

What is Personal Identity Verification (PIV)?

On 27 August 2004, the President signed Homeland Security Presidential Directive 12 (HSPD-12). The directive requires that the Department of State and other Federal agencies implement a “*Federal standard for secure and reliable forms of identification that is issued based on sound criteria for verifying an individual employee’s or contractor’s identity.*”

Federal and contractor employees requiring long-term or frequent access to controlled facilities and/or logical access to controlled information must successfully complete a vetting process through an investigation such as a National Agency Check with Inquiries (NACI), or other National Security community investigation to confirm their identity and suitability for physical and logical access.

What does PIV require of me?

To receive a PIV credential, an Applicant must provide:

- *Two forms of identity source documents in their original form from the list of acceptable documents listed on Department of Homeland Security Form I-9 List A or B, one of which is a valid State or Federal government-issued picture ID, not expired;*
- *A passport photograph;*
- *Your fingerprints in card form, or live-scan if directed;*
- *A Standard Form SF-85P, or SF-86 as appropriate;*
- *Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act as appropriate;*
- *Standard Form SF-85PS (Supplemental Questionnaire) if required;*

- *Additional information to confirm your identity, or as required to complete the vetting process.*

Why must the DoS collect this information?

The DoS must collect this information to:

- *Conduct a NACI, or other National Security community investigation to establish your identity and suitability for access DoS facilities and/or information systems;*
- *Ensure the individual to whom the credential is issued is the same as the intended recipient on whom the background investigation was completed.*

What legal authority does the DoS have to collect this sensitive personal information?

The Department may collect this information pursuant to:

- *Privacy Act of 1974, as amended, under authority of 22 U.S.C. 2658;*
- *Executive Orders 10450 and 12968;*
- *Section 506(A) of the Federal Records Act of 1950.*

Can the DoS share the information collected?

The Department may lawfully share the personal information:

- *In the conduct of appropriate national agency checks;*
- *When appropriate to other Federal, State or municipal law enforcement agencies for law enforcement purposes;*
- *To agencies having statutory intelligence responsibilities;*
- *To agencies having oversight or review authority with regard to investigative responsibilities.*

Will my sensitive information be protected?

The Department protects all personal information by:

- *Restricting storage of PIV information in the electronic form to secure and accredited information systems;*
- *Restricting storage of hard-copy information to secure, controlled access facilities;*
- *Restricting access by DoS personnel to those having an explicit need to know acting in the performance of their duties, and trained in the protection of sensitive information and the PIV proofing and registration process;*
- *Restricting disclosure to only those Federal, State, or authorized municipal law enforcement agencies as allowed by law or regulation.*

Where do I go to receive my credential if my application is approved?

A representative from the Department office where you will work, or Human Resources office will explain the process to receive your credential and the locations where you may receive your credential.

What may I use my credential for?

Credentials issued by the DoS may only be used for:

- *Display when located within Department facilities or on DoS property closed to the public;*
- *Upon request of Federal Protective Officers, or other authorized individuals when entering, leaving or on DoS property;*
- *To access DoS information systems when required and in the use of Public Key Infrastructure (PKI) applications;*
- *For identity verification at other Federal and State facilities when required.*

Are there any restrictions on the use of my credential?

Department credentials may not be used for:

- Identification for any purpose other than those directly related to the performance of your duties as a DoS government or contractor employee;
- To assist others in gaining unauthorized access to Federal facilities, or information.

The unauthorized use of a credential, or attempt to clone, modify, or obtain data from any credential for any purpose will subject the offender to penalty/disciplinary action.

When must I replace my credential?

Credentials must be replaced when:

- The credential will expire within six (6) weeks, or is expired;
- The credential was lost:

Report loss immediately to the Security Control Center: (202) 647-0099.

Submit a brief memorandum to your supervisor stating the circumstances in which the credential was lost.

- The credential is stolen:

Report the theft immediately to the Security Control Center: (202) 647-0099.

File a report with the police in the jurisdiction of the theft.

Submit a copy of the police report, or memorandum to your supervisor.

- The data contained on the credential has been compromised:

Report loss immediately to the Security Control Center: (202) 647-0099.

- Your security clearance changes;

- When your personal information changes;
Name changes;
The photo no longer resembles you.

- The credential is damaged, or no longer serviceable.

If I am denied a credential, what are my rights?

If your PIV credential is denied or revoked, you may:

- Ask that a PIV Applicant Representative be assigned to assist you in removing any incorrect information that adversely affected the Identity Proofing process;
- Request an amendment of information you believe is not timely, accurate, relevant, or complete;
- File a written appeal with the Department of State, Diplomatic Security in accordance with current procedures.
- To reach a PIV Applicant Representative, call DS/DO/DFP at 202-647-4418.

Can I request the information on which the denial or revocation of my credential was based?

You may request the information that such decisions were based upon by making a request in writing under the Privacy Act. Records of denied/revoked credentials are kept for a period of 3-5 years.

- Requests should be sent to:

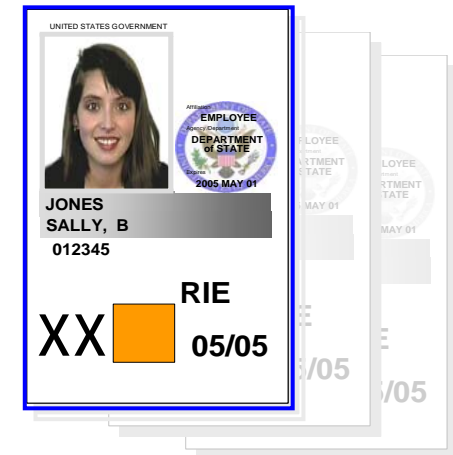
Office of Information Programs and Services
A/ISS/IPS/RL/RC
U. S. Department of State, SA-2
515 22nd Street, NW
Washington, DC 20522-6001

- Additional information may be found under FOIA on the U.S. Department of State Web site at www.state.gov.

The United States Department of State
Bureau of Diplomatic Security



Personal Identity Verification (PIV)



Applicant Rights And Responsibilities