



United States  
**Office of  
Personnel Management**

Federal Investigative Services Division  
Federal Investigations Processing Center  
Boyers, Pennsylvania 16018-0618

In Reply Refer To

Your Reference.

**Federal Investigations Notice**

---

Notice No. 06-03

Date: April 13, 2006

**SUBJECT: Implementation of Centralized Clearance Database**

**(This FIN Supersedes FIN 02-08)**

**Background**

In Federal Investigations Notice 02-08, dated June 17, 2002, the Office of Personnel Management (OPM) Federal Investigative Services Division (FISD) implemented the Clearance Verification System (CVS). Since that time, Federal agencies have been required to submit employee and contractor clearance information to FISD for inclusion in CVS.

On December 17, 2004, the President signed the Intelligence Reform and Terrorism Prevention Act of 2004 (Act). Section 3001(3)(e)(1) of the Act provides for the creation of an *"integrated, secure, database into which appropriate data relevant to the granting, denial or revocation of a security clearance or access pertaining to military, civilian, or government contractor personnel shall be entered from all authorized investigative and adjudicative agencies."*

The Act gave the OPM the responsibility of establishing and maintaining this database. Within OPM, FDIS is charged with managing the database.

On December 12, 2005, the Deputy Director for Management, Office of Management and Budget (OMB), issued guidance meant to enhance the "reciprocal recognition of existing personnel security clearances." The OMB guidance specifically tasked OPM to add data fields to the CVS to support this goal, and tasked agencies with updating those data fields by March 31, 2006.

On December 15, 2005, the enhanced version of CVS became operational and able to accept expanded agency clearance information in support of reciprocity. All existing agency clearance information was migrated to the enhanced CVS.

**Agency Responsibilities**

Agencies must submit their clearance data to the enhanced CVS in the new format (provided by Attachment I).

Agencies must conduct daily updates to their clearance information to reflect changes: new clearances, revocations, denials, suspensions, cancellations, and other clearance actions, in support of reciprocity.

Agencies must begin a cycle of complete data refreshes to occur at least monthly. Agencies should contact the FISD IT Access Branch at 724-794-5612 (x7232) to determine precise refresh schedules (1<sup>st</sup> of the month, every other Tuesday, etc.) in order to ensure that the system does not receive more information than it can process on any given day. *Clearances that are not refreshed at least monthly will expire automatically.*

Agencies, especially those with limited data load requirements, may input the daily/incremental changes and additions to individual records via the Personnel Investigations Processing System (PIPS) agency menu. However, most agencies will submit data in batch to CVS via the OPM Secure Portal, <https://opmis.xsp.org>. (Membership to the portal is by invitation only, and only authorized members are permitted to submit CVS data.)

While the technical aspects of these data loads have not changed with the advent of the enhanced CVS, we have added an additional feature to the CVS upload screen which requires the submitter to indicate if the submission is a daily/incremental file, or a refresh file. This new feature is shown in Attachment 2. *All adjudicative changes to existing clearance records (see Attachment 1, Record Type "E", position 85) such as denials, revocations, suspensions, cancellations, new clearances authorizations or revalidations, must be made using the daily/incremental load function.* "Refresh" loads intend only to refresh active valid clearances and will disregard any position 85 "change" entries.

### **Data Integrity**

Before a daily update or monthly refresh record can be successfully loaded, a Subject record must already exist in the PIPS, and the appropriate investigative record must already exist in the Suitability/Security Investigations Index (SII). If a Subject record does not exist in PIPS, or there are discrepancies between the personal identifiers in PIPS and in the agency record, the data load for that record will fail. Likewise, if there is no investigative record in SII, or if the investigation is inadequate to support the clearance record, the data load for that record will fail.

Agencies will receive error reports via the Portal within 24 hours of data submission which will alert them of any submitted clearance information that cannot be posted due to data discrepancies. It is incumbent upon agencies to resolve the data errors. If the error is in the data submitted by the agency, the submitter can simply make the correction in their data, and resubmit. If the error lies with information in PIPS, the agency must contact their OPM FISD point of contact for these matters to request the needed data change.

All investigations conducted by OPM are recorded in the SII. Other investigative service providers (ISP's) who have statutory or delegated investigative authority are required to notify OPM to make an SII record when they initiate an investigation. Notification is made either by submitting a form OFI-79 to OPM or by using function 3 of the PIPS Agency Menu. If the ISP fails to report the investigation, any attempts to load clearance data based upon it will fail. The agency attempting to load the clearance data must work with the ISP to have the investigative basis properly recorded in SII.

OPM does not own the clearance information posted by agencies to CVS. This information remains the property of the submitting agency and that agency alone is responsible for its accuracy.

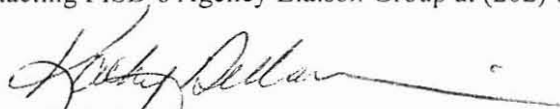
### **Verification of Clearances and Reciprocity**

Agency security personnel may verify the clearances of individuals whose information resides on CVS by accessing PIPS in whatever manner they are accustomed to. The PIPS Agency Menu, function 2 (SII/DCII/JPAS Search) provides access to clearance, investigation, subject and polygraph information. Security officers that do not have access to PIPS via the OPM Secure Portal should contact FISD's Agency Liaison Group at (202) 606-1042 to arrange for access.

Clearances granted by the Department of Defense (DoD) are not maintained in CVS, and will be verified by checking DoD's Joint Personnel Adjudication System (JPAS). A link exists between PIPS and JPAS which will allow the PIPS user direct access to JPAS. Function 2 of the PIPS Agency Menu includes a prompt labeled "Do you want to initiate a JPAS search?"

Where clearances cannot be verified via database checks, security personnel may communicate directly with the agency believed to have granted the clearance in question. At the request of OMB's Reciprocity Working Group, FISD has created and posted to the "public library" section of its secure portal a list of contact information for all agencies which grant security clearances. We have also created and posted a new comprehensive Interagency Clearance Verification Request form which should be used for manual clearance verification requests in place of other agency-specific forms.

Information related to the posting of information on CVS, the OPM portal, and other matters discussed in this FIN may be obtained by contacting FISD's Agency Liaison Group at (202) 606-1042.



Kathy L. Dillaman  
Associate Director  
Federal Investigative Services Division

---

**Inquiries:** OPM/FISD, Agency Liaison Group (202) 606-1042

**Code:** 732 National Security, 736 Investigations, Intelligence Reform and Terrorism Prevention Act of 2004

**Distribution:** SOIs

**Notice Expires:** When superseded by subsequent issuances

**Federal Investigations Notice 06-03, Attachment 1**

The following is the layout of the file to be provided by an agency when reporting clearance information to be posted to the enhanced CVS. (note: the format below is for batch-loading of clearance information; individual records may be updated by using the PIPS agency menu)

***Record Type ‘E’ – Clearance Eligibility***

<b>Position</b>	<b>Field Length</b>	<b>Mandatory</b>	<b>Description</b>
01 – 09	9	Yes	SSN of the Subject
10 – 13	4	Yes	SOI of the Granting Authority
14 – 14	1	Yes	Clearance Level Valid Values: C = Confidential L = L Q = Q S = Secret T = Top Secret
15 – 15	1	Yes	Record Type Valid values are: ‘E’ = Clearance/Eligibility Data ‘ ‘ = Assumes Clearance/Eligibility Data
16 – 23	8	Yes	Grant Date Format YYYYMMDD
24 – 43	20	Yes	Subject’s Last Name
44 – 51	8	Yes	Subject’s Date of Birth Format YYYYMMDD
52 – 53	2	Yes, if born in US or US Territory	Subject’s Place of Birth – State
54 – 73	20	Yes, if no Place of Birth State	Subject’s Place of Birth – Foreign Country
74 – 74	1	No	Exception Contains a ‘Y’ if any Conditions, Waivers, and Deviations exist.
75 – 75	1	No	Type Valid values are: F = Final I = Interim
76 – 81	6	No	Special Access. Valid values are: SCI = Sensitive Compartmented Information SAP = Special Access Programs SAPSCI = eligible for both ‘ ‘ = Not Reported

<b>Position</b>	<b>Field Length</b>	<b>Mandatory</b>	<b>Description</b>
82 – 82	1	No	Standard Code indicating standard used to determine eligibility. A = E.O. 12968 B = DCID ' ' = Not Reported
83 – 83	1	No	Contact Granting Authority Indicates if the Granting Authority reporting the Clearance wishes to be contacted by any Authority that is considering granting a Clearance or Perm Cert based on this Clearance record. Valid values are: Y= Yes Blank = No
84 – 84	1	No	Non-U.S. Immediate Family Member(s) Indicates the Subject with the Clearance has Non-U.S. Immediate Family Member(s). Valid values are: Y= Yes N= No Blank = Not Reported
85 – 85	1	Yes, if submitting incremental information in batch format	Status Updates: (Codes used to change the clearance eligibility status) C = Canceled (clearance administratively withdrawn, non-derogatory) D = Denied (clearance denied following adjudication) N = Notice of Clearance Eligibility (determination based on adjudication or reciprocity to establish a new clearance, or to re-establish a previous clearance following revocation, denial, cancellation or suspension) R = Revoked (clearance withdrawn for cause) S = Suspended (clearance temporarily withdrawn for cause) V= Revalidated (clearance administratively re-certified to be valid)  General Updates: (Code used to update non-clearance status information) U= Update (change to immediate family member information, special access, waivers, deviations, exceptions, etc.)

**Record Type 'P' – Polygraph Information**

<b>Position</b>	<b>Field Length</b>	<b>Required</b>	<b>Description</b>
01 – 09	9	Yes	SSN of the Subject
10 – 13	4	Yes	SOI of the Agency/Org reporting the Polygraph exam
14 – 14	1		Blank
15 – 15	1	Yes	Record Type Valid values are: 'P' = Polygraph Data
16 – 23	8	Yes	Date the Polygraph exam was administered. Format YYYYMMDD
24 – 27	4	Yes	SOI of the Agency that administered the Polygraph exam *
28 – 29	2	Yes	Polygraph Type CI = Counter Intelligence Scope FS = Full Scope
30 – 84	55		Blank
85 – 85	1	Yes	Action Code Indicates the type of action to be performed: N = New Polygraph data to be added U = Update existing Polygraph with data provided D = Delete Polygraph record

\* - If submitting agencies do not know the SOI of the administering agency, they should contact their liaison at that agency or OPM's Agency Liaison Group at (202) 606-1042.