U.S. Office of Personnel Management
Federal Investigative Services
Request for PIPS/CVS User ID/Access

Federal agencies may request direct access to OPM's Personnel Investigations Processing System (PIPS) and Central Verification System (CVS) for personnel, as needed to perform specified assigned duties, by completing this form. In order to receive PIPS/CVS access, individuals must be U.S. citizens and have a minimum level investigation of a Tier 2 or Tier 3, dependent on whether the individual occupies a public trust or national security position. To ensure proper use of system information, individuals nominated for system use must also be investigated, adjudicated and trained appropriately for the position they hold and the duties they perform.

Interim system access may be granted prior to the completion and favorable adjudication of the final investigation. To be granted interim access, the following is required:

- Completion of the standard investigative questionnaire to include applicable supporting documentation
- Submission and successful scheduling of the appropriate level of investigation (minimum T2 or T3 or equivalent)
- Favorable review of the standard questionnaire and supporting documentation by the appropriate adjudicating authority
- Completion of the following national agency checks with favorable review by the appropriate adjudicating authority:
    - FBI fingerprint (FBI CJIS)
    - FBI name check (FBIRMB)
    - OPM SII
    - DCII
- Interim clearance or access granted by the appropriate adjudicating authority, and entry of this decision into CVS

The established SOI Security Official will ensure the policies and security procedures for use of this system are understood by nominated users at the time the user is presented with this form for completion of Section 1. The Security Official will also ensure the user has obtained access to the NP2 Portal and has had the opportunity to read the CVS User Manual. Users must adhere to PIPS/CVS security policies as a condition for system access.

Completed, signed forms can be mailed or emailed via the NP2 Portal messaging as an attachment to OPM-FIS Agency System and Liaison (OPM-FIS ASL). OPM will make the access determination and provide the user with account access information.

Address questions regarding the completion of this form or PIPS/CVS access procedures to OPM staff at: (724) 794-5612, ext. 4600.

Section 1:

This section is to be completed by the user who will hold the individual account. All fields must be completed for access determination and shall be legible. The potential user must read, sign [1g], and date [1h]. If this section is incomplete, the request will be returned without action.

Section 2:

This section is to be completed by the user's immediate supervisor or the Security Official. Information in this section is mandatory and defines what specific system privileges the user may be granted by OPM.

2a – Provide Agency name and Division along with complete physical location.

2b – Provide OPM assigned 4 character Security Office Identifier (SOI: usually begins with alpha character) for user workload management.

2c – Provide the level of investigation from the subject's last complete investigation and check if the level of investigation was determined using the OPM Position Designation System.

2d – Provide the closing date of the most recent background investigation.

2e – Provide the date the investigation was favorably adjudicated.

2f – Provide the date the interim access or clearance was entered in CVS. Access is reported via the HSPD-12 tab in CVS.

2g – Select the type of account requested:

New: user has never had a PIPS/CVS account with OPM.
Modify: user has a current account but needs modification to current privileges. (Provide current User ID)
Reinstate: user has an account but time lapse in use has caused the account to expire. (Provide current User ID)

2h – Select the method through which the user will access the system:

Via NP2 Portal: Security Officials must ensure that the user has an active NP2 Portal account prior to submitting the request. (Contact your agency Portal Approver to arrange user's portal account)

U.S. Office of Personnel Management
Federal Investigative Services
Request for PIPS/CVS User ID/Access

Via Stand-Alone Terminal: This access requires additional information and special programming. Contact OPM-FIS ASL for more details.

2i – Select **only** the functions the user will need to perform direct job duties. Privileges are assigned on an as-needed basis.

Description of System Functions
Case Status: Authorized agency officials can obtain the overall status of a case. Detailed information about the case is located on the "Case Assignment Tracking Screen" (CATS), such as the status and result of each item in the case. Users can only view case information on those cases attributed to the Security Office Identifier (SOI) of the User ID.
Investigation Service Provider: Submit Investigation Data (formerly OFI-79): Investigative Service Providers (ISPs) use this function to report their investigations electronically to OPM's Security and Suitability Investigations Index (SII), as required by Executive Order 10450. ISPs can report the initiation, closing, and adjudication through the three-step process.
Request SAC: This function provides for direct request and initiation of Special Agreement Checks (SAC). A written agreement is required between the agency and OPM.
Print Documents: This function enables agency SOI's to print from their PIPS Terminal. Agencies can print: OPM Investigation Scheduled Notices, Advance Fingerprint Reports, Advance NAC Reports, and/or Case Closing Transmittals with results of investigations. Special programming and an agreement with OPM must be in place to request this function.
Download Documents: This function enables agency SOI's to download various OPM documents: OPM Investigation Scheduled Notices, Advance Fingerprint Reports, Advance NAC Reports, and/or Case Closing Transmittals with results of investigations. The download function transmits the information in a .txt file to the SOI. Special programming and an agreement with OPM must be in place to request this function.
Download Case Status Information: Agencies with automated tracking systems of their own, and who request a large volume of OPM cases, may arrange for OPM to transmit status information for download by the agency. Special programming and an agreement with OPM must be in place to request this function.
Enter Agency Adjudication: This function enables OPM customers to report the adjudicative action taken on an OPM investigation.

Description of System Functions
Search SII/CVS/JPAS: CVS contains information on security clearances, investigations, suitability and fitness determinations, Homeland Security Presidential Directive 12 (HSPD-12) Personal Identification Verification (PIV) credentials, and polygraph data. A search of CVS performs a simultaneous search of the SII, CVS, and the Joint Personnel Adjudication System (JPAS). JPAS is an independent information system operated by Department of Defense (DOD).
Add/Update Subject Data: In rare instances, an agency may have a need to add a Subject record to the system. Subjects should only be added to CVS to support the reporting of clearances, investigative data, HSPD-12 credentials, and polygraphs in accordance with reciprocity policies For updates to subject records, contact FISCTR Boyers Corrections Tech (NTC) in NP2 Messaging and include the reason for the change as well as the four subject identifiers (Name, SSN, Place of Birth, and Date of Birth).
Add/Update Clearance/Access Data: For agencies that submit clearance records to CVS, this function allows the user to add new clearance information and update existing clearances, in order to maintain currency in CVS.
Add/Update Polygraph Data: This function enables agencies to report full scope and counterintelligence polygraph data. Agencies can also modify their polygraph data contained in CVS.
Add/Update HSPD-12 Data: This function enables agencies to post and modify reciprocal HSPD-12 determinations in CVS.

If you have any questions on the functions in this section contact OPM-FIS ASL.

Section 3:

This section is to be completed by the Security Official. By completing this section, the Security Official certifies that the information on the form is accurate, the user is in a position which requires the requested access, and the user meets all the specified criteria for use of the system. This section must be complete and signed by the appropriate agency official or the request will be returned without action.

Clear Form

U.S. Office of Personnel Management
Federal Investigative Services
Request for PIPS/CVS User ID/Access

Send completed form to: OPM-FIS ASL via messaging in the NP2 portal
For questions: (724) 794-5612, ext. 4600 Option 4 (PIPS/CVS)

Section #1: To be completed by the user requesting account

[1a] Last Name:	**[1b] First Name:**	**[1c] Middle Name:**
[1d] Work Phone:	**[1e] SSN:**	**[1f] Select One:** ☐ **I am a U.S. Citizen** ☐ **I am not a U.S. Citizen**

Privacy Act Statement: Requesting this information is authorized by Section 301 of Title 5, U.S. Code, which permits an agency head to issue regulations on employee conduct and for the protection of agency records and property. Executive Order 9397 authorizes the use of your Social Security Number (SSN) as the means of identifying individuals in agency personnel records system. This information is used to control issuance of appropriate USERID's to authorize personnel and to maintain USERID control system accuracy. Furnishing this information is voluntary. However, failure to provide it may result in OPM not providing the USERID/Access needed to perform your official duties.

PII/Privacy Act/Data Integrity Statement:
I understand that this system contains sensitive information such as Personally Identifiable Information (PII), records about individuals requiring protection under the Privacy Act, sensitive financial information, and information that cannot be released under the Freedom of Information Act. I will protect all sensitive information received from OPM and will not introduce any unauthorized data onto OPM's system.

Computer Use/Password Disclosure Statement: I understand my USERID and password are for my exclusive use only. I agree to protect my password from disclosure by all reasonable means, and not to divulge it willingly or permit its use knowingly by another person. If I believe my password has been compromised or used by another person, I will immediately notify my supervisor and the Office of Personnel Management.
I will not attempt to access my own record in PIPS/CVS for any purpose, including testing/training situations.
I will not access the record of a coworker, associate or relative without the express approval of my supervisor. I understand that unauthorized access of investigative files or information is prohibited by law, and punishable by a fine of not more than $5,000 (5 U.S.C. 552a). I also understand that use of government computers for private or personal use is prohibited by law and may result in administrative action or criminal prosecution (18 U.S.C. 641; Executive Order 11222).

I have been afforded the opportunity to read the CVS User Manual to include the Security section regarding use of this system. I have read the above and understand the responsibilities inherent with being issued a PIPS/CVS UserID. Upon request, I may receive a copy of this signed statement.

[1g] Signature of User:	**[1h] Date:**

Section #2 To be completed by User's immediate supervisor

[2a] Agency & Division Name:

Office Location:

[2b] SOI: (provide only one)	**[2c] Level of last investigation:**	**[2d] Date investigation completed:**
		[2e] Date of favorable adjudication:
		[2f] Date interim access or clearance entered in CVS:

[2g] Type of Account (Select one)	☐ New user account ☐ Modify existing user account Current USER ID: ☐ Reinstate account Current USER ID:
[2h] Access Method (Select one or both and note requirements in instructions)	☐ Via NP2 Portal Account ☐ Via Virtual Private Network (VPN)

[2i] Function(s) Required

Agency Menu	*OPM use only*		*CVS Menu*
	Agency Menu	*CVS Menu*	
☐ Case Status [Conduct OPM Case Status Check for Pending Investigations]	[1]	[1a]	☐ Search SII/CVS/JPAS [non-Investigative Service Provider View]
☐ Investigative Service Providers: Submit Investigation Data (Formerly OFI-79)	[3]	[1b]	☐ Search SII/CVS/JPAS [Investigative Service Provider View]
☐ Request SAC [Special Agreement Checks require written agreement with OPM.]	[4]	[2]	☐ Add/Update Subject Data
☐ Print Documents [Refer to instructions]	[6a]	[3]	☐ Add/Update Clearance/Access Data
☐ Download Documents [Refer to instructions]	[6b]	[4]	☐ Add/Update Polygraph Data
☐ Download Case Status information [Refer to instructions]	[7]	[5]	☐ Add/Update HSPD-12 Data
☐ Enter Agency Adjudication	[8]		

Section #3: To be signed by the Security Official

I certify the above user requires the requested access to perform job duties on behalf of this agency. I also certify that the above user meets the minimum requirements for the requested system access and has been appropriately investigated, adjudicated, and trained to perform their assigned duties. The information provided on this form is accurate and complete and may be used by OPM in making the access determination for this user. As the Security Official, I understand that I am responsible for oversight of proper system use for SOI system users, and must notify OPM of system use infractions and changes in user access requirements.

[3a] Name of Security Official:	**[3b] Title:**	**[3c] Date:**

[3d] Signature of Security Official:	**[3e] Phone and Email of Agency Official:**