



Privacy Impact Assessment  
for the

# **Fraud Detection and National Security Directorate**

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

**Appendix D**

**September 24, 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 D

### Fraudulent Document Recognition Training

#### Summary:

The mission of U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security Directorate's (FDNS) is to determine whether individuals or organizations filing for immigration benefits pose a threat to national security, public safety, or the integrity of the nation's legal immigration system. FDNS supports USCIS's mission by enhancing USCIS's effectiveness and efficiency in detecting and removing known and suspected fraud from the application process, thus promoting the efficient processing of legitimate applications and petitions.

FDNS facilitates the *Fraudulent Document Recognition Training* to detect and deter fraud by recognizing fraudulent immigration documents as well as detecting impostors. This course trains USCIS personnel on how to identify types of counterfeit identification documents commonly used by terrorists, identification theft offenders, and illegal immigrants. Topics include how to identify immigration documents, specifically Permanent Resident Cards and Employment Authorization Documents (EAD), common document security features, photocopy examination of altered genuine documents, as well as a review on impostor detection.

The purpose of this *Fraudulent Document Recognition Training* course is to educate and enhance the FDNS employee's ability to identify and differentiate between genuine, counterfeit, and altered documents. The training allows FDNS personnel to determine what fraudulent documents look like and understand how fraudulent documents relate to immigration benefit fraud, issues of terrorism, and other national security issues. During the course of the training, the facilitator provides examples of both genuine and counterfeit documents to distinguish the difference between fraudulent documents and valid documents that have failing or worn features.

USCIS provides *Fraudulent Document Recognition Training* to USCIS personnel only; USCIS does not use a virtual training environment for this training. FDNS holds this training course in a classroom setting at a secured USCIS facility. The training consists of a PowerPoint presentation covering detection and examination of Permanent Resident Cards and EADs. Instructors share real immigration documentation obtained through fraud investigations or the administrative process to review security features of genuine, counterfeit, and altered documentation. However, there is no handout and students must return all training materials at the end of the training session. The PowerPoint is stored on the FDNS internal drive and the immigration documents are stored in a secured locked room. These training materials are restricted to those with a valid need-to-know.

FDNS will retain this presentation indefinitely and update it as appropriate to include new versions of cards and new fraud techniques employed by aliens to circumvent regulation.



## Data Elements:

The training presentation and immigration documents may contain real and fraudulent information about individuals. Personally identifiable information (PII) from the Permanent Resident Card, EAD card, and photocopied documents may include: the individual's name, address, Social Security Number, A-Number, date of birth, receipt filing number, photograph, country of birth, admission code, financial information, employment history, and education history.

## Population:

Individuals who submitted fraudulent and altered documents to USCIS.

## Privacy Mitigation:

FDNS provides *Fraudulent Document Recognition Training* to USCIS personnel with a need-to-know for training purposes. To prevent the risk of disclosing more information than necessary, FDNS minimizes the use of PII by removing unnecessary or irrelevant content from training materials that are not aligned with the objective of the training goals.

The electronic PowerPoint will be used as a part of this training. Access to the Fraudulent Document Recognition Training is restricted to employees with a valid need-to-know. The instructor will only use government-issued equipment to store and access this training. FDNS stores this presentation on an internal drive that is not accessible to users outside FDNS. FDNS will maintain security controls for any relevant materials.

FDNS stores the official physical records in a locked compartment and will not leave the records unattended. FDNS will store these records in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room where a guard and card reader controls access. FDNS collects all original, fraudulent, or photocopied document examples provided during training at the end of the training session and stores them securely.