



Privacy Impact Assessment  
for the

# **Fraud Detection and National Security Directorate**

**DHS/USCIS/PIA-013(a)**

**Appendix E**

**September 25, 2013**

**Contact Point**

**Donald K. Hawkins**

**Privacy Officer**

**United States Citizenship and Immigration Services**

**(202) 272-8030**

**Reviewing Official**

**Jonathan R. Cantor**

**Acting Chief Privacy Officer**

**Department of Homeland Security**

**(202) 343-1717**



## APPENDIX E

### **Southeast Region Immigration Services Officer Fraud Referral Intake Log (SER ADJ Fraud Referral Intake Log)**

#### **Summary:**

FDNS created the *SER ADJ Fraud Referral Intake Log* to capture and track all incoming fraud referrals from U.S. Citizenship and Immigration Services (USCIS) Immigration Services Officers (ISO).

Southeast Region (SER) ISOs document suspected fraud and forward the file to USCIS Fraud Detection and National Security Directorate (FDNS) after a supervisor approves a case for further inquiry. FDNS documents all incoming fraud referrals from ISOs in the *SER ADJ Fraud Referral Intake Log* spreadsheet and creates a record in FDNS Data System (FDNS-DS).<sup>1</sup>

FDNS reviews the referral for completeness and will either accept or decline the referral. If declined, the FDNS-DS record is “closed” and FDNS returns the Fraud Referral Sheet (FRS) to the referring ISO with an explanation of why FDNS declined the referral. If accepted, FDNS designates the case as accepted in FDNS-DS, conducts research and investigation, and refers prosecutable cases to Immigration Customs and Enforcement (ICE) officers.

Maintaining the *SER ADJ Fraud Referral Intake Log* allows FDNS to:

#### (1) Report Statistics

FDNS Immigration Officers (IO) use the information in the intake log to generate workflow production reports. Each FDNS office manually generates reports and each office captures these reports differently. The intake log allows FDNS offices to report the required numbers with consistency across the region.

#### (2) Conduct Training

FDNS IOs are responsible for training ISOs on how to refer actionable fraud cases and known fraud patterns and trends. The *SER ADJ Fraud Referral Intake Log* captures the reason FDNS declined a fraud referral, which assists FDNS to identify individual and group training needs.

#### (3) Complete the FDNS survey

SER FDNS requires all referrals returned to ISOs with findings must have a five question survey attached for ISOs to complete and return to FDNS. Capturing this data on the *SER ADJ Fraud Referral Intake Log* will assist FDNS to determine where the surveys were sent and if a response was received. It also allows FDNS to reach out to the ISO directly to request a completed copy of the survey.

#### (4) Meet ISO Period Performance Appraisals

Supervisory ISOs request the data from the *SER ADJ Fraud Referral Intake Log* for individual ISO fraud referral counts.

---

<sup>1</sup> For more information on FDNS-DS, see DHS/USCIS/PIA-013, Fraud Detection and National Security Data System (FDNS-DS), available at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).



## Data Elements:

This log maintains information related to the referral, and actions taken by FDNS and ISOs. Data may include:

### *Referral Information*

- Date of fraud referral
- ISO First Name
- ISO Last Name
- Receipt Number

### *FDNS Action*

- Date created in FDNS-DS
- FDNS-DS Number
- Whether the referral was accepted or declined
  - If declined, the reason it was declined
- FDNS findings

### *ISO Action*

- ISO decision on petition/application
- Date ISO issued a Notice to Appear (if applicable)

## Population:

Cases referred by ISOs to FDNS for fraud.

## Privacy Mitigation:

Only FDNS personnel with a need-to-know may access the *SER ADJ Fraud Referral Intake Log*. Further, FDNS maintains the intake log on the shared drive with restricted access, and user login and password controls are in place to monitor usage. In addition, USCIS FDNS provides training to all individuals who will be using the log to confirm proper handling of the information that is maintained. Finally, all USCIS employees are required to complete annual privacy training, which trains employees on the appropriate handling, use, and dissemination of personally identifiable information.