

VA PIV Privacy Policy

1. Introduction

This privacy policy applies only to VA's PIV System. The PIV System was created in response to Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors." This directive requires secure and reliable identification that:

- Is based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.

The goal of HSPD-12 and the PIV System is to issue a standardized government identification card that is resistant to identity fraud, meets a minimum set of privacy standards, will be interoperable with other government agencies, will save time and improve security. The VA ID card can only be issued after identity is verified. It is extremely hard to fake, change, or duplicate, and it can only be issued by accredited employees.

2. Privacy Act

VA follows the requirements of the Privacy Act, which protects your personal information that we maintain in what are called systems of records. A system of records is a file, database, or program from which personal information is retrieved by name or other personal identifier. In other words, the Privacy Act applies when any personal information is used to verify identity or another interaction with VA takes place—such as when information is provided to establish employment. The Privacy Act provides a number of protections for personal information. These protections include how this information is collected, used, disclosed, stored and discarded.

The information and biometrics collected, as part of the Federal identity-proofing program under HSPD-12, are used to verify the personal identity of VA applicants for employment, employees, contractors, and affiliates (such as students, WOC employees, and others) prior to issuing Department identification credentials. The credentials themselves are to be used to authenticate electronic and physical access requests from VA employees, contractors, and affiliates through digital access control systems. These credential are also used to gain access to other federal government agency facilities and systems, where permitted by law.

The information collected is protected by the Privacy Act, and maintained under the authority of 38 USC 501 and 38 USC 901-905. The system of records notice for this system is 103VA07B, Police and Security Records-VA.

Failure to provide all of the requested information may result in a delay or inability to process requests for a VA ID card. It may also result in the denial of issuance of a VA ID card. The inability to obtain an ID card will result in the denial of access to VA facilities and networks. This could have an adverse impact on VA employee contractor or affiliate status where such access is required to perform assigned duties or responsibilities.

Examples of the information collected to perform background checks or to issue a VA ID card are:

<ul style="list-style-type: none">• Full Name• Home/work Address• Contact information (Phone/email)• Social Security Number (and/or an abbreviated version)• Other unique identifiers such as Green Card or Resident Alien number• Physical Attributes (Hair Color, Eye Color, Height, etc.)• Fingerprints or other biometrics• Facial image (photo)	<ul style="list-style-type: none">• Date of Birth• Place of Birth• Other names used• Sex• Citizenship• Where you have lived• Where you went to school• Employment activities• People who know you well• Selective service record• Military history• Illegal drug use
---	---

Notices are published in the Federal Register that describes in more detail when information about you may be made available to others. A copy of the System of Records Notice that covers the PIV System is available at:

<http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2002/pdf/02-31709.pdf>

3. Collection, Storage, Access and Use of Information

The information in this collection will be used solely for identity verification, background checks and issuance of a VA ID card. Information will be stored in paper form, in a secured container, and/or electronically in a secured information system. The Privacy Act System of Records Notice for this system details the safeguards used for the storage of the information in the PIV System. Access to this information is limited to those with a need-to-know, meaning that only those personnel whose duty it is register employees in the system, verify identification, issue credentials and administer and maintain the system, have access to this information.

The information provided will be used to:

- Verify identity
- Complete SAC and NACI background checks, if required
- Issue identification badges
- Authenticate physical and logical access attempts with identification badges.

A “routine use” disclosure of the information in this system of records may be made for: civil or criminal law enforcement, constituent congressional communications initiated at your request, litigation or administrative proceedings in which the United States is a party or has an interest, the administration of VA programs, verification of identity and status, and personnel administration by Federal agencies. Information displayed or stored on a VA ID Card may be provided without consent, as permitted by the Privacy Act:

- To the appropriate government organization if records show a violation or potential violation of law;
- To the Department of Justice, a court, or other decision-maker when the records are relevant and necessary to a law suit;
- To a federal state, local, tribal, or foreign agency that has records needed to decide whether to retain an employee, continue a security clearance, or agree to a contract;
- To a member of Congress or to Congressional staff upon written request;
- To the Office of Management and Budget to evaluate private relief legislation;
- To agency contractors, grantees, or volunteers who have agreed to comply with the Privacy Act and need access to records in order to do agency work;
- To the National Archives and Records Administration for records management inspections; and
- To other federal agencies for notification of card expiration, cancellation or revocation.

4. Privacy Complaints

If there is a belief that VA personnel have used PIV System information in a manner that is inconsistent with this policy and with the Privacy Act System of Records Notice, a complaint may be filed with your facility’s Privacy Officer. All complaints received by Privacy Officers must be logged, assigned a ticket, investigated and the results of the investigation recorded. For more information about how VA handles privacy complaints, refer to VA Handbook 6502.1 Privacy Violation Tracking System (PVTS).

5. Sanctions for Violating this Policy

All sanctions are handled by HR through the employee’s manager/supervisor. Sanctions will be handled on a case-by-case basis, but will be consistent with possible sanctions listed in VA Handbook 5021, Employee/Management Relations, for “failure to safeguard confidential matter” and “violations of the Privacy Act.”