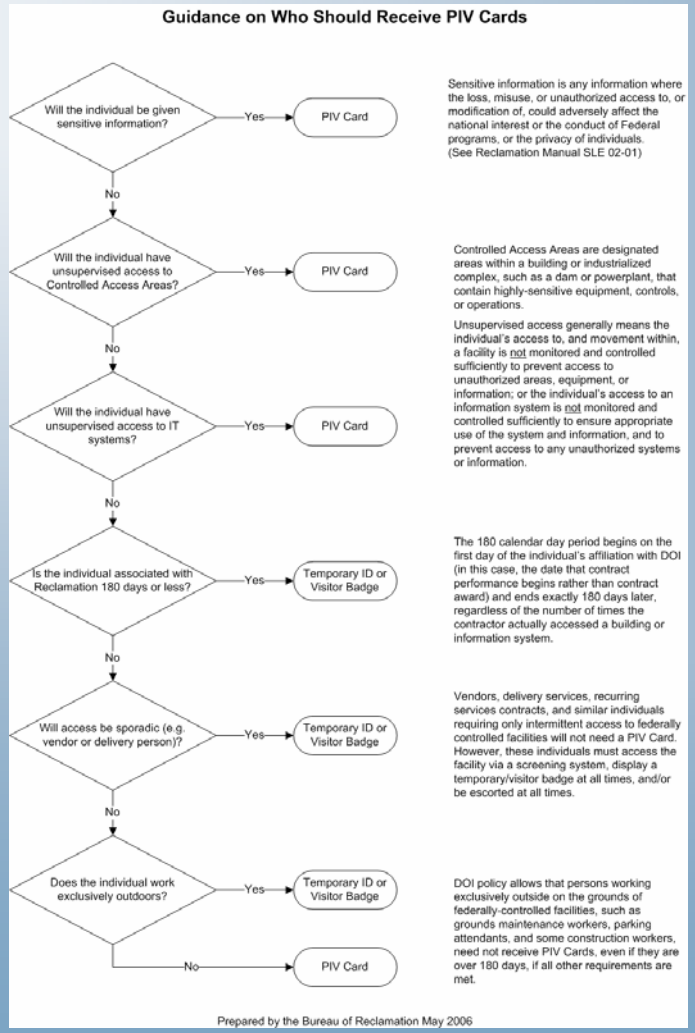
**PHOENIX** — A former engineer at the largest U.S. nuclear power plant allegedly took computer access codes and software to Iran, where he used them to download details of plant control rooms and reactors, officials said Saturday.

Mohammad Alavi, who worked at the Palo Verde Nuclear Generating Station west of Phoenix, was arrested April 9 at Los Angeles International Airport when he arrived on a flight from Iran, authorities said.

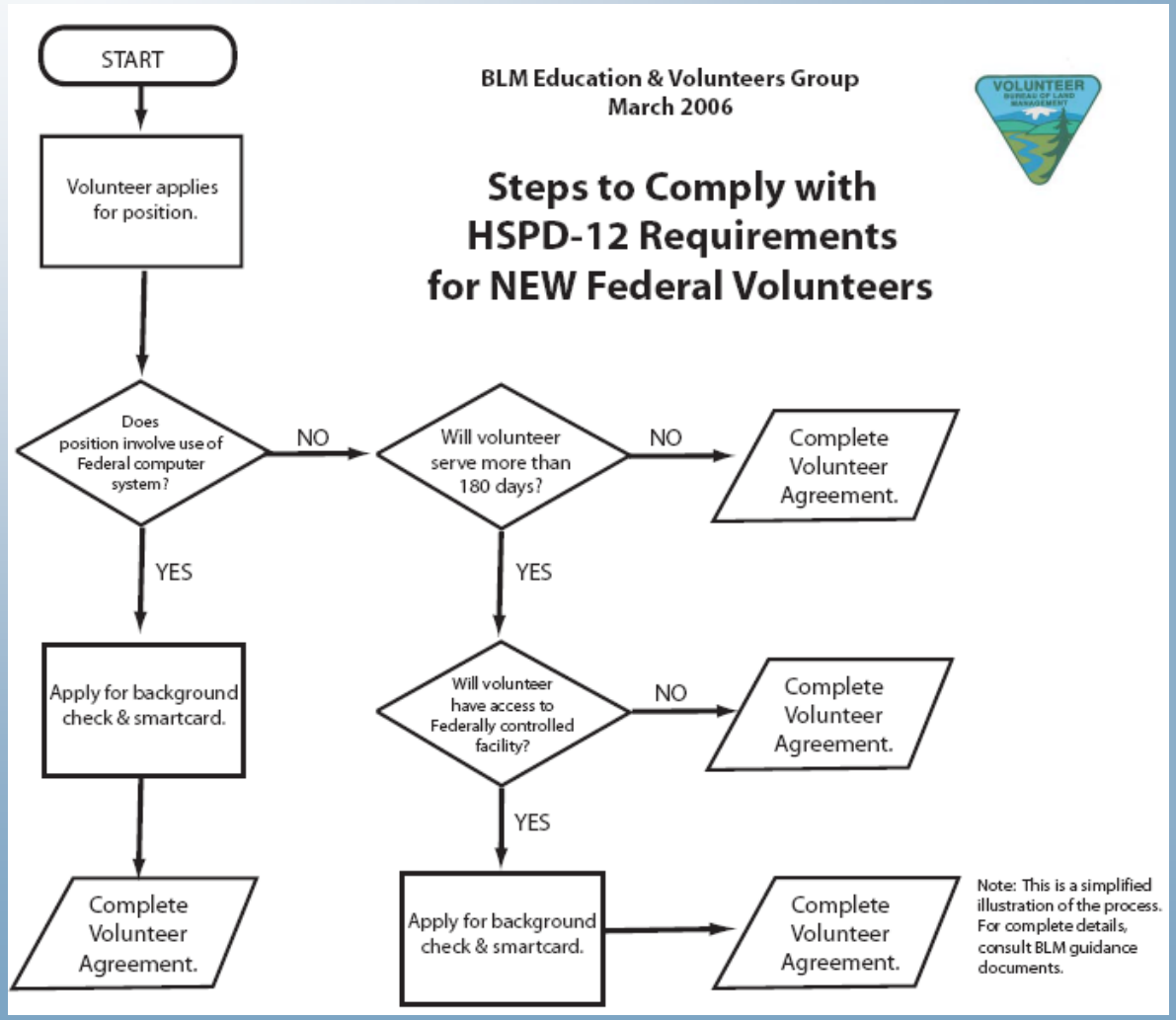
Alavi, 49, is charged with a single count of violating a trade embargo that prohibits Americans from exporting goods and services to Iran. A federal judge in Phoenix denied bail Friday, saying Alavi posed a substantial flight risk. Alavi's attorney said his client denies wrongdoing.

According to court records, the software is used only for training plant employees, but it provides users access to details on the Palo Verde control rooms and the plant layout. In October, authorities alege, the software was used to download training materials from Tehran, using a Palo Verde user identification.

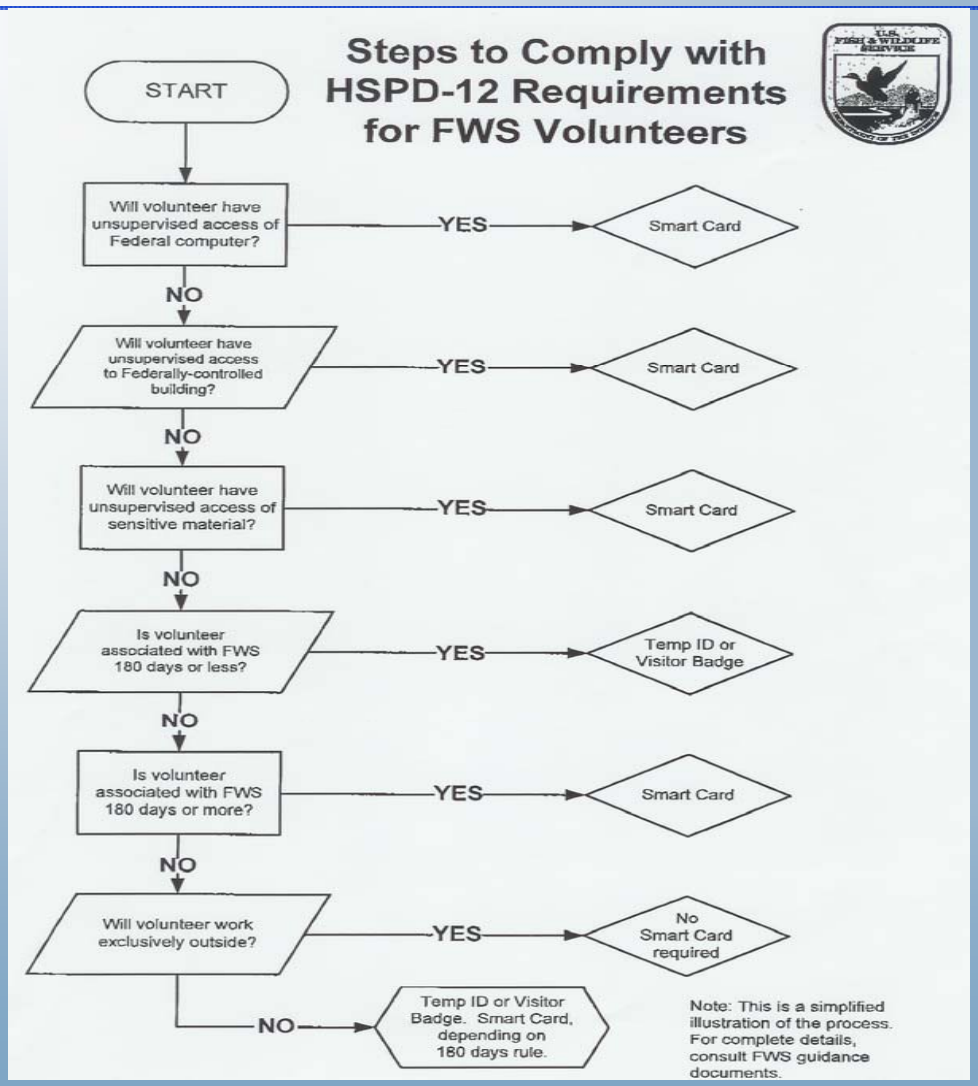
# BOR Policy


Guidance on Who Should Receive PIV Cards
Will the individual be given sensitive information?
Yes
PIV Card
No
Sensitive information is any information where the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy of individuals. (See Reclamation Manual SLE 02-01)
Will the individual have unsupervised access to Controlled Access Areas?
Yes
PIV Card
No
Controlled Access Areas are designated areas within a building or industrialized complex, such as a dam or powerplant, that contain highly-sensitive equipment, controls, or operations.
Unsupervised access generally means the individual's access to, and movement within, a facility is not monitored and controlled sufficiently to prevent access to unauthorized areas, equipment, or information; or the individual's access to an information system is not monitored and controlled sufficiently to ensure appropriate use of the system and information, and to prevent access to any unauthorized systems or information.
Will the individual have unsupervised access to IT systems?
Yes
PIV Card
No
Is the individual associated with Reclamation 180 days or less?
Yes
Temporary ID or Visitor Badge
No
The 180 calendar day period begins on the first day of the individual's affiliation with DOI (in this case, the date that contract performance begins rather than contract award) and ends exactly 180 days later, regardless of the number of times the contractor actually accessed a building or information system.
Will access be sporadic (e.g. vendor or delivery person)?
Yes
Temporary ID or Visitor Badge
No
Vendors, delivery services, recurring services contracts, and similar individuals requiring only intermittent access to federally controlled facilities will not need a PIV Card. However, these individuals must access the facility via a screening system, display a temporary/visitor badge at all times, and/or be escorted at all times.
Does the individual work exclusively outdoors?
Yes
Temporary ID or Visitor Badge
No
PIV Card
DOI policy allows that 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 PIV Cards, even if they are over 180 days, if all other requirements are met.
Prepared by the Bureau of Reclamation May 2006

# BLM Policy


START
BLM Education & Volunteers Group
March 2006
Steps to Comply with HSPD-12 Requirements for NEW Federal Volunteers
Volunteer applies for position.
Does position involve use of Federal computer system?
NO
Will volunteer serve more than 180 days?
NO
Complete Volunteer Agreement.
YES
YES
Apply for background check & smartcard.
Will volunteer have access to Federally controlled facility?
NO
Complete Volunteer Agreement.
YES
Complete Volunteer Agreement.
Apply for background check & smartcard.
Complete Volunteer Agreement.
Note: This is a simplified illustration of the process. For complete details, consult BLM guidance documents.

# FWS "Draft" Policy



# Departmental HSPD-12 Security Guidance Documents

1) Background Investigation of Contract Employees.
2) Guidance Regarding the Installation of Smart Card Readers at DOI Facilities.
3) Definition of Card Issuance and Facility Guidance Regarding HSPD-12.
4) Requirements for the DOI Personal Identity Verification Card (Smart Card) Visual Card Topography.
5) Public Trust Risk Designation Guidance for Individuals Actively Involved in the HSPD-12 PIV-1 Process.
6) OCIO Directive 2006-015 Controlled Logical Access Policy.
7) HSPD-12 Temporary Physical Access Badge Guidance.
8) HSPD-12 and Non-Citizens Guidance.