Defense Counterintelligence and Security Agency
Request for CVS User ID/Access

Federal agencies may request access to the Central Verification System (CVS) for personnel, as needed to perform specified assigned duties. In order to receive CVS access, individuals must be U.S. citizens. Individuals nominated for system use must also be investigated at a minimum level of Tier 2 or equivalent, favorably 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)
- 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 granted or credential issued by the appropriate adjudicating authority, and recorded in CVS

The Security Official for the Security Office Identifier (SOI) will ensure the policies and security procedures for use of this system are understood by nominated users prior to 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 review the CVS User Manual. Users must adhere to CVS security policies as a condition for system access.

Completed, signed forms can be sent via Messaging in the NP2 Portal as an attachment to CVS Help. Following review and successful account creation or modification, the user will receive account access information via Messaging in the NP2 Portal.

If you have questions about the completion of this form or PIPS/CVS access procedures, contact DCSA at: (878) 274-1171, option 2 then option 4.

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. The potential user must read, sign [1g], and date [1h]. If this section is incomplete or illegible, 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 the specific system privileges should be granted based on the user's duties.

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

2b – Provide DCSA assigned 4 character Security Office Identifier (SOI: usually begins with alpha character).

2c – Provide the level of the subject's most recent completed investigation (level must be a minimum of T2 or equivalent).

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

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

2f – If applicable, provide the date interim access or credential data was entered in CVS.

2g – Select the type of account requested:

New: user has never had a PIPS/CVS account.
Modify: user has a current account but needs modification to current privileges or the SOI. (Provide current User ID)
Reinstate: user has an account but time lapse in use has caused the account to expire. (Provide current User ID)
Delete: user no longer requires access to PIPS/CVS. (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)
Via Stand-Alone Terminal: This access requires additional information and special programming. Contact DCSACVSTeam@mail.mil or CVS Help in NP2 Messaging for more details.

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

Defense Counterintelligence and Security Agency
Request for CVS User ID/Access

Send completed form to: CVS Help via messaging in the NP2 portal
For questions: (878) 274-1171, Option 2 then Option 4 (PIPS/CVS)

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

[1a]Last Name:		[1d]Work Phone:	
[1b]First Name:		[1e]SSN:	
[1c]Middle Name:		◉ I am a U.S. Citizen	○ I am **NOT** a U.S. Citizen

Privacy Act Statement: I understand that 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 my Social Security Number (SSN) by DCSA as the means of identifying me in this personnel record system. This information is used to control issuance of appropriate USERID's to authorized personnel and for DCSA to system oversight. Furnishing this information is voluntary. However, failure to provide it may result in NBIB not providing the USERID/Access needed to perform my 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 DCSA and will not introduce any unauthorized data into DCSA'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 Defense Counterintelligence and Security Agency.

I will not attempt to access my own record in 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 information 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 CVS UserID. Upon request, I may receive a copy of this signed statement.

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

NOTE: The signatures must be in the same format. Both the user and Security Official must sign electronically or with a wet signature.

Request for CVS User ID/Access User's Name

Section #2 To be completed by User's supervisor or security officer

[2a] Agency & Division Name:

Office Location:

[2b] SOI (Only one SOI)

[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)

Current user ID:

[2h] Access Method (Select one or both and note requirements in instructions) ☐ Via NP2 Portal Account ☐ Via Virtual Private Network (VPN)

☐ **[1] Case Status:** This function provides the status of a case and detailed information located in 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 associated with the SOI of the User ID.

☐ **[3] Submit Investigation Data (formerly OFI-79):** Investigative Service Providers (ISPs) use this function to report their initiation, closing and adjudication of investigations, as required by title 5 CFR 1400

☐ **[4] Request SAC:** This function provides direct request and initiation of Special Agreement Checks (SAC). A written agreement is required between the agency and NBIB for some SAC's.

☐ **[6a/6b] Print/Download Documents:** This function is no longer available

☐ **[7] Download Case Status Information:** This function is no longer available

☐ **[8] Enter Agency Adjudication:** This function enables agencies to report the adjudicative actions taken on an NBIB investigation. Users may only enter adjudicative decisions for the same SOI as their User ID for CVS.

☐ **[1a/1b] Reciprocity:** Search CVS to view prior investigations, clearances, HSPD-12 Credentials (PIV/CAC Cards), or polygraphs.

☐ **[2] Add Subject Data:** This function is no longer available

☐ **[3] Add/Update Clearance/Access Data:** This function allows the user to add new clearance information and update existing clearances in order to maintain currency and support reciprocity.

☐ **[4] Add/Update Polygraph Data:** This function enables agencies to add or update full scope and counterintelligence polygraph data

☐ **[5] Add/Update HSPD-12 Data:** This function enables agencies to add and modify HSPD-12 card issuances and credential eligibility.

☐ **[6] View/Enroll Continuous Evaluation (CE):** This function enables agencies to enroll and manage their employees for CE. Your Agency must have an agreement in place with DCSA in order to have access to this capability.

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 DCSA in making the access determination for this user. As the Security Official, I understand that I am responsible for oversight of system use for my SOI and must notify DCSA of system use infractions and changes in user access requirements.

[3a] Name of Security Official:

[3b] Title:

[3c] Date:

[3d] Phone and Email of Security Official

[3e] Signature of Security Official:

NOTE: The signatures must be in the same format. Both the user and Security Official must sign electronically or with a wet signature.