

**EXHIBIT 60**  
**FILED UNDER SEAL**

**U.S. CITIZENSHIP AND IMMIGRATION SERVICES**

---



**U.S. Citizenship  
and Immigration  
Services**

***FDNS OFFICER  
BASIC TRAINING***

**NATIONAL SECURITY  
PARTICIPANT GUIDE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

---

**August 2008**

**SYLLABUS****COURSE TITLE:** National Security**COURSE NUMBER:** 701**COURSE DATE:****LENGTH AND METHOD OF PRESENTATION:**

Lecture	Lab	P.E.	Total	Program
6:30	0:00	1:00	7:30	FDNS BASIC

**This lesson is designated as For Official Use Only/Law Enforcement Sensitive (FOUO/LES) and the information contained within must be properly safeguarded. This lesson may NOT be distributed to the public.**

**DESCRIPTION:**

Discuss USCIS policies and procedures regarding the identification, vetting and adjudication of cases involving national security concerns. Provide an overview of the roles and responsibilities of the organizational components involved in processing cases involving national security concerns.

**TERMINAL PERFORMANCE OBJECTIVE (TPO):**

Given a field situation involving the adjudication of an application or petition, the USCIS Officer will understand the relevant USCIS components, policies, and processes associated with adjudicating cases with national security concerns. The USCIS Officer will be able to specify criteria for identifying a national security concern. The USCIS Officer will understand the steps required for deconfliction and vetting, internal and external.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**ENABLING PERFORMANCE OBJECTIVE (EPOs):**

- EPO #1:** Identify the relevant terms of reference relating to cases involving national security concerns.
- EPO #2:** Identify the organizational components responsible for reviewing the results of security checks, vetting and adjudicating cases identified with national security concerns.
- EPO #3:** Apply USCIS policies in adjudicating applications or petitions in cases involving national security concerns.
- EPO #4:** Discuss the term “national security concern” and methods used to identify cases involving national security concerns.
- EPO #5:** Identify the process for deconfliction when handling cases involving national security concerns.
- EPO #6:** Identify the process for internal vetting of cases involving national security concerns.
- EPO #7:** Identify the process for external vetting of cases involving national security concerns.
- EPO #8:** Identify the steps involved in adjudicating a case involving national security concerns.

**STUDENT SPECIAL REQUIREMENTS:**

**METHOD OF EVALUATION:**

Written Examination – Multiple Choice

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

---

## **TABLE OF CONTENTS**

- I. Introduction**
- II. Terms of Reference in National Security Cases**
- III. USCIS Organization and Functions in Processing National Security Cases**
- IV. A USCIS Policy for Vetting and Adjudicating Cases with National Security Concerns**
- IV. B Identification of National Security Concerns**
- IV. C Deconfliction**
- IV. D Eligibility Assessment with Internal Vetting**
- IV. E External Vetting**
- IV. F National Security Case Adjudication**
- V. Application**
- VI. References**
- VII. Policy Memoranda**
- VIII. Additional Electronic Resources**

### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**Presentation****References****I. INTRODUCTION**

USCIS leadership has identified national security protection as the agency's primary mission, and therefore these issues have become a central element in USCIS adjudications.

Prior to the terrorist attacks on September 11, 2001, the legacy Immigration and Naturalization Service (INS) conducted security checks on less than one-third of applicants and beneficiaries seeking immigration benefits.

Today, as part of the background check process, USCIS policy requires the completion of one or more security checks prior to granting immigration benefits.

The background check process allows USCIS to conduct a comprehensive review of the facts of the case to include any identified public safety or national security issues which may or may not result from the security check. The background check process is not considered complete until USCIS has resolved all identified concerns.

Although only a small percentage of the security checks results in adverse information of a national security, because of the large number of applications filed each year, a significant number result in national security hits requiring intensive review and resolution.

USCIS performs security checks regardless of race, ethnicity, national origin or religion.

USCIS Goal: ***"To deliver the right benefit to the right person at the right time, and no benefit to the wrong person."***

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**EPO #1: Identify the relevant terms of reference relating to cases involving national security concerns.**

*“Policy for Vetting and Adjudicating Cases with National Security Concerns” dated April 11, 2008, signed by Jonathan R. Scharfen, Deputy Director.*

**A. National Security (NS) Concern**

1. Exists when an individual or organization has been determined to have an articulable link to prior, current or planned involvement in, or association with, an activity, individual or organization described in 212(a)(3)(A), (B), or (F), 237(a)(4)(A) or (B) of the Immigration and Nationality Act (INA).
2. Includes but is not limited to terrorist activity; espionage; sabotage; and the illegal transfer of goods, technology or sensitive information.
3. Determination requires that the case be handled in accordance with Controlled Application Review and Resolution Program (CARRP) policy.

**B. Known or Suspected Terrorist (KST) hit**

1. A category of individuals who have been nominated and accepted for placement in the Terrorist Screening Database (TSDB); AND
2. Are on the Terrorist Watch List; AND
3. Have a specially coded lookout posted in the Treasury Enforcement Communications System (TECS)/Interagency Border Inspection System (IBIS) and/or the Consular Lookout Automated Support System (CLASS), as used by the Department of State.

**C. Non-Known or Suspected Terrorist (Non-KST) NS Concern**

1. A category of the remaining cases with NS concerns including but not limited to:
  - a. Associates of KST(s)

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- b. Unindicted co-conspirators
- c. Terrorist organization members
- d. Persons involved with providing material support to terrorists or terrorist organizations, and
- e. Agents of foreign governments

Individuals and organizations who fall into the Non-KST grouping may also pose a serious threat to national security.

#### D. Security Checks

1. FBI Name Check
2. FBI Fingerprint Check
3. Treasury Enforcement Communications System(TECS)/Interagency Border Inspection System (IBIS)
4. United States-Visitor and Immigrant Status Indicator Technology (US-VISIT)/Automated Biometrics Identification System (IDENT).

On April 25, 2006, the USCIS Press Office released a fact sheet for the public entitled, "Immigration Security Checks---How and Why the Process Works". The fact sheet can be accessed at [www.uscis.gov](http://www.uscis.gov)

Specific checks or combination of checks required for each application or petition type, pursuant to each component's procedures.

#### E. Internal Vetting

May consist of DHS, open source, or other systems checks; file review; interviews; and other research.

#### F. External Vetting

Consists of inquiries to record owners in possession of the national security information to identify:

(a) fact or fact patterns necessary to determine the nature and relevance of the NS concern, including status and results of any ongoing investigation and the basis for closure of any previous investigation; and

(b) information that may be relevant in determining eligibility, and when appropriate, removability.

#### FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



## **G. Deconfliction**

A term used to describe coordination between USCIS and another governmental agency owner of national security information (the record owner) to ensure that planned adjudicative activities (e.g., interview, request for evidence, site visit, decision to grant or deny a benefit, and the timing of the decision) do not compromise or impede an ongoing investigation or other record owner interest.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**EPO #2: Identify the organizational components responsible for vetting and adjudicating cases identified with national security concerns.**

Processing cases identified as having national security concerns may require extensive coordination between organizational components within USCIS as well as with law enforcement and intelligence agencies outside of USCIS. This coordination is a shared responsibility between the Field and Headquarters.

**A. Office of Fraud Detection and National Security Division (FDNS)**

The office within USCIS established to enhance the integrity of the legal immigration system by identifying threats to national security and public safety, detecting and combating benefit fraud and removing systemic and other vulnerabilities. FDNS falls under the National Security and Records Verification (NSRV) Directorate. FDNS Headquarters is composed of four separate branches: National Security, Intelligence, Fraud, and Mission Support.

1. National Security Branch (NSB) at Headquarters FDNS
  - a. Field Support Unit (FSU)
    - i. Triage requests for assistance from the field
    - ii. Develops and provides training to the field and HQFDNS
  - b. Background Check Analysis Unit (BCAU)
    - i. Externally vets KST NS concerns
    - ii. Provides advice and technical assistance to the field
    - iii. Detailed to other agencies and DHS components
      - A. Terrorist Screening Center (TSC)
      - B. National Joint Terrorism Task Force (NJTTF)
      - C. FBI's National Name Check Program (NNCP)
      - D. Immigration and Customs Enforcement (ICE)

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- c. Adjudication Support Unit (ASU)
    - i. Formerly known as National Security Advisory Unit (NSAU)
    - ii. Develops and coordinates case resolution strategies relating to national security cases.
    - iii. Coordinates with Intelligence and Law Enforcement Agencies to declassify or use classified information when required
  - d. Policy Support Unit (PSU)
    - i. Formerly known as National Security Policy and Strategy Unit (NSPS)
    - ii. Provides policy analysis and guidance for the National Security Branch to help shape operations, procedures, and strategies.
2. FDNS Immigration Officers in the Field
- a. Located at each field office, asylum office and service center.
  - b. Review, research, and analyze information relating to applications/petitions when there are national security, public safety, or fraud concerns.
  - c. Do not adjudicate
  - d. Document work in FDNS-Data System (FDNS-DS) a national database used by FDNS to monitor and track referrals and cases involving national security concerns, suspected and confirmed fraud, and egregious public safety concerns.
  - e. Primary conduit for law enforcement coordination such as ICE, FBI, and members of the local JTTF to support the USCIS mission of ensuring the integrity of the immigration

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

system and removing those who pose a threat to the U.S.

## **B. Office of Domestic Operations**

Composed of the Office of Field Operations and Service Center Operations.

Office of Field Operations provides policy and operational direction to field offices and the National Benefits Center as well as manages assignments and monitors the resolution of cases involving national security concerns.

Service Center Operations provides policy and operational direction to service centers (Vermont, Nebraska, Texas, and California) and manages assignments and monitors the resolution of cases involving national security cases.

- a. Service Centers
  - i. Have established procedures to review all IBIS, FBI fingerprint & FBI name check results when the initial response is received; this includes the immediate review of Rap sheets.
  - ii. All national security concerns and concerns are referred to local Background Check Units (BCU)
  - iii. FDNS Immigration Officers do not handle the national security cases.
- b. Field Offices
  - i. Have established procedures to ensure all IBIS, FBI Fingerprint & FBI Name Check results have been received, reviewed, and are current prior to the granting of an immigration benefit.
  - ii. Each Field Office has an established referral process to the local FDNS Immigration Officer for cases identified as having national security concerns.

## **C. Office of Refugee, Asylum, and International Operations (RAIO)**

The headquarter components of RAIO provides policy and operational direction to asylum offices, the Refugee Corps and USCIS offices overseas. The headquarter components of RAIO manage assignments and monitors the resolution of cases having national security concerns.

### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**EPO #3: Apply USCIS policies in adjudicating applications or petitions in cases involving national security concerns.**

**A. Controlled Application Review and Resolution Program (CARRP) Overview**

1. Provides agency-wide national security policy
2. Decentralizes the authority to vet and adjudicate cases with national security concerns – from HQFDNS to field offices
3. Establishes the Fraud Detection and National Security Data System (FDNS-DS) as the primary system for documenting activities (vetting, deconfliction, resolution activities) of national security cases
4. Distinguishes between two types of national security concerns
  - a. Known or Suspected Terrorist (KST)
  - b. Non-KST
5. Applies to all applications and petitions that convey immigrant or non-immigrant status
6. Rescinded specific previous USCIS national security policy memoranda
7. Effective upon the issuance of operational guidance from the Directorate of Domestic Operations and each component within the Directorate of Refugee, Asylum, and International Operations (RAIO)
8. Policy memorandum and Operational Guidance is For Official Use Only (FOUO)
9. Establishes a standard CARRP workflow consisting of four stages in order to identify, record, and complete applications/petitions with a national security concern
10. Completed by Designated Officers as outlined in each component's individual guidance

*“Policy for Vetting and Adjudicating Cases with National Security Concerns”* dated April 11, 2008, signed by Jonathan R. Scharfen, Deputy Director.

Domestic Operations:  
See *“Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns”* dated April 24, 2008, signed by Don Neufeld.

International Operations: See page 8 *“Guidance for International Operations Division on the Vetting, Deconfliction, and Adjudication of Cases with National Security Concerns”* dated April 28, 2008, signed by Alanna Ow.

Asylum Division:  
See *“Issuance of Revised Section of the Identity and Security Checks Procedures Manual Regarding Vetting and Adjudicating Cases with National Security Concerns”*, dated May 14, 2008, signed by Joseph Langlois

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

11. Policy and Operational Guidance introduces a reference tool, “Guidance for Identifying National Security Concerns”

- a. Introduced Background Check and Adjudicative Assessment (BCAA) form which replaced the National Security Record (NSR)- Use suspended in July 2008.

Refugee Affairs  
Division: See  
“Operational Guidance  
for Vetting and  
Adjudicating Refugee  
Cases with National  
Security Concerns”  
dated May 14, 2008,  
signed by Barbara  
Strack.

Suspension of BCAA -  
Refer to USCIS  
Memorandum, dated  
July 18, 2008, from  
Michael Aytes, Acting  
Deputy Director,  
entitled, “Interim  
procedures for  
Documenting and  
Tracking New,  
Pending and Inventory  
Cases with National  
Security Concerns.”

## B. Four Stages in the CARRP Workflow

### 1. Identifying National Security Concerns

- a. Generally results from security check but may be identified from other source at any time during the adjudication process
- b. Confirm match
- i. KSTs via Terrorist Screening Center (TSC)
  - ii. Non-KSTs
- c. Document articulable concern
- i. Designated Worksheet(s)
  - ii. FDNS-DS
- d. Consider effect of NS indicators relating to family members and close associates on the individual

See “Guidance for  
Identifying National  
Security Concerns”  
attached to each  
individual component’s  
guidance.

In some instances, the petitioner, beneficiary, applicant, dependant or derivative may be a family member or close

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

associate of a subject who has an identified NS concern. Such information may impact the individual's eligibility for the benefit sought and/or may indicate a NS concern for the individual. In these cases, the officer must determine if the NS concern relates to the individual, and if so, if it gives rise to a NS concern for the individual. A close associate includes but is not limited to a roommate, co-worker, employee, owner, partner, affiliate, or friend.

## 2. Eligibility Assessment/Internal Vetting

- a. Thorough review of application/petition/file
- b. Security checks
- c. Basic systems checks (USCIS/DHS)
- d. Supplemental systems checks (USCIS/DHS/Open Source/Other), as required
- e. Depending on operational guidance, additional actions may take place such as Request for Evidence (RFE), interview, site visit. \*\*\*Deconfliction required prior to USCIS action.
- f. For KSTs and Non-KST NS concerns, the Field conducts internal vetting and the eligibility assessment.

## 3. External Vetting

Outreach to record owner of national security information:

- a. To obtain information that may be relevant in determining eligibility
- b. To obtain information regarding the nature and extent of the national security concern
- c. For KST, HQFDNS maintains sole authority for KST external vetting

### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



- d. For Non-KST NS concerns, the Field conducts external vetting
4. Adjudication of National Security Cases (CARRP Adjudication)
- Evaluation of results of internal and external vetting to make eligibility determination.
- a. For KSTs, seek HQFDNS assistance
- b. For Non-KST NS concerns, Senior-level official has authority to approve or discretion to seek HQFDNS assistance. See operational guidance for definition senior-level official.
5. At any stage of the process, any of the following actions may occur:
- a. Deconfliction
- b. Request for Assistance to HQFDNS
- c. Determination that the case is not national security and is released for routine adjudication
- d. A KST becomes a non-KST NS Concern or non-national security
- e. A non-KST becomes a KST

Flexibility and communication is required to handle the variety and complexity of the caseload.

### **C. Exceptions to CARRP Policy: Petitions that Do Not Convey Status**

1. Petitions that do not convey immigrant or non-immigrant status are not vetted and adjudicated under CARRP. Adjudication of these petitions establishes eligibility for the visa category not admissibility.
2. Regardless, certain steps are required if a national security concern should arise:
- a. National security concern must be documented. (Designated Worksheet(s)/FDNS-DS)

Domestic Operations:  
See p. 40 “Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns” dated April 24, 2008, signed by Don Neufeld.

International Operations: See page 8 “Guidance for

#### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

b. Thorough review for ineligibility and fraud concern

c. Deconfliction

d.

**LE**

International Operations Division on the Vetting, Deconfliction, and Adjudication of Cases with National Security Concerns” dated April 28, 2008, signed by Alanna Ow.

**D. CARRP Policy and Exemptions for the INA Section 212(a)(3)(B) Terrorism-Related Provisions and NS Concerns**

1. If an exemption is granted under INA § 212(d)(3)(B)(i) of the Act, AND no other NS concern is identified, no further vetting is required and the application/petition may continue through routine adjudication.
2. If an exemption is available but will not be granted under INA § 212(d)(3)(B)(i), the individual is inadmissible or otherwise barred from receiving an immigration benefit and the application must be denied.
  - a. Must be documented in FDNS-DS per established procedures. An IBIS record must be created.
3. p. 35 of Domestic Ops Guidance: If an exemption is available and will be granted under INA § 212(d)(3)(B), AND no other NS concern is identified, the application/petition with a NS concern will be released for routine adjudication as a NNS concern.
  - a. No FDNS-DS is required.

For determinations on material support and other terrorist-related exemption determinations, see the following memoranda:

dated July 28, 2008 from Acting Deputy Director Michael L. Aytes, entitled, “Implementation of Section 691 of Division J of the Consolidated Appropriations Act, 2008, and Updated Processing Requirements for Discretionary Exemption to Terrorist Activity Inadmissibility Grounds”

dated March 26, 2008, from Deputy Director Jonathan Scharfen, entitled “Withholding Adjudication and Review of Prior Denials of Certain Categories of Cases Involving Association with, or Provision of Material Support to, Certain Terrorist Organizations or Other Groups”

AND

Dated May 24, 2007

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

---

**Participant Guide**

from Deputy Director Jonathan Scharfen, entitled "Processing the Discretionary Exemption to the Inadmissibility Ground for Providing Material Support to Certain Terrorist Organizations"

See respective operational guidance for specific handling steps for material support cases. Domestic Operations: See p. 30- 34 and p 44 "Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns" dated April 24, 2008, signed by Don Neufeld.

**E. Special Considerations**

1. Specific guidance on these applications and cases may be found in the respective operational guidance.
  - a. Application for Employment Authorization (Forms I-765)
  - b. Application for Travel Authorizations (Form I-131)
  - c. (Forms I-765 and I-131)
  - d. Application for Replacement Permanent Resident Card (Form I-90)
  - e. Santillan Cases
  - f. Appeals/Motions to Reconsider or Reopen
  - g. Application for Naturalization

**ALWAYS DECONFLICT PRIOR TO USCIS ACTION!!!!**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**EPO #4: Identifying National Security Concerns****A. National Security (NS) Concern**

Exists when an individual or organization has been determined to have an articulable link to prior, current or planned involvement in, or association with, an activity, individual or organization described in 212(a)(3)(A), (B), or (F), 237(a)(4)(A) or (B) of the INA.

1. Articulable Link
  - a. Exists when two things are connected in a way that can be explained
  - b. Defined as capable of being expressed, explained or justified
  - c. Connection is between NS activity as described in INA § 212(a)(3)(A), (B), or (F), or INA §237(a)(4)(A) or (B), and the individual
  - d. Must consider totality of the circumstances
  - e. Does the information allow a reasonable inference to be drawn as to the connection
  - f. Connection need not rise to the level required for the issuance of an NTA (clear and convincing) but there must be some connection
2. Two Types of NS Concerns
  - a. Known or Suspected Terrorist (KST)
  - b. Non-KST

**B. Known or Suspected Terrorist (KST) NS Concern**

1. Homeland Security Presidential Directive-6 (HSPD-6)
  - a. Signed into effect on September 6, 2003.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

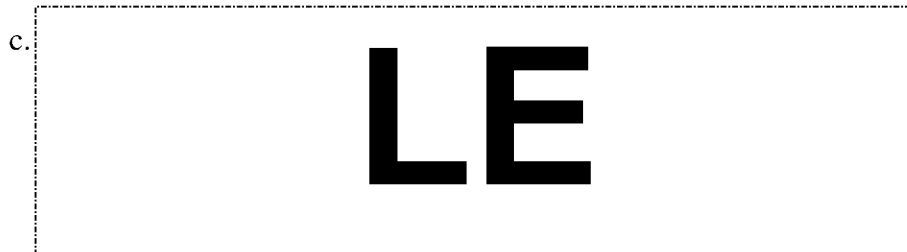
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- b. To further integrate and widen the use of terrorist screening information.
- c. Established the Terrorist Screening Center (TSC) to consolidate U.S. Government terrorist screening information.
- d. Directs federal agencies to provide appropriate terrorist information to the National Counterterrorism Center (NCTC), which in turn provides the TSC access to all appropriate terrorist information or intelligence.

2. Terrorist Identities Datamart Environment (TIDE)

[http://www.nctc.gov/docs/Tide\\_Fact\\_Sheet.pdf](http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf)

- a. U.S. Government's central repository of information on international terrorist identities.
- b. Supports the U.S. Government's various terrorist screening systems or "watch list" and the U.S. Intelligence Community's overall counterterrorism mission.



- d. Information from TIDE is imported into the Terrorist Screening Database (TSDB), an unclassified but restricted database that houses the Terrorist Watch List.
- e. Individuals on this list are considered to be Known or (appropriately) Suspected Terrorists (KST).

3. Terrorist Screening Center (TSC)

- a. Operational and running 24/7 since December 2003.



**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**LE**

c. The TSC, TSOU or case agent may or may not contact USCIS in response.

d. **LE**

**LE** This information may assist in establishing whether there is a definitive match and it may assist the originating agency in their review of the case. USCIS Officers may comply with this request; however, USCIS Officers must NOT forward asylum applications to the TSC.

e. The TSC should not be contacted unless there is a KST hit: **LE** hit directing contact with the TSC. Do NOT request to speak with Richard Kopel, Deputy Director at the TSC.

4. Known or Suspected Terrorist (KST) Hit

a. TECS/IBIS

i. **LE**  
ii. **LE**  
iii. **LE**

b. National Crime Information Center (NCIC)

i. Identified by **LE**

ii. **LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

iii.



## c. Consular Lookout Automated Support System (CLASS)

- i. CLASS may indicate that the subject is on the Terrorist Watch List. Information from CLASS is used by State Department Officials as well as USCIS Officers overseas.

**C. Non-KST National Security Concern**

Non-KST NS Concerns may be identified as the result of security checks but also through other means such as:

- CLASS
- Department of State Security Advisory Opinions (SAOs)
- DHS system checks
- Testimony elicited during an interview;
- Review of the petition or application, supporting documents, the A-file, or related files;
- Leads from other U.S. Government agencies or foreign governments;
- Other sources, including open source research.

See “Guidance for Identifying National Security Concerns” an appendix or attachment to the respective CARRP Operational Guidance

## 1. Statutory Indicators

Sections found in the Immigration and Nationality Act (INA)

- a. Security related inadmissibility grounds  
212(a)(3)(A)

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

## i. Espionage

A. Foreign Intelligence: Information relating to capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence, except for information on international terrorist activities.

B. Counterintelligence: Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Definitions for Foreign Intelligence and Counterintelligence found at:

Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms

## ii. Sabotage

iii. Violation or evasion of any law prohibiting the export from the United States of goods, technology, or sensitive information

<http://www.dtic.mil/doctrine/jel/doddict/>

b. Terrorist related inadmissibility grounds  
212(a)(3)(B) and (F)

## i. Terrorist Activity Defined

INA 212(a)(3)(B)(iii)

Any activity which is unlawful under the laws of the place where it is committed (or which, if it had been committed in the United States, would be unlawful under the laws of the United States or any State) AND which involves any of the following:

A. The hijacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle).

B. The seizing or detaining, an threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



implicit condition for the release of the individual seized or detained.

C. A violent attack upon an internationally protected person or upon the liberty of such a person.

Internationally protected person as defined in section 1116(b)(4) of title 18, United States Code

D. An assassination.

E. The use of any-

F. biological agent, chemical agent, or nuclear weapon or device, or

G. explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property.

H. A threat, attempt, or conspiracy to do any of the foregoing.

ii. Engage in Terrorist Activity Defined

INA 212(a)(3)(B)(iv)

In an individual capacity or as a member of an organization-

A. To commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity;

B. To prepare or plan a terrorist activity;

C. To gather information on potential targets for terrorist activity;

D. To solicit funds or other things of value for a terrorist activity; a Tier I or II terrorist

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

organization; or a Tier III organization unless the solicitor can demonstrate by clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization;

- E. to solicit any individual--to engage in conduct otherwise described in this subsection; for membership in a designated terrorist organization (Tier I or Tier II); for membership in an undesignated terrorist organization (Tier III) unless the solicitor can demonstrate by clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization;
- F. to commit an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training--for the commission of a terrorist activity;
1. to any individual who the actor knows, or reasonably should know, has committed or plans to commit a terrorist activity;
  2. to a designated terrorist organization (Tier I or Tier II) described or to any member of such an organization; or
  3. to an undesignated terrorist organization (Tier III), or to any member of such an organization, unless the actor can demonstrate by clear and convincing evidence that the actor did

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

not know, and should not reasonably have known, that the organization was a terrorist organization.

- iii. Inadmissibility for Terrorist Activity INA 212(a)(3)(B)

In general, any alien is inadmissible who-

- A. has engaged in a terrorist activity,
- B. a consular officer, the Attorney General, or the Secretary of Homeland Security knows, or has reasonable ground to believe, is engaged in or is likely to engage after entry in any terrorist activity (as defined in clause (iv));
- C. has, under circumstances indicating an intention to cause death or serious bodily harm, incited terrorist activity;
- D. is a representative of—
  - 1. a terrorist organization; or
  - 2. a political, social, or other group that endorses or espouses terrorist activity;
- E. is a member of a designated terrorist organization (Tier I or II)
- F. is a member of an undesignated terrorist organization (Tier III) unless the alien can demonstrate by clear and convincing evidence that the alien did not know, and should not reasonably have known, that the organization was a terrorist organization;
- G. endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization;

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

H. has received military-type training from or on behalf of any organization that, at the time the training was received, was a terrorist organization (as defined in clause (vi)); or

Military-type training defined in section 2339D(c)(1) of title 18, United States Code

I. is the spouse or child of an alien who is inadmissible under this subparagraph, if the activity causing the alien to be found inadmissible occurred within the last 5 years

J. EXCEPTION- does not apply to a spouse or child--who did not know or should not reasonably have known of the activity causing the alien to be found inadmissible under this section; or whom the consular officer or Attorney General has reasonable grounds to believe has renounced the activity causing the alien to be found inadmissible under this section.

iv. Terrorist Organization Defined

A. Tier I – Foreign Terrorist Organization (FTO)

1. An organization designated under section 219 of the INA by the Secretary of State a finding that the organization engages in terrorist activities or terrorism.
2. These organizations threaten U.S. nationals or the national security of the U.S.
3. Over 40 different organizations are currently designated and include such organizations as HAMAS, Al Qaeda, Hizballah, and Revolutionary Armed Forces of Colombia (FARC).

INA 212(a)(3)(B)(vi)

<http://www.state.gov/>

B. Tier II – Terrorist Exclusion List (TEL)

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

<http://www.state.gov/>

1. An organization otherwise designated, upon publication in the Federal Register, by the Secretary of State in consultation with or upon the request of the Attorney General or the Secretary of Homeland Security, as a terrorist organization, after finding that the organization engages in terrorist activities as defined in the Act.
2. There is no requirement that these organizations threaten U.S. nationals or the national security of the U.S.

See the Department of Treasury listing of Specially Designated Global Terrorist Entities pursuant to Executive Order 13224. The Department of the Treasury Office of Foreign Assets Control (OFAC) maintains on its website a list of individuals and groups designated under this executive order. The list can be found on the OFAC's website at <http://www.treas.gov/offices/enforcement/ofac/>

#### C. Tier III – Undesignated Terrorist Organization

1. An organization that is a group of two or more individuals, whether organized or not, which engages in, or has a subgroup which engages in, terrorist activities
2. There is no official list for Tier III organizations.

Some organizations listed likely meet the Tier III undesignated terrorist organization definition.

- c. Security related deportability grounds  
237(a)(4)(A) and (B)
- d. Exceptions to Asylum Eligibility  
208(b)(2)(A)
- e. Inadmissible Aliens – Money Laundering  
212(a)(2)(I)
- f. Issuance of visas – Revocation of visas or other documents  
221(i)
- g. Removal of aliens inadmissible on security and related grounds  
235(c)

#### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- h. Mandatory detention of suspected terrorists; habeas corpus; judicial review  
236A
  - i. Deportable Aliens – Miscellaneous crimes  
237(a)(2)(D)
2. Non-Statutory Indicators

Officers must be alert for indicators of NS concerns and realize that activities or involvement does not need to satisfy the legal standard for admissibility or removability in determining the existence of NS concern. However, Officers must understand that the presence of an indicator does not necessarily mean a NS concern exists. Officers must consider the totality of circumstances in the determination process to include but not limited to: results of all required security checks; evidence in file; testimony of individual; credibility.

- a. Employment, Training, or Government Affiliations

**LE**

A. State Sponsors of Terrorism

**LE**

More detailed information can be found at “Overview of State Sponsored Terrorism” in [Country Reports on Terrorism](#) at [www.state.gov](http://www.state.gov)

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

Act, and Export Administration Act.

<u>Country</u>	<u>Designation Date</u>
Cuba	March 1, 1982
Iran	January 19, 1984
North Korea	January 20, 1988
Sudan	August 12, 1993
Syria	December 29, 1979

iii.

LE

b. Suspicious Activities

Certain types of activities may require additional scrutiny if identified during the adjudicative process to determine whether there is a link to a national security concern. This includes but is not limited to:

i.

LE

ii.

iii.

iv.

LE

v.

vi.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

vii.

viii.

ix.

x.

**LE**

c. Suspicious Financial Activities

**LE**

i.

ii.

iii.

iv.

v.

vi.

vii.

viii.

**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



ix.

**LE**

x.

xi.

**d. Hawala**

- i. Alternative remittance system originally from India and South Asia. Hawala
- ii. Means “trust”, “reference”, or “exchange”
- iii. Commonly-used but informal method of transferring money quickly, domestically or internationally.
- iv. Requires hawala dealers (also known as *hawaladars*) on the front-end to communicate with hawala dealers on the back-end in order to advise of the requirement to transfer funds.
- v. Transactions allow for easy conversion of currency, leave no paper trail, and do not involve physical movement of currency.
- vi. Example: An individual needs to send money to his family overseas. He provides the cash to a local hawala dealer. The hawala dealer contacts a hawala dealer overseas, who using his own money, arranges to get the money in local currency to the family. The overseas dealer carries debt until he needs to send money back to the original hawala dealer or until other arrangements can be made to balance accounts.
- vii. In the U.S., hawala dealers are considered to be

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

operating a money service business.

viii. With the passage of the USA PATRIOT Act, failure to register a money service business is considered a felony violation. In short, hawala dealers in the U.S. must be registered as a money service business.

e. **LE**

**LE**

3. Security Check Indicators

a. FBI Name Check

i. Background

The National Name Check Program (NNCP) within the FBI conducts manual and electronic searches of the FBI's Central Records System (CRS) which encompasses the centralized records of FBI Headquarters, field offices, and Legal Attaché offices. The CRS contains all FBI investigative, administrative, personnel, and general files.

<http://www.fbi.gov/hq/nationalnamecheck.htm>

**LE**

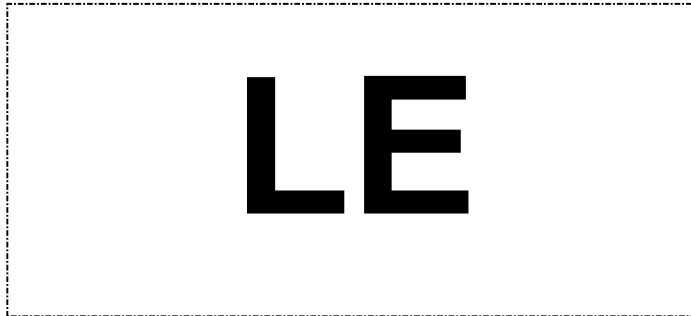
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

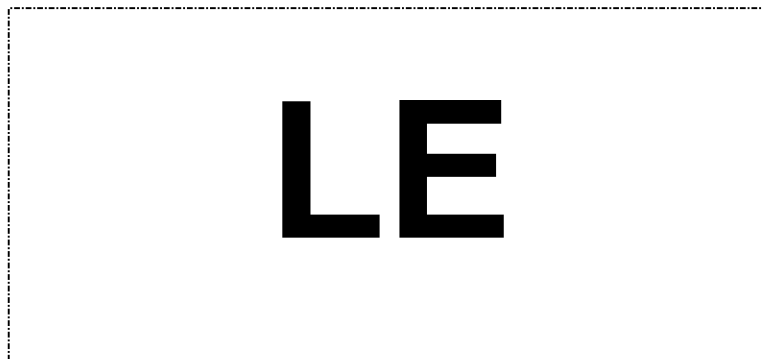
ii. Responses

A. No Record

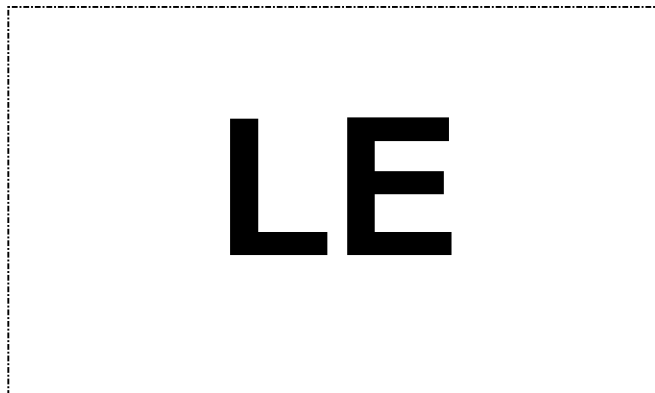
B. Positive Response



C. Unknown Response



D. Pending Response



*“Revised National Security Adjudication and Reporting Requirements”, as of February 4, 2008, signed by Michael Aytes, Associate Director, Domestic Operations.*

*“FBI Name Check Process and Clarification for Domestic Operations”, dated December 21, 2006 signed by Michael Aytes, Associate Director,*

iii. Validity

A.



**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

B.

**LE**

Domestic Operations.

iv. Indicators

**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

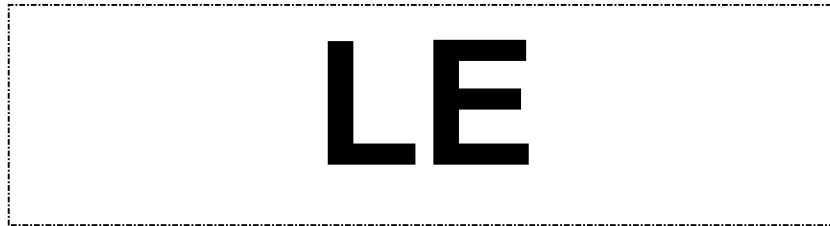
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

b. FBI Fingerprint Check

i. Background

The FBI Fingerprint Check is separate and distinct from the FBI Name Check. It provides information relating to the applicant's criminal history within the U.S. based on biometrics.

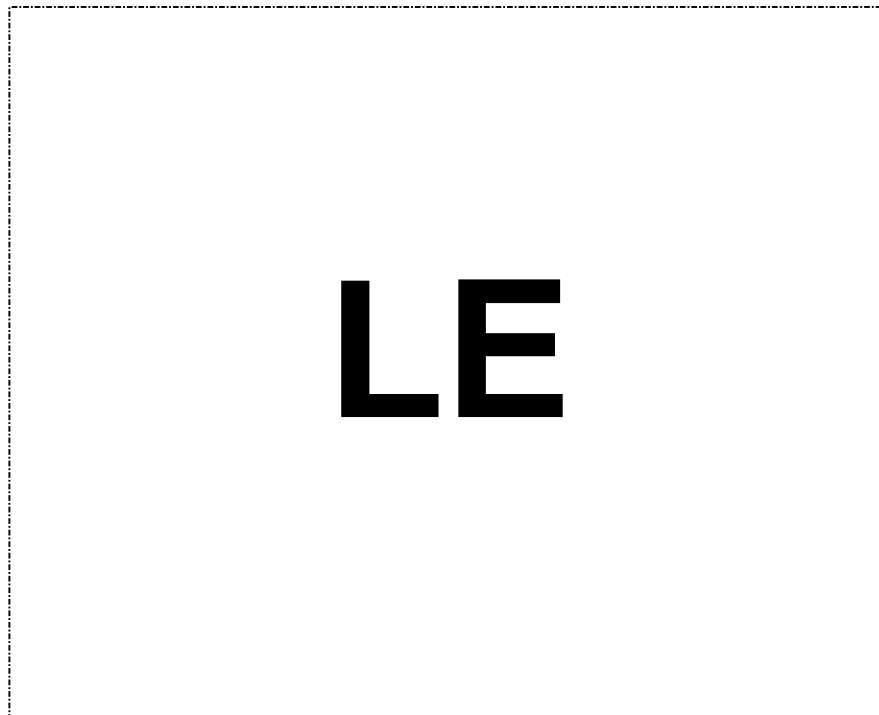
ii. Responses



iii. Validity

Must be less than 15 months old at the time of adjudication

iv. Indicators



**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**LE**

c. TECS/IBIS

i. Background

USCIS conducts 33-35 million IBIS checks per year & receives approximately 10,000 hits of a national security nature. Approximately 1,500 are KSTs.

ii. Responses

A.

B.

iii.

iv.

A.

**LE**

B.

C.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

D.

LE

1.

2.

LE

E.

LE

1.

2.

3.

4.

LE

d. US-VISIT/IDENT

i. Background

Various government agencies, including DHS Components (USCIS, CBP, and ICE), DOS, the FBI, and the National

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

Ground Intelligence Center (NGIC), load biographical and biometric information into US-VISIT/IDENT.

ii. Indicators

US-VISIT/IDENT Watch list includes, but is not limited to, biographic and/or biometric information for KSTs;

LE

LE

and individuals inadmissible or removable under sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Act.

#### D. Initiating a Referral

Consult with local management for procedures on forwarding a national security concern to the designated officer. Generally the following officers are designated to conduct vetting and deconfliction activities.

1. Asylum Office – NS concern is forwarded to the FDNS Immigration Officer.
2. Field Office – NS concern is forwarded to the FDNS Immigration Officer.
3. Service Center - NS concern is forwarded to the Background Check Unit (BCU).
4. Overseas Office – see supervisor
5. Refugee Corps –see supervisor

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



**EPO #5: Introduce the process of deconfliction when handling cases involving national security concerns.****A. Deconfliction**

1. Coordination between USCIS and another governmental agency owner of national security information (the record owner) to ensure that planned adjudicative activities (e.g., interview, request for evidence, site visit, decision to grant or deny a benefit, and the timing of the decision) do not compromise or impede an ongoing investigation or other record owner interest.
2. May happen at any stage of adjudication process
3. May happen multiple times during the adjudication of a single application
4. Completed by designated officer
  - a. Primarily FDNS Immigration Officer in the field and asylum offices
  - b. Primarily BCU staff at Service Center
  - c. Consider including designated adjudications officer on discussions with record owner
5. Ensures that record owner is aware that the individual has a benefit pending with USCIS
6. Provides USCIS with opportunity to ask about



**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**LE**

7. Provides record owner with opportunity to submit questions, to consider additional information that may inform further action or investigation of the case, and to comment on decision
  - a. Preparing for RFE, Interview or Site Visit
  - b. Following receipt of additional information/evidence
  - c. Preparing for Decision
  - d. Must be material to benefit sought

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**EPO #6: Identify the process for internal vetting of cases involving national security concerns.**

**A. Eligibility Assessment**

1. Precludes lengthy vetting if statutory grounds for ineligibility or bars exist
2. File review and required systems and security checks must be complete and valid
3. Includes adjudicative and internal vetting activities
4. Deconfliction must occur prior to decision
5. Further internal vetting may be required if no grounds of ineligibility are evident or grounds may be easily overcome
6. Officers should understand that the guidance for the eligibility assessment, internal and external vetting vary slightly among that of Directorate of Domestic Operations and those of the components within the Office of Refugee, Asylum and International Operations in order to accommodate unique aspects found in each program.
7. Completed by Designated Officers
  - a. Internal vetting on KSTs and non-KSTs

**LE**

**B. Internal Vetting**

1. Prior to initiating internal vetting, consider:
  - a. Does the derogatory information relate to the subject?
    - i. Confirm identity.
    - ii. Do not assume that the information in the security check relates to your applicant.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- b. Does the information in the referral meet the criteria for a NS concern?
  - i. If not, or if information comes to light that the concern no longer remains, the case may be returned to the routine adjudication process.
- c. What types of systems checks should be run to support the determination for eligibility, admissibility, credibility?

**LE**

**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

## 2. Internal Vetting: Systems Checks

FDNS-Data System (FDNS-DS) USCIS System	Query people, organization, and addresses for fraud and NS links
National File Tracking System (NFTS) USCIS System	Search for unconsolidated A/T/Receipt files
Central Index System (CIS)	Search for unconsolidated A/T/Receipt files Search for Aliases
Computer Linked Application Information Management System (CLAIMS) 3 & 4 USCIS Systems	Obtain filings as beneficiary and petitioner Obtain addresses
<b>LE</b>	
<b>LE</b> TECS	Due to NS concern
<b>LE</b>	
Commercial Databases	Results of street addresses, businesses, & associates can be queried in FDNS-DS and in SQAD
Arrival and Departure Information System (ADIS)	Travel History
<b>LE</b>	
Consular Consolidated Database (CCD) Department of State System	In addition to non-immigrant, immigrant, and DV visa queries, a "Text Search" is available

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

	under Cross Applications which allows for a search by names, addresses, businesses, phone numbers, etc.
<b>LE</b>	
ENFORCE	Query by name, FINS or Biometric information to obtain immigration violations
Image Storage Retrieval System (ISRS) USCIS System	Assists in determining identities (photo/fingerprint)
Benefits Biometric Support System (BBSS)	Assists in determining identities (results of fingerprint checks to include availability of RAP sheet)
<b>LE</b>	
United States Visitor and Immigrant Status Indicator Technology (US-VISIT)	Biometric system used by DOS/CBP/Asylum Branch
Refugee, Asylum, and Parole System (RAPS) Teleview	Used by Asylum Branch
Deportable Alien Control System (DACS) Teleview	Detention & Removal docket management system which is to be replaced by ENFORCE Alien Removal Module (EARM)
Student and Exchange Visitor Information System (SEVIS)	Student status
Open source/Internet Queries	Google, Yahoo, Ask.com, Dogpile, Youtube, MySpace, LinkedIn, etc.

### 3. Internal Vetting: Methods, Techniques, and Other Tools

a.

**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**Participant Guide**

b.

c.

d.

e.

f.

g.

h.

i.

j.

**LE**

Refer to the March 2006 "Guide to Names and Naming Practices" which provides by nationality typical components of a name, unique characteristics of naming customs, and common spelling variations in English of names.

<http://dockets.justia.com/>

<http://fdns.uscis.dhs.gov/>

k. Intel Fusion

<https://intel.ice.dhs.gov>

**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



ii.

LE

iii.

iv.

l. USCIS Intranet - Asylum Virtual Library provides background and historical information regarding country conditions.

<http://powerport.uscis.dhs.gov/intranet/asylum/index.htm>

m. USCIS Intranet - Country of Origin Unit background and historical information regarding country conditions.

<http://powerport.uscis.dhs.gov/rjc/index.htm>

n. CBP's Special Interest Alien Handbook

o. USPER

LE

p. Using sensitive or classified information as leads for research, RFEs, and lines of inquiry

LE

How does one ensure that that the people with which they discuss cases have

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

the appropriate clearance?

**LE**

Include First Name, Middle Initial, Last Name and agency about the individual you are requesting security clearance verification.

#### 4. Documenting

- a. Outlines a set of facts that can be used to determine whether a national security concern exists, existed at one time but is no longer present or has not yet been eliminated to the satisfaction of the investigating agency.
- b. Provides a record of the status and results of security and systems checks, as well as results of inquiries to and responses from offices within USCIS, components within DHS and external agencies which provides information relevant to USCIS' determination of eligibility.

c.

**LE**

d.

e. Other Government Agency (OGA)

f.

**LE**

- g. Include the date the check was conducted and the results, whether positive or negative.
- h. The source (system) of the information and date obtained should be annotated clearly annotated in order to protect against any unauthorized disclosure of Third Agency information or information protected by confidentiality provisions, such as Asylum, VAWA, Legalization, etc.
- i. If results of an internet search are referenced, the website address (URL) and date the information was retrieved from the website should be annotated in the record at a minimum. Make sure to printout and/or attach a screen shot because information changes or disappears.
- j. Ensure that the appropriate caveats are on the prepared

#### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

documents (e.g. memoranda to file, e-mail correspondence).

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**Add below to FOUO caveat when TECS/IBIS information is present:**

This document and the data herein are derived from TECS and are loaned to USCIS for official use only. This document or the information contained herein should be directed to the agency from which the document/information originated or Customs and Border Protection - Freedom of Information Act (FOIA) Office. Disclosure provisions have been established by the document, Memorandum of Understanding between Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Services (USCIS) for use of the Treasury Enforcement Communications System (TECS).

k. Realize what is documented may end up in discovery.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**


This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**EPO #7: Identify the process for external vetting of cases involving national security concerns.**

**A. External Vetting Overview**

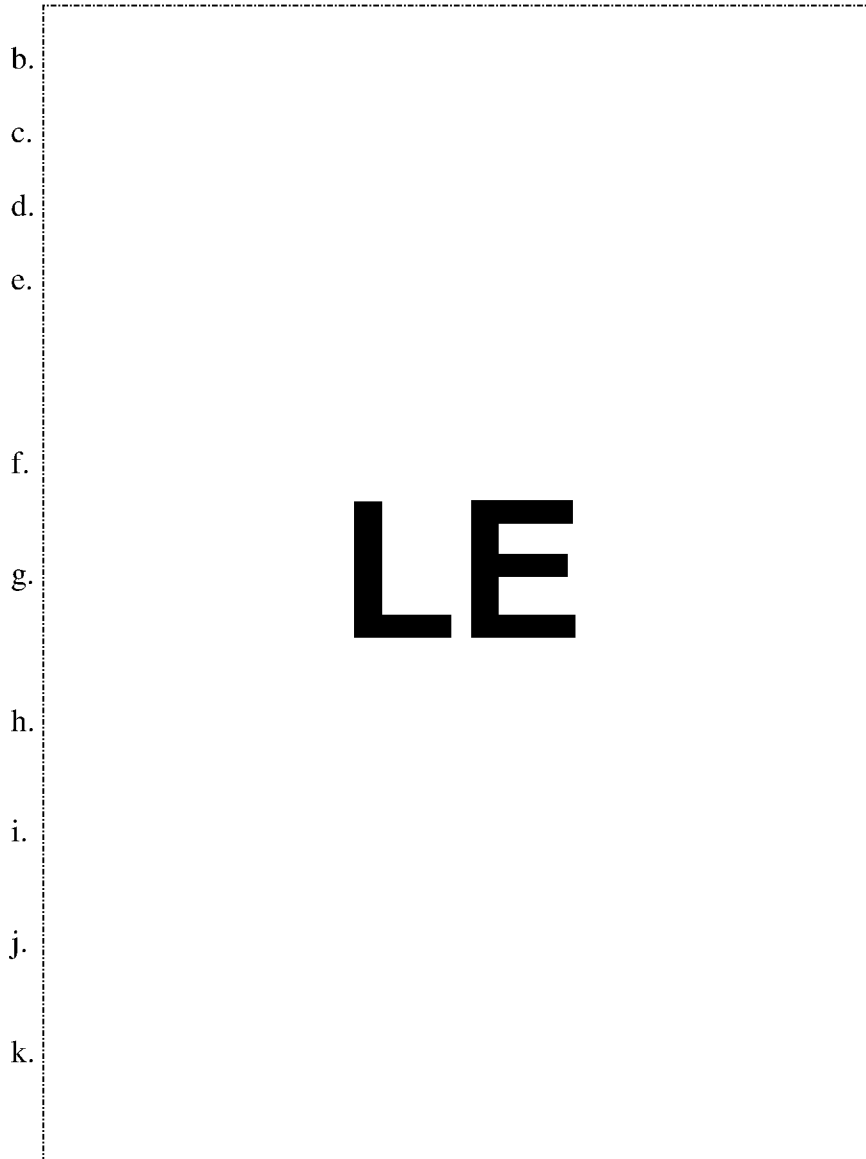
1. Consists of inquiries to record owners in possession of the national security information to identify: (a) fact or fact patterns necessary to determine the nature and relevance of the NS concern, including status and results of any ongoing investigation and the basis for closure of any previous investigation; and (b) information that may be relevant in determining eligibility, and when appropriate, removability.
2. Used as a last resort since obtaining detailed information about the national security concern is limited to those individuals who have a need to know to perform their official duties and requires security clearances when handling classified information.
3. For KSTs, HQFDNS has sole responsibility for external vetting
4. For Non-KSTs, the field is responsible for external vetting by Designated Officers
  - i. Generally BCU and FDNS IOs
  - ii. For Overseas Offices, IO HQ

**B. External Vetting of Non-KST NS Concerns**

1. Preparation for Non-KST External Vetting
  - a. Be familiar with the individual's immigration status, pending applications
  - b. Be familiar to the extent the information is available (e.g. results of IBIS hit);
  - c. Develop lines of inquiry for case discussion with record owner
  - d. 
2. Outreach
  - a. Be aware that the outside agency may not know who USCIS is or understand what USCIS does

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



USCIS Office of Security & Integrity intranet site.

<http://osi.uscis.dhs.gov/>

### 3. Considerations for Information Sharing and Confidentiality

All DHS components are considered part of one “agency” for information sharing purposes. As such, there is no restriction on internal (within DHS) information exchange and sharing provided the person has an authorized purpose for accessing the information in the performance of his or her duties (i.e., a valid need-to-know), possesses the requisite security clearance (there is no requirement for a security clearance to access sensitive but unclassified (FOUO) information), and assures adequate safeguarding and protection of

*See “DHS Policy for Internal Information Exchange and Sharing” dated February 1, 2007.*

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

the information.

Sensitive but unclassified (FOUO) information may be shared with other agencies or organizations outside of DHS, provided: a need-to-know has been established; the information is shared in the furtherance of a coordinated and official governmental activity, to include homeland defense; and if the information requested or to be discussed does not belong to USCIS, comply with the originating agency's policy concerning third party discussion and dissemination.

Classified information originated by another DHS component, or classified information originated by another government agency shall not be further disseminated outside of DHS without prior approval of the originator.

a. Privacy Act, 5 U.S.C. 552(a)

- i. Protection against unauthorized disclosure of information collected and maintained in USCIS systems of records both in the electronic and paper form.
- ii. Restricts disclosure of information relating to U.S. citizens and LPRs in the absence of a written waiver from the individual to whom the information pertains or a routine use contained in a DHS SORN.
- iii. By policy, DHS has extended the protections afforded by the Privacy Act to personally identifiable information contained in mixed records systems (i.e., systems containing information on visitors and aliens as well as on LPRs and U.S. citizens).

<http://ors.uscis.dhs.gov/foia/index.htm>

A contact list of FOIA/Privacy Officers is also provided on the website.

b. Confidentiality Provisions

- i. Sections 210 and 245A of the Immigration and Nationality Act limit the use and disclosure of information provided by "amnesty" applicants under the 1986 Immigration Reform and Control Act.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- ii. Section 384 of the 1996 Illegal Immigration Reform and Immigrant Responsibility Act, as amended, 8 U.S.C. 1367, limits the use and disclosure of information relating to aliens seeking protection under the Violence Against Women Act (VAWA), as amended, or as T or U non-immigrants.
- iii. Under 8 C.F.R. § 208.6, information regarding an individual's status as an asylum seeker or asylee, information contained in or pertaining to his or her application, and records pertaining to any credible fear or reasonable fear determination generally must not be disclosed without the written consent of the applicant or a waiver from the Secretary of DHS. By policy, the confidentiality provisions of 8 C.F.R. § 208.6 have been extended to information contained in or pertaining to refugee applications.

See Memorandum entitled "Confidentiality of Asylum Applications and Overseas Verification of Documents and Application Information" dated June 21, 2001 and Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants dated June 3, 2005

#### c. Records Sharing

- i. Part I, Section 14 of the Records Handbook addresses how to handle requests from outside agencies to review USCIS files.
- ii. Outside agencies may be permitted to review a USCIS file for law enforcement purposes and under the routine use provision described by the specific Privacy Act notice for the type of record requested.
- iii. State or local agencies who want access to records for reasons other than law enforcement or a routine use purposes described by the Privacy Act notice may file a Freedom and Information Act (FOIA) request.
- iv. Any questions regarding the sharing of files should be addressed to the Records section of USCIS.

The Record Handbook can be found on the DHSONLINE Portal, at the USCIS Office of Records Services website:  
[http://ors.uscis.dhs.gov/pol\\_imp/roh/index.htm](http://ors.uscis.dhs.gov/pol_imp/roh/index.htm)

#### 4. Other Considerations when Externally Vetting Non-KSTs

- a. Understand the importance to law enforcement agencies of the chain of custody of evidence in criminal proceedings.
- b. Be aware that agencies post hits in TECS for a variety of

#### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

reasons. The objective of the conversation with the record owner is to determine if the reason the hit was posted was based on an articulable concern.

- i. Gather information and evidence for criminal prosecution
- ii. Informational and historical purposes
- iii. Intelligence collection which may support investigative initiatives or may be for targeting or pattern analysis.

c. Note-taking

Take clear notes during the conversation with the record owner and ensure that the answers to questions asked are accurately documented. In some instances, the Officer may need to take notes pertaining to classified information. The classified notes page must adhere to the protocol for derivative information from a classified source and must be protected accordingly.

5. Liaisons with DHS Components

- a. In accordance with DHS policy, all DHS components are considered one agency. Information from these components is oftentimes "Law Enforcement Sensitive" and must be protected regardless.
- b. All DHS components are considered part of one "agency" for purposes of the Privacy Act 5 U.S.C. § 552a(a)(1), (b)(1).
- c. No DHS component should consider another DHS component to be a separate agency for information-sharing purposes.
- d. Absent any legal prohibitions as set forth by the Department's General Counsel, information shall be shared within DHS whenever the requesting officer or employee has an authorized purpose for accessing the information in the performance of his or her duties(2), possesses the requisite security clearance, and assures adequate safeguarding and protection of the information.

Memorandum, "DHS Policy for Internal Information Exchange and Sharing" dated February 1, 2007

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

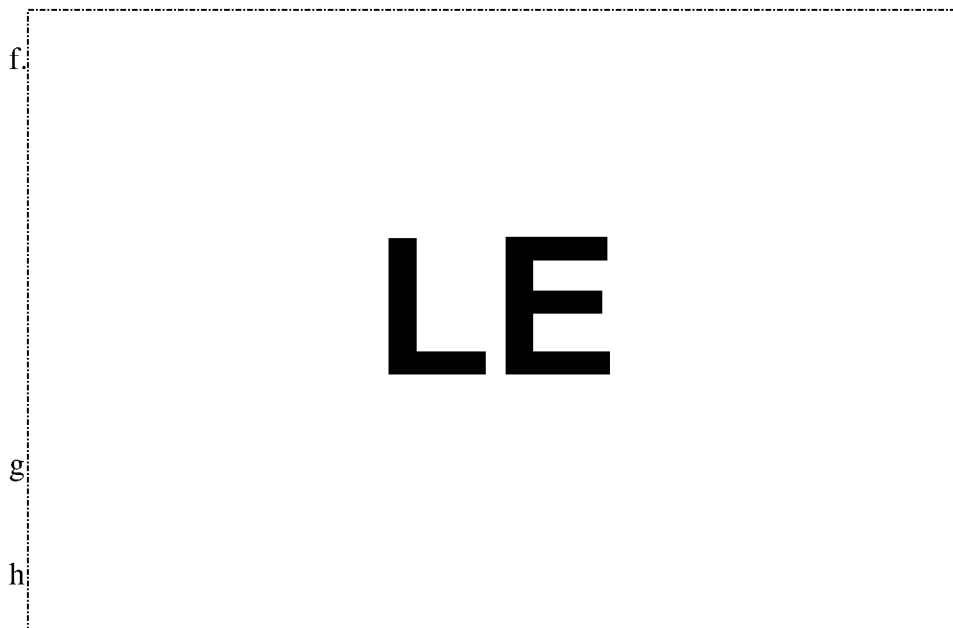
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



- e. From this point forward, information-access and -sharing agreements with outside entities will be negotiated and entered into on behalf of the Department as a whole, not on behalf of an individual DHS component.
- U.S. Secret Service (USSS)
  - U.S. Coast Guard
  - U.S. Immigration and Customs Enforcement (ICE)
  - U.S. Customs and Border Protection (CBP)
  - Transportation Security Administration (TSA)
  - U.S. Citizenship and Immigration Services (CIS)
  - Federal Emergency Management (FEMA)
  - Directorate for National Protection Programs
  - Directorate for Science and Technology
  - Directorate for Management
  - Office of Policy
  - Office of Health Affairs
  - Office of Operations Coordination
  - Office of Intelligence and Analysis
  - Federal Law Enforcement Training Center (FLETC)
  - Domestic Nuclear Detection Office
6. Liaison with CBP's National Targeting Center (NTC)
- a. Established on October 22, 2001.
  - b. 24/7 operation with the centralized mission of coordinating anti-terrorism targeting and supporting all CBP Anti-Terrorism activities.
  - c. Supports and responds to inquiries from the field, conducts tactical targeting to identify actionable targets, develops Automated Targeting System (ATS) rules, and supports Intelligence Driven Special Operations (IDSO).
  - d. All Terrorist Watch list encounters by CBP are processed through the NTC.
  - e. Liaisons assigned to the NTC-P: U.S. Coast Guard, ICE, TSA, Office of Intelligence, Federal Air Marshal Service and FBI.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



7. Liaison with Joint Terrorism Task Force (JTTF)

Retrieved on 4/15/08  
from

[http://www.fbi.gov/pa  
ge2/dec04/jtff120114.h  
tm](http://www.fbi.gov/pa/ge2/dec04/jtff120114.htm)

- a. JTTF was established in the 1980s.
- b. The FBI is the lead agency for terrorism investigations and the JTTFs.
- c. JTTFs serve three main purposes:
  - i. prevent terrorist attacks;
  - ii. respond to and investigate terrorist incidents or terrorist-related activity; and
  - iii. identify and investigate domestic and foreign terrorist groups and individuals targeting or operating within the U.S.
- d. The National JTTF (N-JTTF) located at FBI headquarters, includes representatives from a number of other agencies.
- e. The task forces are composed of federal, state, local agencies and are located in over 100 locations throughout the U.S.
- f. USCIS liaises with JTTF through the ICE representative on JTTF. The following list of agencies are full-time members of

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

## JTTFs:

- Air Force Office of Special Investigations (AFOSI)
- Bureau of Alcohol, Tobacco, and Firearms (ATF)
- Central Intelligence Agency (CIA)
- Customs and Border Protection (CBP)
- Defense Criminal Investigative Service
- Department of Interior's Bureau of Land Management
- Diplomatic Security Service (DSS) (within DOS)
- Federal Protective Service (FPS) (within ICE)
- Immigration and Customs Enforcement (ICE)
- Internal Revenue Service (IRS)
- Naval Criminal Investigative Service (NCIS)
- Postal Inspection Service
- Treasury Inspector General for Tax Administration
- U.S. Border Patrol (within CBP)
- U.S. Park Police
- U.S. Army
- U.S. Marshall Service (USMS)
- U.S. Secret Service (USSS)

## 8. Guardian Threat Tracking System

- a. FBI web-based counterterrorism incident management application that allows terrorism threats and suspicious activities to be viewed instantaneously by all users.
- b. Purpose of the system is to ensure that threat information is available immediately to all users, to have the capability to search incidents for trends and patterns to be able to forward threat data to other divisions or users and to ensure that no terrorism incident is left uninvestigated.

**C. External Vetting Decision Criteria**

At the conclusion of the external vetting process for Non-KST NS concerns, the designated officer must consider the facts or fact patterns developed and determine whether the case is Non-National Security and release for routine adjudication OR National Security and proceed to final adjudication of the CARRP process.

Domestic Operations:  
See p. 23-24  
“Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns” dated April 24, 2008, signed by Don Neufeld.

1. A Non-National Security determination should be made if results of

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

the external vetting fall into one or more of the following categories:

a.

b.

c.

d.

e.

f.

g.

h.

i.

j.

k.

l.

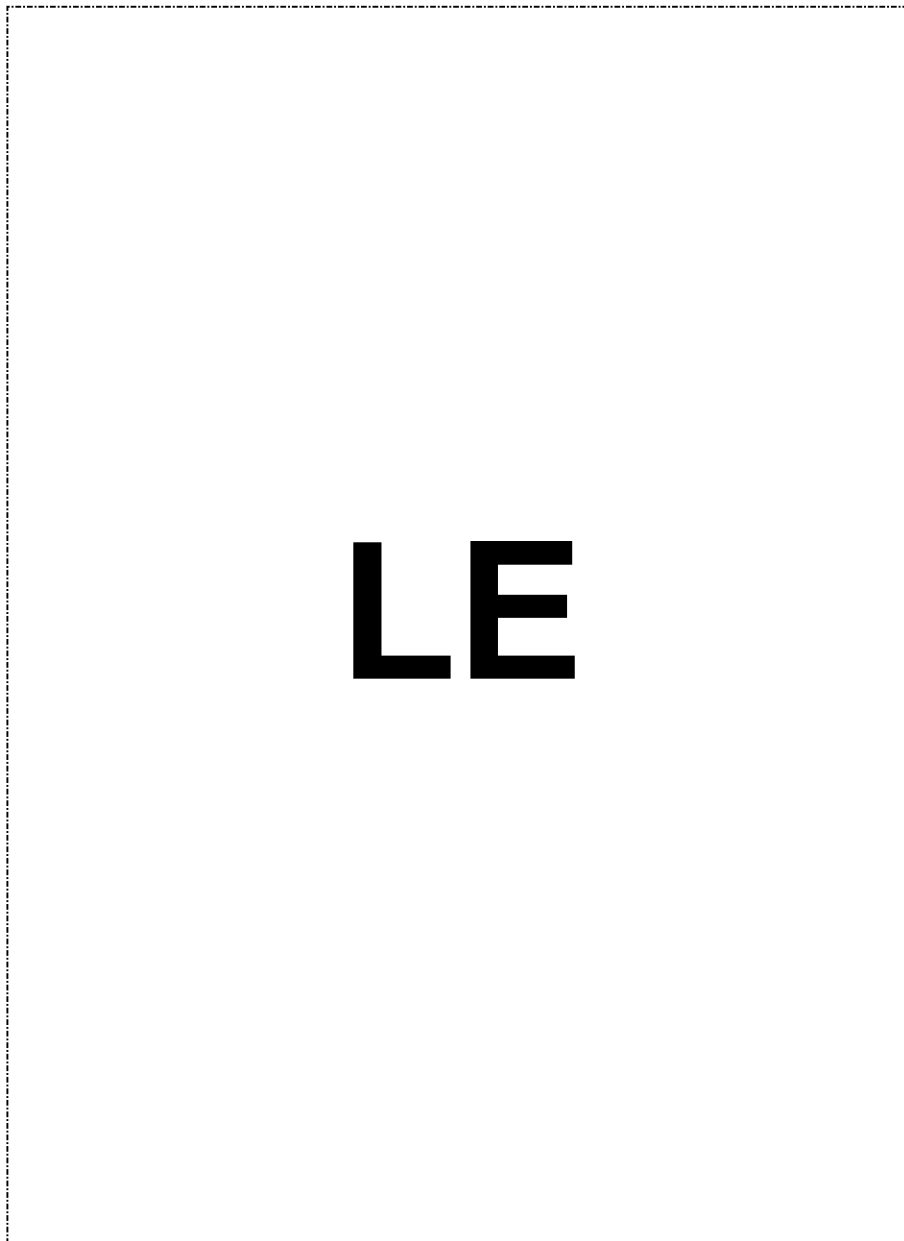
m.

**LE**

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

2. A National Security determination should be made if results of the external vetting fall into one or more of the following categories:



**D. Request for Assistance to HQFDNS**

1. General Types of Requests

Domestic Operations:  
See “Operational  
Guidance for Vetting  
and Adjudicating Cases

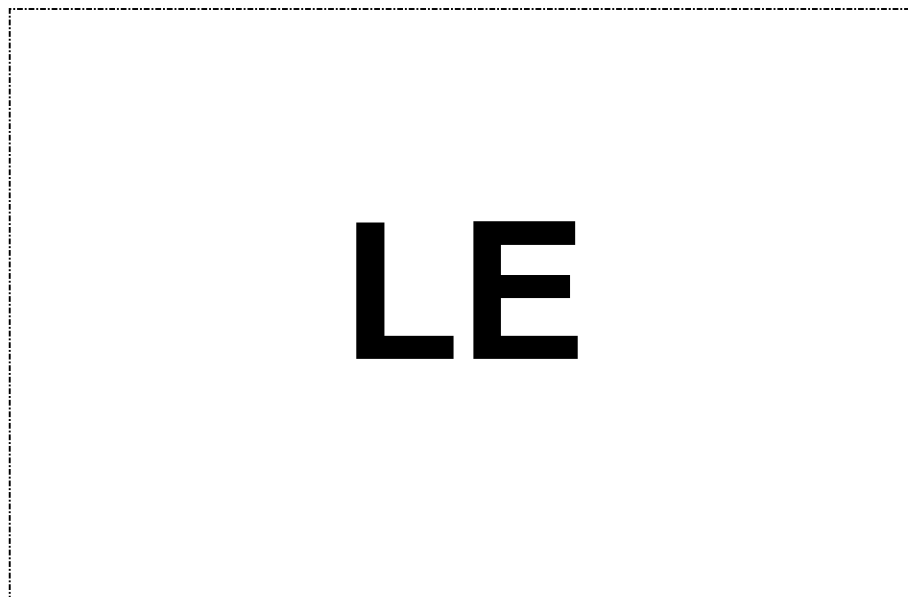
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- a. Unable to determine if articulable concern exists to NS
- b. Internal vetting KSTs/non-KSTs
- c. External vetting of non-KSTs
- d. External vetting of KSTs
- e. If a NS concern remains but a record owner cannot be identified
- f. Coordination with Intelligence Community members
- g. If the local JTTF office is not responsive
- h. Unable to identify a POC for Third Agency Referrals (positive response from FBI Name Check)
- i. Adjudicative advice
- j. Assistance for declassification/use of classified information

with National Security Concerns” dated April 24, 2008, signed by Don Neufeld.

2. Method of Request



3. Intelligence Community (IC)  
Requests for information from the intelligence community should be routed to HQFDNS.

HQFDNS has the capability to query classified systems and send official requests to members of the intelligence community.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

## a. High Side Checks

Database checks of information and intelligence systems on the Joint Worldwide Intelligence Community System (JWICS) that may include information up to and including TOP SECRET and Sensitive Compartmented Information (SCI) information.

- i. NCTC (National Counterterrorism Center) online
  - A. primary source of terrorism information/intelligence produced by the NCTC.
  - B. NCTC intelligence products come from the intelligence community
- ii. TIDE (Terrorist Identities Datamart Environment)
  - A. U.S. government central repository of information on international terrorist identities.

B.

**LE**

iii.

**LE**

## b. Executive Order 12333

“United States Intelligence Activities” dated December 4, 1981, requires all government agencies and departments involved in intelligence activities to provide the President and the National Security Council with intelligence information to protect the United States from security threats. Government agencies and departments within the executive branch that have a national intelligence mission are collectively called the Intelligence Community (IC).

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

## c. Executive Order 13354

“National Counterterrorism Center” dated August 27, 2004, requires all government agencies that possess or acquire non-domestic terrorism and counterterrorism information to immediately notify the National Counterterrorism Center (NCTC).

## d. Members of the IC include:

- Director of National Intelligence
- Under Secretary of Defense for Intelligence
- Air Force Intelligence
- Army Intelligence
- Central Intelligence Agency
- Coast Guard Intelligence
- Defense Intelligence Agency
- Department of Energy
- Department of Homeland Security
- Department of State
- Department of the Treasury
- Drug Enforcement Administration
- Federal Bureau of Investigation
- Marine Corps Intelligence
- National Geospatial-Intelligence Agency
- National Reconnaissance Office
- National Security Agency
- Navy Intelligence

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



**EPO #8: Identify the steps involved in adjudicating a case involving national security concerns.**

While our agency mission is to administer the benefit provisions of immigration law, our primary mission and obligation is to protect national security.

Adjudications Officers reviewing cases involving national security concerns must:

1. Seek to ensure that those who pose a threat to national security do not obtain immigration benefits
2. Protect Sensitive But Unclassified (SBU) information and classified information from disclosure

**A. Adjudicative Steps for Cases Involving National Security**

1. Ensure that if the file or a document is classified, the Officer has a “need to know” and the appropriate clearance to review the classified material. Ensure that the classified material is appropriately marked and properly stored.
2. Notify local USCIS Office of Chief Counsel (OCC) attorney if the case is in litigation and determine due dates.
3. Check Central Index System and NFTS for relating files and charge file to Officer.
4. Check FDNS-DS to ensure case is up-to-date. Update adjudicative activities regularly in FDNS-DS.
5. Review the information gathered during internal vetting (and external vetting, if applicable) to understand the actions that have been taken. Review the designated worksheet(s) and any older versions of the national security document such as National Security Record (NSR), Case Resolution Record (CRR), the National Security Notification (NSN), the Significant Incident Report (SIR), and any other IBIS resolution forms.
6. Review file completely which includes ensuring that the required security checks (IBIS, FBI Fingerprint, FBI Name Check, IDENT/USVISIT for asylum cases) are complete and valid.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

7. Establish a detailed timeline of the subject's immigration history, noting any and all discrepancies.
8. Verify the authenticity of documents and information provided by the subject with the Department of State (DOS) via DOS Reciprocity Tables, CCD, official request to DOS consular office where the subject and family members were born, lived, attended school, etc.
9. Perform open source searches and print out pertinent information.
10. Look for consistency in testimony and documentation to establish credibility. If there are inconsistencies, follow up questions or a Request for Evidence (RFE) may be required to explain the inconsistencies. The answers to the questions or RFE will assist the officer to make a credibility finding and determine how a negative finding of credibility may impact the eligibility for the benefit sought, as it relates to USCIS discretionary authority or Good Moral Character.
11. Clearly document changes made to the application or petition during the interview. Clearly note inconsistencies or irregularities as well as responses to follow up questions relating to the inconsistencies or irregularities on the Adjudicator's Worksheet, in a Memorandum to File or in a sworn statement.
12. Formulate adjudication strategy and discuss with management, OCC and/or NSAU/HQFDNS, as appropriate.
13. Prepare a detailed line of inquiry for interview and/or RFE, Notice of Intent to Deny (NOID) or Notice of Intent to Terminate (NOIT).
14. Deconflict with law enforcement prior to interview or issuance of RFE, NOID, NOIT.
15. Interview or issue RFE, NOID, NOIT. In certain instances, the interview may be audio or video taped.
16. Draft decision. Among considerations when drafting are questions regarding who will sign the decision, legal sufficiency and anticipated court activity.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

17. Deconflict with law enforcement prior to final decision.
18. Obtain supervisory concurrence for final decision and update the designated worksheet(s).
19. Issue decision.
20. Issue Notice to Appear (NTA), if appropriate. Coordinate with law enforcement agency, OCC, and ICE Counsel.

Note: FDNS is the primary conduit for coordination with law enforcement and therefore deconfliction is generally conducted by FDNS officers.

### **B. Application of 212(a)(6)(C)(i) Inadmissibility and Good Moral Character (GMC)**

1. Inadmissibility for Willful Misrepresentation or Fraud
  - a. An alien who either by fraud or willfully misrepresenting a material fact seeks to procure a visa, documentation, or admission into the United States or for any other immigration benefit is inadmissible Section 212(a)(6)(C)(i) of the INA.
  - b. Does not need to be under oath
  - c. Does not matter if given orally or in writing
  - d. Material fact is information that is necessary for the alien to be eligible for the benefit
  - e. Examples
    - i. Submitting a fraudulent birth certificate to establish a mother/daughter relationship for Form I-130, Petition for Alien Relative
    - ii. Using a fraudulent passport at time of entry
    - iii. Submitting fraudulent employment history to obtain an employment visa
  - f. Remember and consider the alien may be eligible to apply for a waiver of this inadmissibility under section 212(i).

#### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

## 2. Good Moral Character (GMC)

- a. For naturalization, found in sections 101(f) and 336(d) of the INA and 8 CFR 316.10(b)(2)(vi).
- b. False testimony under oath for the purpose of obtaining an immigration benefit constitutes a bar to a finding of GMC if the testimony was given in the period the applicant must show GMC.
- c. Testimony does not need to be material.
- d. False testimony must be under oath **and** given orally.
- e. Case law supports the idea that misrepresentation need not be material at the time of the N-400 interview but in order to support a finding of poor moral character the misrepresented fact must be linked to some area of eligibility.
- f. Example:
  - i. USCIS knows the applicant has a criminal record but during interview the applicant claims no record. For false testimony, not only does the applicant need to admit to the criminal record but they need to admit why they kept the information from the interviewing officer.
  - ii. Other false statements, such as on a application, can lead to a conclusion that a person GMC, but the automatic bar only applies to false testimony.

### *In short:*

*The inadmissibility ground requires that the fraud or misrepresentation be material to obtaining an immigration benefit; however, does not require that the action or statement be under oath or given orally.*

*An automatic finding of lack of GMC for false testimony does not require that the testimony be material to the N400; however, it does require that the oral testimony is under oath.*

## **D. Use of Classified Information in Immigration Proceedings**

Officers **may consider** third agency information to understand the nature of the threat and to develop Requests for Evidence (RFE) or lines of inquiry **but may not disclose** the information (e.g. in an interview or written decision) without the express permission of the originating agency.

See DHS Memorandum "Department of Homeland Security Guidelines for the Use of Classified Information in

### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

**Furthermore, DHS policy precludes the use of classified information, as the basis for denial of a benefit, without (formal) authorization by the Secretary of DHS and permission of the owning agency.**

Immigration Proceedings”, dated October 4, 2004 and signed by Tom Ridge.

DHS policy for disclosing classified evidence requires multiple steps and is a time-consuming process which includes:

- Requesting declassification from owning agency
- Obtaining permission of owning agency
- Obtaining approval from ICE National Security Law Division
- Obtaining approval from the Secretary of Homeland Security

Requests for declassification or use of classified information must be made to HQFDNS as a last resort.

Keeping in mind that timely notification of litigation filing is critical as short timelines often cannot be met in cases that require:

- Declassification of pertinent information;
- Obtaining permission from a Third Agency to “use”/disclose information in a written decision; or
- Authorization to use classified information “in camera” by the Department.

Always remember that reviewing anything classified requires that all who see or hear the classified information have BOTH the clearance needed to review the material AND a need to know.

## **E. Federal Litigation**

### 1. 336(b) Actions

- a. Only naturalization applications (N-400)
- b. Applicant can file with court 120 days after interview
- c. Federal Court has jurisdiction

### 2. Mandamus

- a. May be filed on any type of application or petition with federal court
- b. USCIS maintains jurisdiction

#### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- c. The court will issue instructions to USCIS and other agencies to complete certain tasks within certain timeframes. For instance, a court may order the FBI to complete the FBI Name Check request within 45 days of the court's order with USCIS instructed to adjudicate the application within 45 days of the completion of name check.
3. Vetting and/or Adjudications Officer's Role
    - a. Notify USCIS counsel and supervisor of litigation.
    - b. Inquire about the next court deadline and expectations.
    - c. Know the case and next steps.
    - d. Don't make promises that cannot be kept. Be extremely frank with USCIS Counsel regarding issues, obstacles.
    - e. Notify USCIS Counsel if USCIS cannot meet deadlines. It is better to ask for an extension than to be found in contempt of court.
    - f. Anticipate court actions and respond appropriately
    - g. Notify USCIS Counsel of contemplated actions (e.g. site visit, interview, RFE, decision). In some Federal Circuits, concurrent jurisdiction is observed – effectively giving USCIS the opportunity to interview and request evidence from an applicant while the case is subject to court action. In other Circuits, courts hold that they have exclusive jurisdiction and that USCIS cannot take any action without the permission of the court, either through a remand or specific instructions.
    - h. Know local basic court procedures.
    - i. Maintain custody of file, copy for USCIS counsel.
  4. USCIS Office of Chief Counsel (OCC)
    - a. Represents USCIS' interests.
    - b. Liaison between USCIS (e.g. Adjudications or Vetting Officer) and Assistant U.S. Attorney
    - c. USCIS Counsel works with the AUSA to address court inquiries and should notify the AUSA of any intended action.
    - d. Coordinates appropriate information-sharing activities with the AUSA and will identify appropriate parties to the discussion.
  5. Assistant U.S. Attorney (AUSA)

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

- a. Represents USCIS in Federal Court
- b. Employed by the Department of Justice
- c. Familiar with court procedures and the preferences of individual judges.
- d. May offer advice regarding decisions, to include review of the decision to determine legal sufficiency and/or risk of bad case law
- e. Generally not very knowledgeable of immigration law
- f. Third Agency rule prohibits the disclosure to the AUSA of any law enforcement sensitive information in the possession of USCIS which originated with another agency, unless that source agency has consented to such a disclosure to the AUSA.

**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

## IV. APPLICATION

### A. In-Class Exercises

- 4 Scenarios - CARRP Case?
- 15 Scenarios - Identifying NS Concerns
- 2 Scenarios – Considering Classified Information
- 10 Scenarios – External Vetting

## V. REFERENCES

A. INA §§ 101(a)(43), 212(a)(3), 219, 237(a)(4), 237(c), 240(b)(4)(B),

B. 8 C.F.R. §§ 103.2(b)(16)(i)-(iv), 235.8

## VI. POLICY MEMORANDA

### A. National Security

1. USCIS Policy Memorandum, “*Policy for Vetting and Adjudicating Cases with National Security Concerns*”, dated April 11, 2008.

### B. FBI Name Check

1. USCIS Operational Memorandum, “*FBI Name Check Process and Clarification for Domestic Operations*,” dated December 21, 2006.
2. USCIS Memorandum, “*Revised National Security Adjudication and Reporting Requirements*,” dated February 4, 2008.

### C. Department of Homeland Security

1. “*DHS Policy for Internal Information Exchange and Sharing*” dated February 1, 2007.
2. DHS Secretary’s Memorandum, “*Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings*,” dated October 4, 2004.

### D. Asylum-related

1. “*Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies*” dated April 18, 2007.

#### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).



2. “*Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants*” dated June 3, 2005.
3. “*Protocols for Handling Asylee Adjustment Cases That May Warrant Initiation of the Asylum Status Termination Process*” dated July 19, 2004.
4. “*Confidentiality of Asylum Applications and Overseas Verification of Documents and Application Information*” dated June 21, 2001.

## VII. ADDITIONAL ELECTRONIC RESOURCES

- A. 2008 Customs & Border Protection Special Interest Alien Handbook
- B. Fraudulent Document Laboratory (FDL) Guides
  1. Middle Eastern Calendar Guide
  2. North African & Middle Eastern Stamp Guide (entry & exit stamps)
- C. 2008 National Counterterrorism Center Calendar
- D. Al Qaeda Manual
- E. A Guide to Naming Practices
- F. National Security Terms of Reference Tables
- G. USCIS Fact Sheet, “*Immigration Security Checks—How and Why the Process Works,*” dated April 25, 2006.
- H. Statement of Mutual Understanding of Information Sharing with Dept of Citizenship and Immigration Canada
- I. Websites for Basic and Supplemental Systems Checks
- J. Department of Homeland Security For Official Use Only (FOUO) Coversheet
- K. Sample Background Checklist
- L. Sample Classified Notes Page

### **FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).