

**EXHIBIT 58**  
**FILED UNDER SEAL**

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

---



# U.S. Citizenship and Immigration Services

## *BASIC*

### **COURSE 235 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

---

**JANUARY 2010**

**SYLLABUS****COURSE TITLE:** National Security**COURSE NUMBER:** 235**COURSE DATE:** January 2010**LENGTH AND METHOD OF PRESENTATION:**

Lecture	Lab	P.E.	Total	Program
6:00	0:00	2:00	8:00	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.**

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**DESCRIPTION:**

Discuss USCIS policies and procedures regarding the identification 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 Immigration Services Officer will be able to understand the security check process and specify criteria for identifying a national security concern. The Immigration Services Officer will have an understanding of the relevant USCIS components and processes associated with vetting and adjudicating cases with identified national security concerns.

**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 vetting and adjudicating applications or petitions in cases involving national security concerns.

**EPO #4:** Identify the types of security checks completed by USCIS as part of the background check process.

**EPO #5:** Discuss the term “national security concern” and methods used to identify cases involving national security concerns.

**EPO #6:** Identify the process for eligibility assessment, deconfliction, and external vetting of cases involving national security concerns.

**EPO #7:** Identify the steps involved in adjudicating a case involving 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**STUDENT SPECIAL REQUIREMENTS:**

Read pages 221 - 224 in *Immigration Law and Procedure in a Nutshell, 5<sup>th</sup> Edition*, by David Weissbrodt and Laura Danielson.

**NOTE:** Like other reference guides and textbooks, *Immigration Law and Procedure in a Nutshell* is written by a private author, and is **not** a U.S. Government publication. Accordingly, any opinions expressed in the text are those of the author, and not those of U.S. Citizenship and Immigration Services or the Department of Homeland Security. This text is being used to provide background information on the law to the student, in order that the student may apply that background to the duties performed by USCIS adjudicators.

Additionally, the Fifth Edition of this book was published in 2005. Since the immigration law and policy is constantly changing and evolving, it is always important to verify whether there have been changes to the law or procedures when using this or other reference materials.

**METHOD OF EVALUATION:**

Written Examination – Multiple Choice (Open Book)

**Handling For Official Use Only (FOUO) Material**

Materials and information are to be controlled, handled, transmitted, distributed, and disposed of in accordance with US DHS policy relating to Sensitive But Unclassified (SBU) information and is not to be released to the public, or other personnel who do not have a valid "need-to-know" reason without prior approval from the originator. It is important to note that the caveat "For Official Use Only" is NOT a security classification; however, FOUO material must be safeguarded.

- FOUO material should not be left unattended on desks
- FOUO material should be placed out of sight when not in use
- Unauthorized personnel should not be allowed in the area when FOUO material is being reviewed

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**TABLE OF CONTENTS**

	<b><u>PAGE</u></b>
<b>I. Introduction</b>	<b>9</b>
<b>II. A Terms of Reference in National Security Cases</b>	<b>10</b>
<b>II. B USCIS Organization and Functions in Processing National Security Cases</b>	<b>13</b>
<b>II. C USCIS Policies in National Security Cases</b>	<b>16</b>
<b>II. D Requirements for Security Checks</b>	<b>27</b>
<b>II. E Identification of National Security Concerns</b>	<b>47</b>
<b>II. F National Security Eligibility Assessment and Vetting Process</b>	<b>83</b>
<b>II. G National Security Case Adjudication</b>	<b>94</b>
<b>III. Summary</b>	
<b>IV. Application</b>	<b>101</b>
<b>V. References</b>	<b>107</b>
<b>VI. Appendix</b>	<b>A1</b>

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**Presentation****References****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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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

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

**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. Determination requires that the case be handled in accordance with Controlled Application Review and Resolution Program (CARRP) policy.

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

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.

4. 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



### 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)
  - 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).

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

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)

### E. Internal Vetting

- May consist of DHS, open source, or other systems checks; file review; interviews; and other research as specified in the Operational Guidance.

### G. Deconfliction

A term used to describe coordination between USCIS and another governmental agency owner of national security information (the record

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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.

## H. Designated Officer

Domestic Operations Guidance:

For purposes of CARRP, a designated officer is an Immigration Services Officer, Immigration Analyst, Immigration Officer, Adjudications Officer, Asylum Officer or Refugee Officer who has been designated by local management to be trained, competent and knowledgeable in CARRP procedures.

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

# Practical Exercise!

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

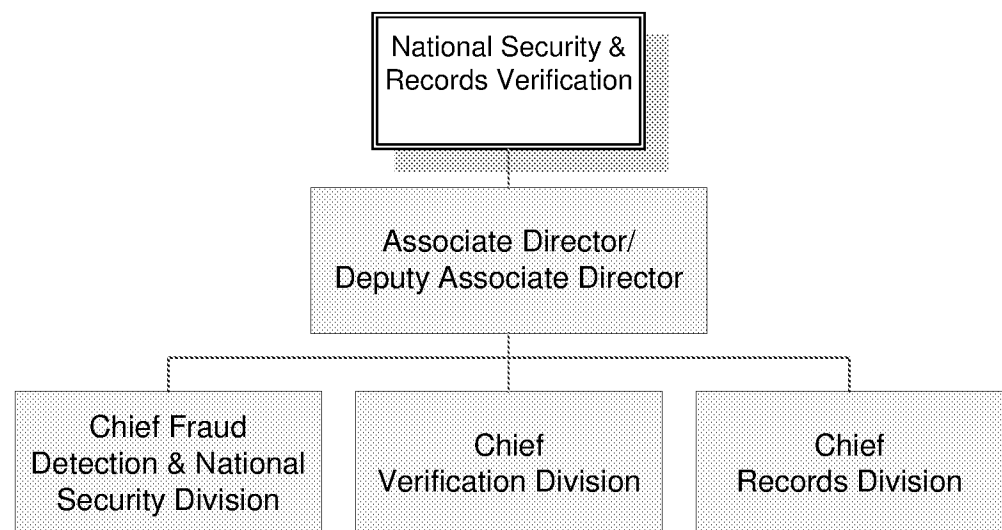
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**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 of Fraud Detection and National Security Division (FDNS) falls under the National Security and Records Verification (NSRV) Directorate. It was 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 Headquarters is composed of four separate branches: National Security, Intelligence, Fraud, and Mission Support.



**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**HQ FDNS National Security Branch**

1. National Security Branch (NSB):
  - a. One of four branches in HQFDNS
  - b. Provides support to USCIS officers in the field during the vetting and adjudication of cases with NS Concerns
  - c. Works closely with law enforcement agencies and the Intelligence Community to facilitate the exchange of information with the field
  
2. National Security Branch (NSB) at Headquarters FDNS
  - a. Operations Support Services
    - i. Triages requests for assistance from the field
    - ii. Provides subject matter expertise on adjudicative and vetting assistance
  
  - b. Program Oversight and Analysis
    - i. Conducts QA reviews and prepares reports and analysis
  
  - c. Policy and Program Development
    - i. Works with other components to develop and maintain national security policies
  
  - d. Other Government Agency Liaison
    - i. Works in partnership with law enforcement agencies and the Intelligence Community
  
    - ii. 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**

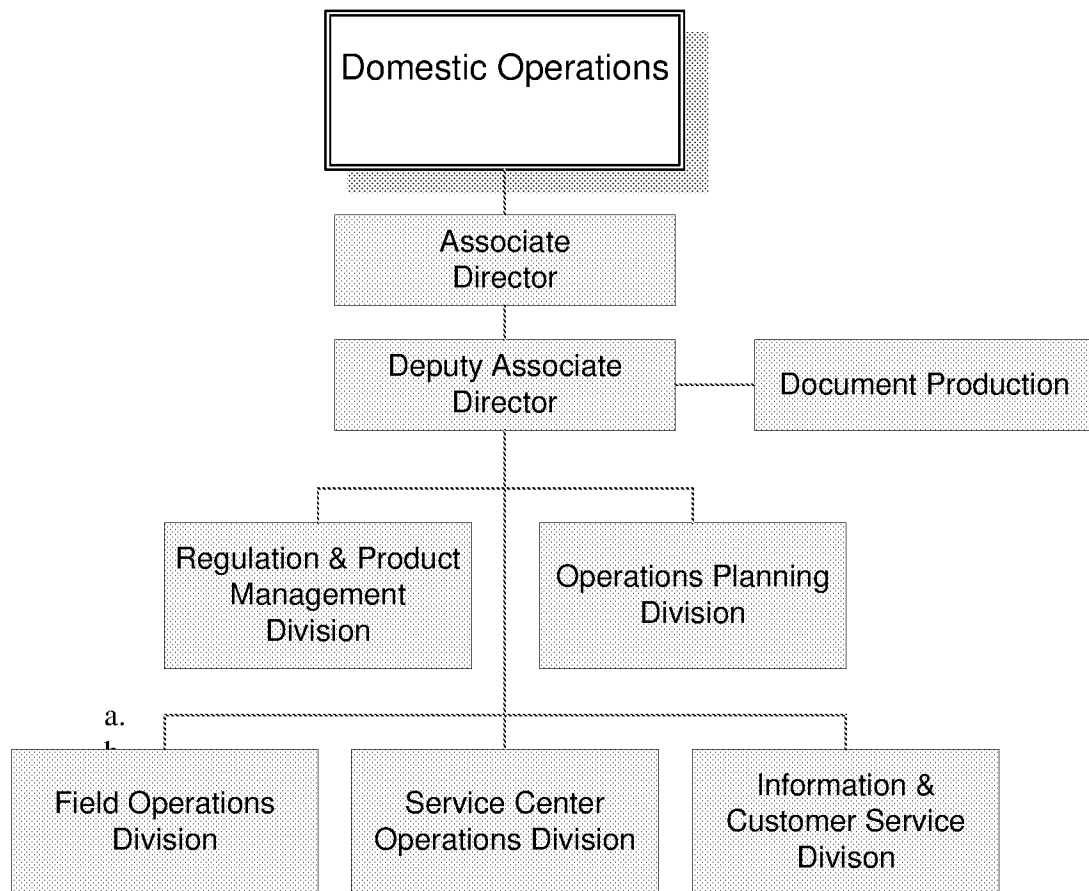
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**3. 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 system and removing those who pose a threat to the U.S.
- f. While FDNS IOs receive direction and oversight from HQFDNS, they report to and work for local management

**B. Office of Domestic Operations****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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



### 3. Service Centers:

- a. 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.
- b. All national security concerns and concerns are referred to local Background Check Units (BCU)
- c. FDNS Immigration Officers in the Center Fraud Detection Operation (CFDO) do not generally process the national security cases but may assist.

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

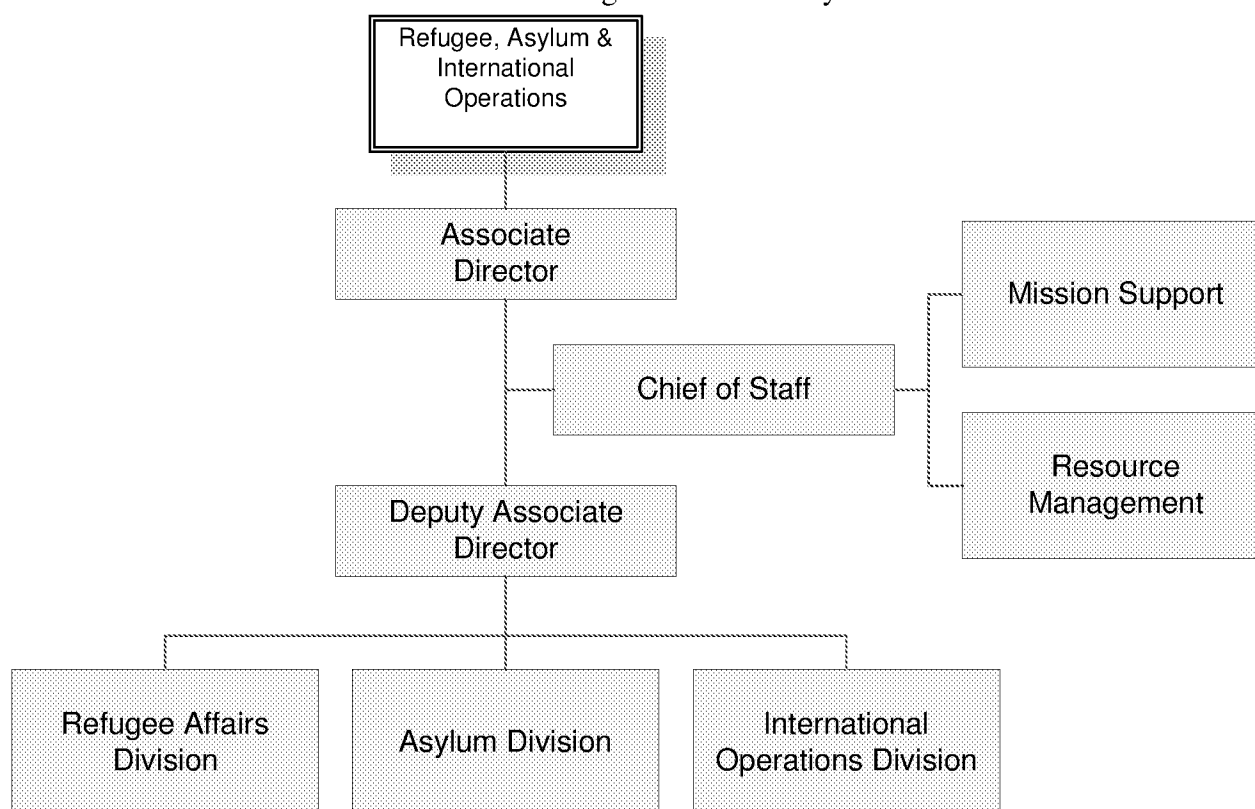
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

## 4. 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.
- iii. National Benefits Center (NBC) falls under the Office of Field Operations. BCU staff at NBC handle NS 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 monitor 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**EPO #3: Apply USCIS policies in vetting and adjudicating cases involving national security concerns.**

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

1. Provides agency-wide national security policy
  - Defines key terms so we (USCIS) are all on the same page
  - Rescinds multiple NS memos
2. Decentralizes the authority to vet and adjudicate cases with national security concerns
3. Effective with the issuance of operational guidance from the Directorate of Domestic Operations and each component within the Directorate of Refugee, Asylum, and International Operations (RAIO).
  - Domestic Operations - April 24, 2008
    - Field and Service Centers
  - International Operations - April 28, 2008
  - Asylum - May 14, 2008
  - Refugee - May 14, 2008
4. 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.
5. Distinguishes between two types of national security concerns
  - a. Known or Suspected Terrorist (KST)
  - b. Non-KST
6. Applies to all applications and petitions that convey immigrant or non-immigrant status
7. Rescinded specific previous USCIS national security policy

*“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”

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



---

**Participant Guide**

memoranda.

dated April 28,  
2008, signed by  
Alanna Ow.

8. Establishes a standard CARRP workflow consisting of four stages in order to identify, record, and complete applications/petitions with a national security concern
9. Completed by Designated Officers as outlined in each component's individual guidance.
10. Introduces Guidance for Identifying National Security Concerns (Attachment A).  
Used by all components
11. Introduced Background Check and Adjudicative Assessment (BCAA) located in FDNS-DS.

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

Policy and Operational Guidance introduces the reference tool, "Guidance for Identifying National Security Concerns" and the Background Check and Adjudicative Assessment (BCAA) .

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

---

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**B. Updated CARRP Guidance**

1. *“Additional Guidance on Issues Concerning the Vetting and Adjudication of Cases Involving National Security Concerns”* signed by Michael Aytes on February 6, 2009
  - a. Cases with unresolved national security concerns need USCIS Deputy Director’s concurrence for approval
  - b. Processing of CARRP cases where lookout **LE** has been removed from system
2. *“Revised Guidance Pertaining to the Adjudication of Form I-90, Application to Replace Permanent Resident Card”* signed by Donald Neufeld on February 6, 2009
  - a. Addresses both Egregious Public Safety and National Security cases
  - b. Issuance of I-551 will not be delayed due to any pending resolution
3. *“National Security Adjudication and Reporting Requirements Update”* signed by Donald Neufeld on February 9, 2009
  - a. Rescinds February 4, 2008 guidance to approve certain applications if Name Check is pending for over 180 days
  - b. All applications need a definitive FBI Name Check Response and IBIS resolution prior to final adjudication
4. *“Uniform Instruction for Standardized CARRP File Identification and Movement of CARRP Cases within the USCIS”* signed by Donald Neufeld, DOMO, Gregory B. Smith, Associate Director, NSRV on March 26, 2009
  - a. CARRP File Identification with specific coversheet
  - b. Creation of dedicated email accounts for CARRP 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**C. 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. (BCAA/FDNS-DS)
  - b. Thorough review for ineligibility and fraud concern
  - c. Deconfliction
  - d. If approved and the national security concern remains, TECS/IBIS record must be created in accordance with Operational Guidance

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

Domestic Operations Operational Guidance lists the petitions that do not convey immigrant/non-immigrant status:

I-129	(not requesting a Change of Status (COS) or Extension of Stay (EOS))
I-129F	Fiancé/e
I-130	Alien relative
I-140	Employment
I-360	Religious Worker cases only
I-526	Alien entrepreneur
I-600/I-800	Adoption
I-824	Application for action on petition

Why are these petitions not covered by CARRP\*?

These petitions are adjudicated based on eligibility. Since they do not convey status, inadmissibility is not considered during the adjudication.

Regardless, if a NS concern is identified, it must be documented in FDNS-DS and the BCAA.

The petition must also be carefully reviewed for an ineligibilities and potential fraud.

If the NS concern remains, lookouts are required to notify DOS. See the operational guidance for details.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Which applications and petitions does CARRP policy cover?

- All other applications
  - e.g. I-485, N-400, I-765, I-687, I-821, etc.
- Petitions
  - Form I-129 petitions requesting change of status (COS) or extension of Stay (EOS)
  - Form I-730 (alien relative of asylee or refugee)

### Field Responsibilities – CARRP:

Designated Officers in the FIELD are responsible for:

- Establishing articulable link
- Contacting the Terrorist Screening Center for KST NS concerns
- Internal and External Vetting of Non-KSTs
- Internal Vetting of KSTs
- Deconfliction on KSTs and Non-KSTs
- Adjudicating all NS related applications and petitions
  - Approvals on Non-KSTs require Senior level official in Field (see Ops Guidance)
  - If KSTs are otherwise approvable (after eligibility assessment/internal vetting), request for assistance to HQFDNS for external vetting

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

### HQFDNS Responsibilities - CARRP

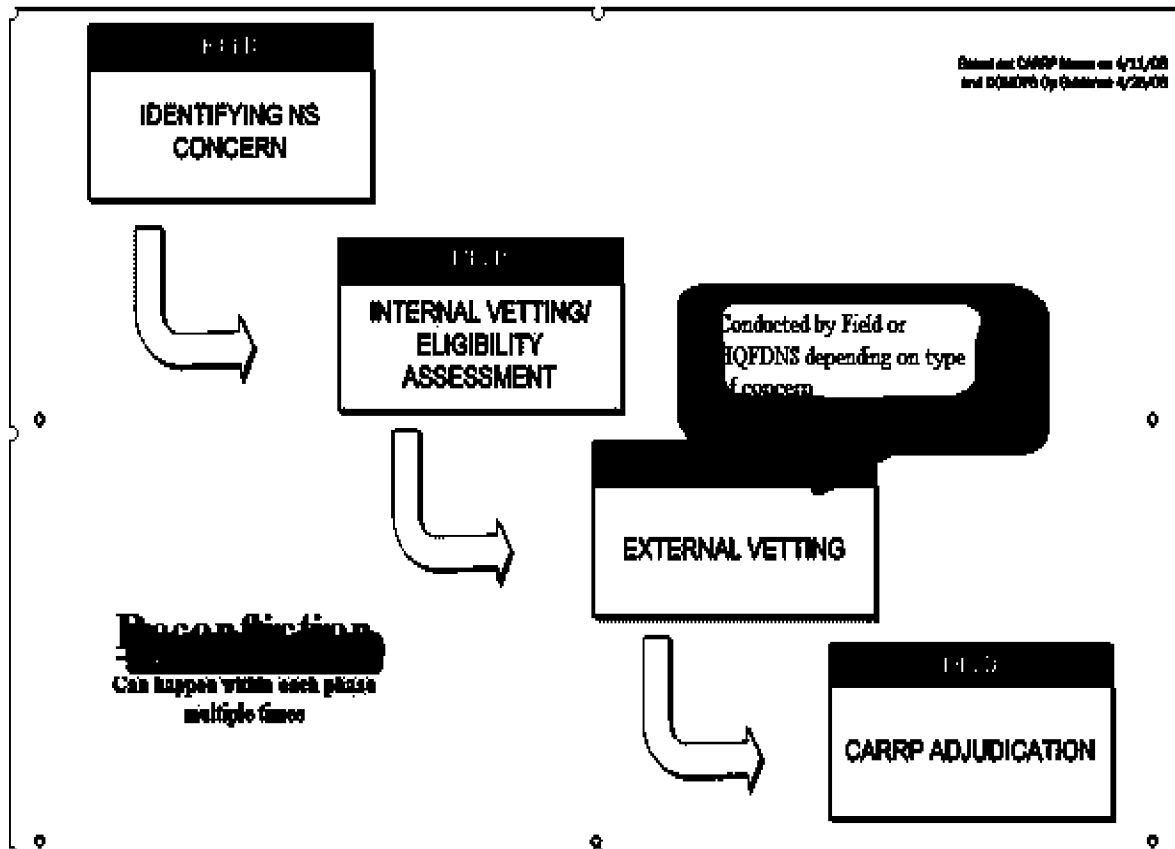
HQFDNS is responsible for:

- External vetting of KST hits Outreach to Intel Community, when required
- Requests for declassification/use of classified information
- Provides advice, technical assistance, and operational support on KST and Non-KST cases with NS concerns to the field
  - Vetting
  - Adjudication

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

## D. Four Stages in the CARRP Workflow



### 1. Identifying National Security Concerns

- a. Generally results from security check but may be identified from other sources at any time during the adjudication process

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- b. Confirm match
  - i. KSTs via Terrorist Screening Center (TSC) by designated officer
  - ii. Non-KSTs
- c. Determine and document articulable concern by designated officer
  - i. Background Check and Adjudicative Assessment (BCAA)
  - ii. FDNS-DS
- d. Consider effect of NS indicators relating to family members and close associates on the individual

In some instances, the petitioner, beneficiary, applicant, dependant or derivative may be a family member or close 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, business owner, partner, affiliate, or friend.

## 2. Eligibility Assessment includes 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

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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
  - d. For Non-KST NS concerns, the Field conducts external vetting
- ### 4. Final Adjudication of National Security Cases (CARRP Adjudication)

If NS concern remains, 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.

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

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



### D. CARRP Policy and Exemptions for the INA Section 212(a)(3)(B)(i) 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 or BCAA documentation 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

#### Material Support Cases - Guidance

- *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.* 7/28/08 Michael L. Aytes, HQ USCIS
- *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.* 3/26/08 Jonathan Scharfen, HQUSCIS
- *Authorization to process cases involving the provision of material support to the AUC.* 3/10/08 Paul S. Rosenzweig DHS Policy
- *Authorization to process cases involving the provision of material support to the ELN.* 12/18/07 Paul S. Rosenzweig DHS Policy
- *Processing the Discretionary Exemption to the Inadmissibility Ground for Providing Material Support to the Revolutionary Armed Forces of Colombia (FARC).* 09/06/07 Jonathan Scharfen HQUSCIS

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**Participant Guide**

- + (Material Support)
- Attachment: Material Support Exemption Worksheet
- *Processing the Discretionary Exemption to the Inadmissibility Ground for Providing Material Support to Certain Terrorist Organizations 5/24/07 Jonathan Scharfen*

Organizations or Other Groups”

AND

Dated May 24, 2007 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. Includes information on handling both NS concerns and egregious public safety concerns
  - a. Application for Employment Authorization (Forms I-765)
  - b. Application for Travel Authorizations (Form I-131)
  - c. Application for Replacement Permanent Resident Card (Form I-90) - updated guidance has been issued
  - d. Santillan Cases – also known as EOIR cases
  - e. Appeals/Motions to Reconsider or Reopen
  - f. Application for Naturalization

Designated Officer -----ALWAYS DECONFLICTS PRIOR TO USCIS ACTION!!!!!!

Santillan cases: Based on a class

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

---

**Participant Guide**

action lawsuit against USCIS. These are individuals (class members) who have been granted adjustment of status by an Immigration Judge, and based on the settlement regarding this lawsuit, USCIS must provide proof of their status within a certain period of time.

I-90 to replace permanent resident card – updated guidance\*

- Guidance includes NS and EPS cases
- The issuance of Form I-551, must not be delayed due to any pending resolutions.
  - *Derogatory information will be resolved only after the adjudication of the I-90 application.*

*\*See Interoffice Memorandum signed February 06, 2009: Revised Guidance Pertaining to the Adjudication of Form I-90.*

*Santillans aka EOIR grants who have not been issued evidence of their status*

- *USCIS must provide evidence of status within a certain time frame after the class member's InfoPass appointment (after the EOIR grant)*
  - *30 days if granted on or after 4/1/2005*
  - *60 days if granted before 4/1/2005*
- *Refer to*
  - *Dom Ops guidance p. 32-33 and*
  - *USCIS memorandum dated December 29, 2005, "Interim Guidance for Processing of Status Documentation for EOIR adjusted Lawful Permanent Residents Pursuant to Permanent Injunction in Santillan"*

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

**Reminders:**

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

---

**Participant Guide**

- Memorandum and Operational Guidance is For Official Use Only (FOUO)
- DHS Management Directive about Safeguarding Sensitive But Unclassified (SBU) Information aka FOUO for DHS purposes
- DHS Guidelines for the Use of Classified Information in Immigration Proceedings aka Ridge Memo

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

---

**USCIS ACADEMY  
NATIONAL SECURITY**

**26  
JANUARY 2010**

**EPO#4: Identify the requirements for conducting security checks.**

USCIS requires that specific checks or a combination of checks are completed for each application or petition type, pursuant to each component's procedures. These security checks are meant to identify any ineligibilities for the immigration benefit sought and to ensure the individual is not a risk to national security or public safety.

Each year that results in USCIS conducting different types of checks on 6-7 million individuals seeking immigration benefits.

**. USCIS Security Checks Overview**

In addition to records checks against USCIS immigration systems, the following additional security checks are conducted:

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).

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**FBI Name Check**

FBI's National Name Check Program (NNCP) reviews and analyzes potentially identifiable documents to determine whether a specific individual has been the subject of or mentioned in any FBI investigation(s), and if so, what (if any) relevant information may be disseminated to the requesting agency.

The NNCP conducts manual and electronic searches of the FBI's Central Records System (CRS) Universal Index (UNI). The CRS 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

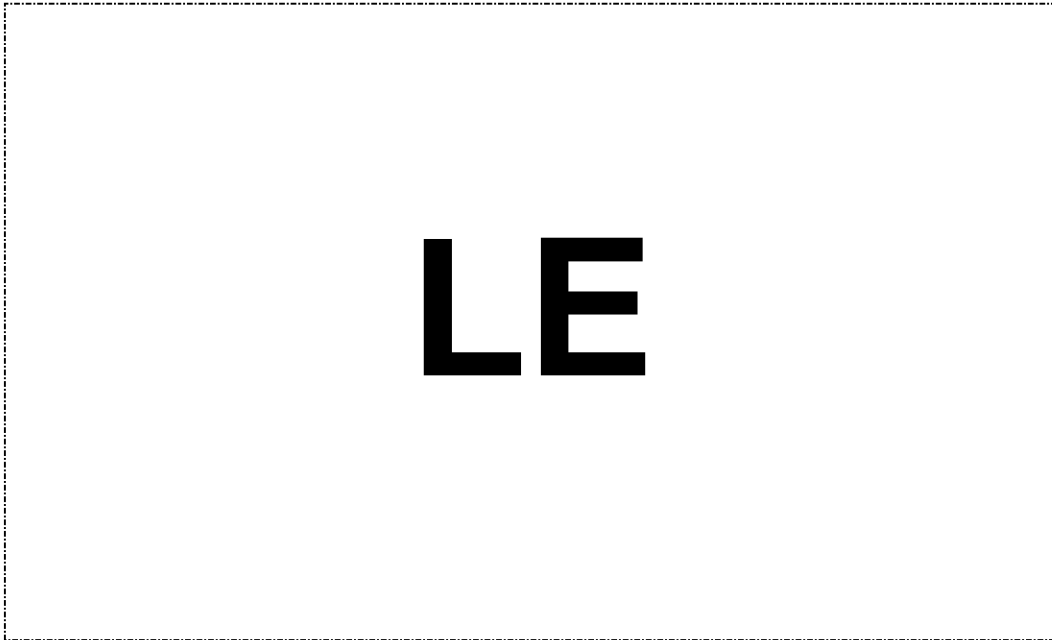
- Results
  - No Record
  - Positive Response
  - Unknown Response
  - Pending
- Validity
  - Definitive response valid indefinitely for application
  - For other applications, valid for 15 months

Agency/entity submission to the FBI's NNCP. Submissions are accepted via magnetic tape, hard copy, telephone, or fax. Today, they are submitted electronically.

LE

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

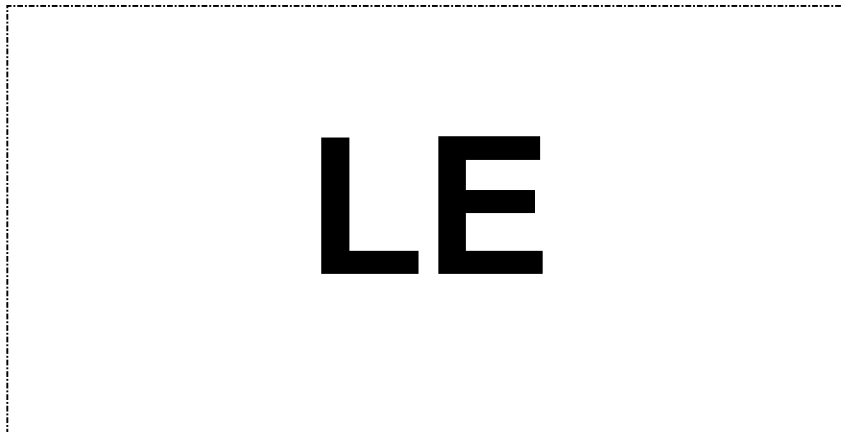
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



Results of FBI Name Check

The results of a FBI Name Check do not necessarily reveal the same information as do the results of the FBI's fingerprint check or IBIS.

a. Pending Response



*"FBI Name Check Process and Clarification for Domestic Operations"*, dated December 21, 2006

b. No Record (NR)



**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**Participant Guide**

**LE**

signed by Michael Aytes, Associate Director, Domestic Operations.

c. Positive Response (PR)

**LE**

d. Unknown Response (UN)

**LE**

-NOTE: See the PowerPoint for the Screen Shot of FBI Name Check.

-Also see the LHM-Letterhead Memorandum.

e. Validity of FBI Name Check

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



- a. A definitive (No Record, Positive or Unknown Response) is valid indefinitely for the application for which it was conducted.
- b. A definitive response used to support other applications is only valid for 15 months from the FBI process date.
- c. Only one definitive response is necessary. Adjudication may continue in those instances where a final FBI response has been received even though additional "pending" responses remain unresolved for that name.
- d. Age Limits –

An FBI Name Check is required for any applicant age 14 years and older at the time of adjudication except Form I-485, which has an upper age limit.

Form I-485: If an applicant is 80 years and a day, a name check will not be performed. For the purpose of the name check, the upper age limit of 80 years is defined as the date the applicant turns 80 years old.

If an applicant is less than 14 years of age at the time of filing but turns 14 years old while the application is pending, then a name check is required. If a new name check is required, the manual spreadsheet process must be used.

- e. Multiple Name Checks for Same Application –

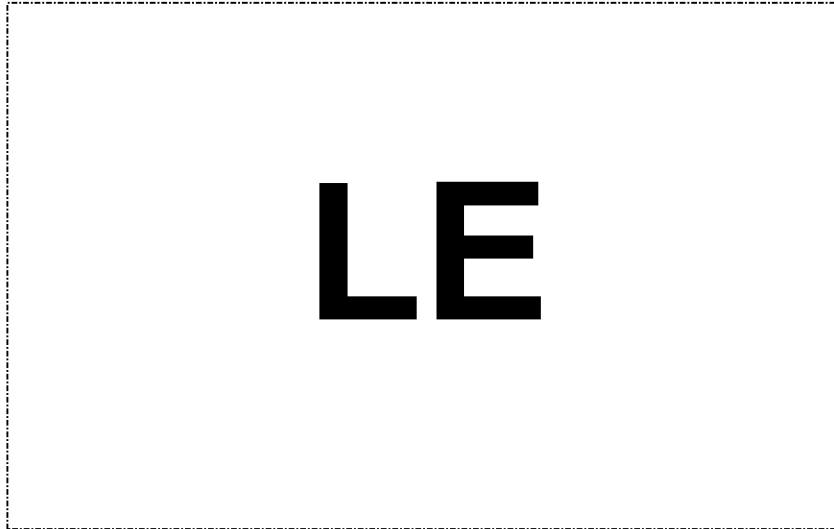
LE

LE

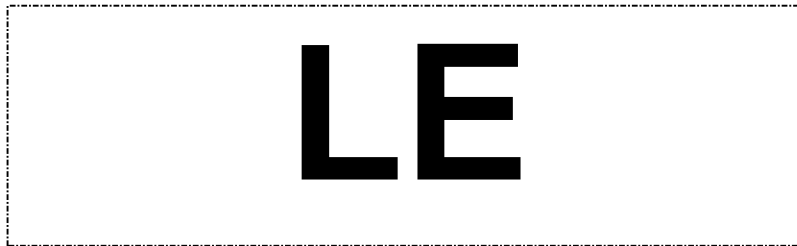
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

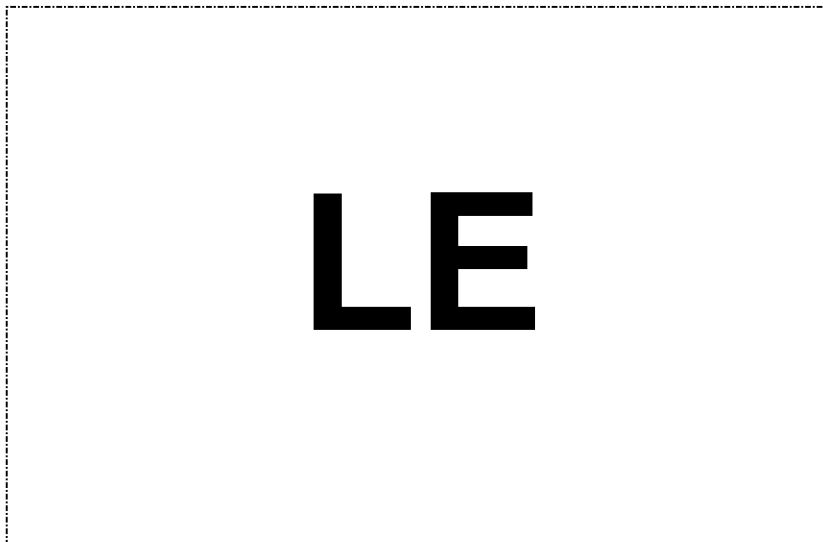
f. Response with Incorrect Date of Birth



g. Response with Incorrect A#



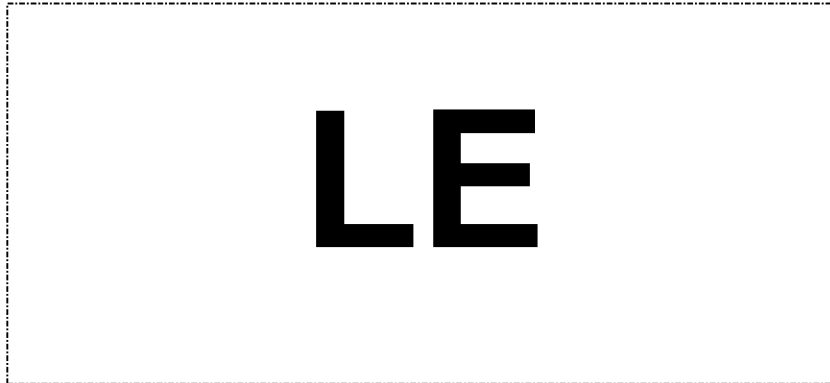
h. Applicant's Place of Birth is Incorrect/Missing



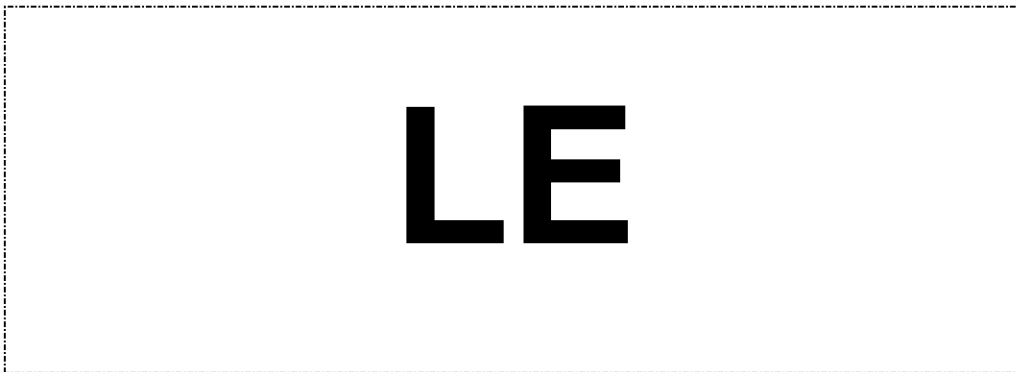
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

i. No Data Is Found When Querying the Name Check Results



FBI Name Check Facts:



**Request Has Been Pending for Months, Should a New Request be Submitted?**

- No. Although some cases seem to take an inordinate amount of time to move from a PENDING response to a final response, submitting a second check will actually delay clearance.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

## C. FBI Fingerprint Check

### 1. Background

- The FBI Fingerprint Check is separate and distinct from the FBI Name Check. The FBI Fingerprint Check provides information relating to the applicant's criminal history primarily within the U.S. The applicant appears in person at a USCIS Application Support Center (ASC) to be fingerprinted. Results are transmitted electronically to the FBI's Criminal Justice Information Services (CJIS) Division, queried in the Integrated Automated Fingerprint Identification Systems (IAFIS) and returned electronically. Non-IDENT, IDENT, Unclassifiable.

Note: FBI Name Check is conducted on a name and year of birth whereas the FBI fingerprint check requires the applicant's biometrics. The applicant is fingerprinted and those prints are run against the FBI fingerprint file records.

The FBI website, <http://www.fbi.gov/hq/cjisd/iafis.htm>, provides the following information:

The Integrated Automated Fingerprint Identification System, more commonly known as IAFIS, is a national fingerprint and criminal history system maintained by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division. The IAFIS provides automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year. As a result of submitting fingerprints electronically, agencies receive electronic responses to criminal ten-print fingerprint submissions within two hours and within 24 hours for civil fingerprint submissions. USCIS submissions for applications are civil fingerprint submissions.

The IAFIS maintains the largest biometric database in the world, containing the fingerprints and corresponding criminal history information for more than 47 million subjects in the Criminal Master File. The fingerprints and corresponding criminal history information are submitted voluntarily by state, local, and federal law enforcement agencies.

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

## 2. Applications/Petitions Requiring FBI Fingerprint Check

Generally, applicants age 14 and over must be fingerprinted (upper age limits depend on the application/petition) when applying for the following benefits:

- a. Asylum/Refugee/NACARA
- b. Temporary and Permanent residency
- c. Family Unity/Temporary Protected Status
- d. Application for Replacement Permanent Resident Card
- e. Certain Waivers
- f. Naturalization
- g. Petitions for Removal of Conditional Residency
- h. Adoption (U.S. citizen petitioners/household members age 18+)

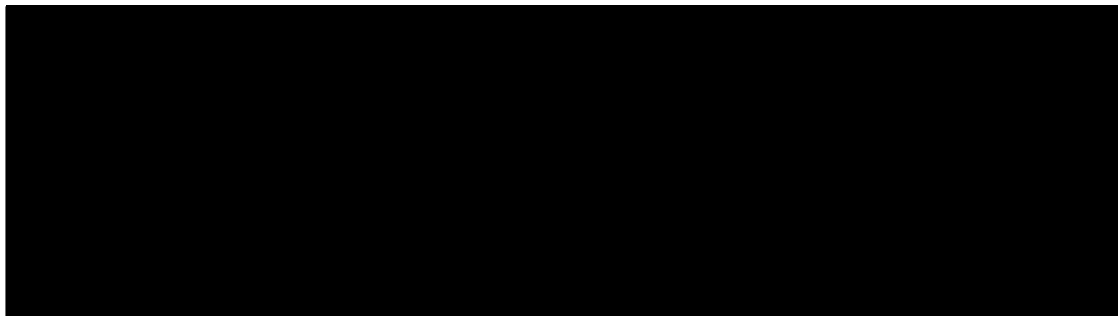
Officers must ensure that the fingerprint results for the petitioner or beneficiary are valid for each petition or application requiring those results.

## 2. Validity of FBI Fingerprint Check

- a. Must be less than fifteen (15) months old at the time of adjudication

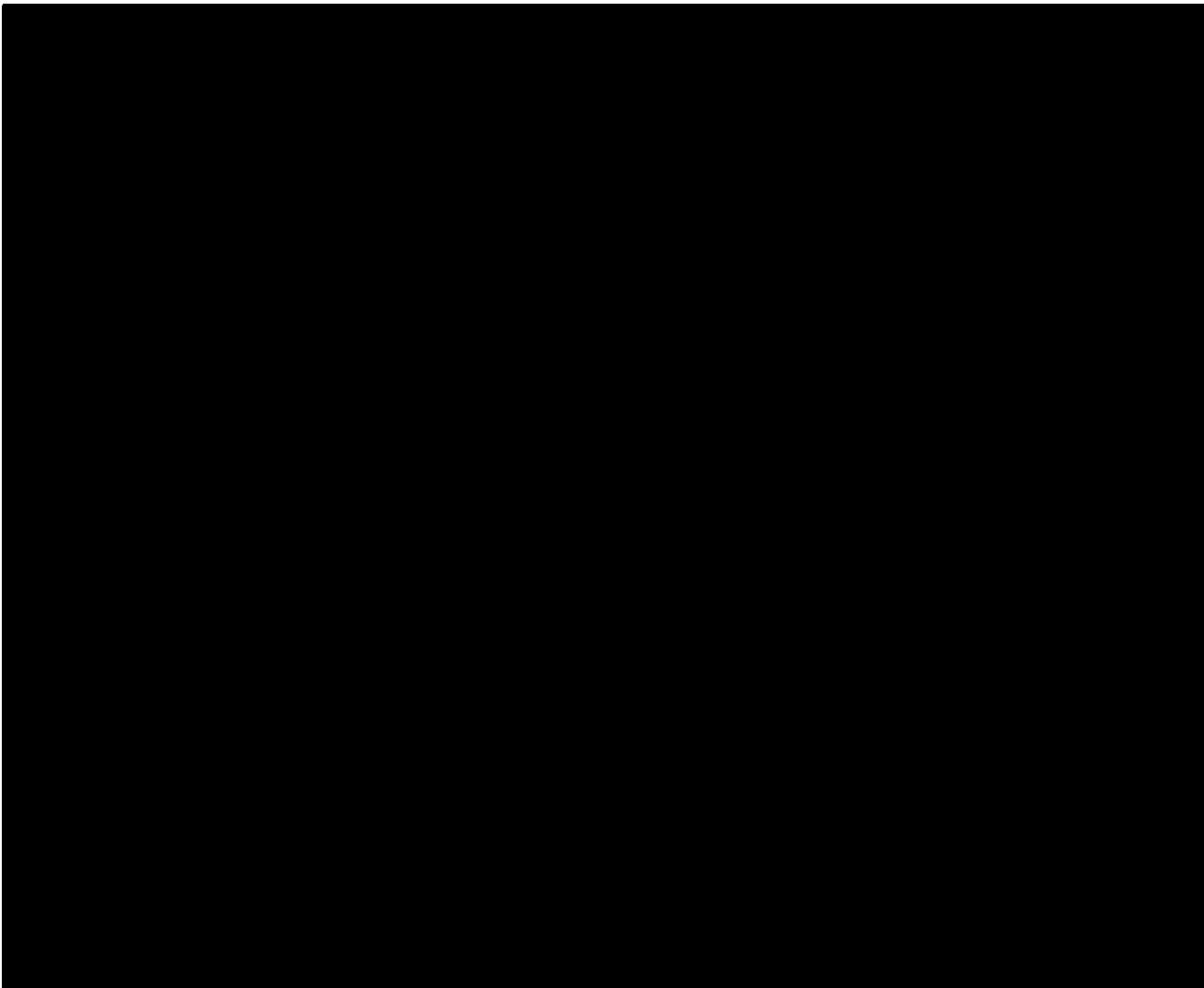
Note: No definitive list of applications/petitions that require fingerprints have been identified. If students are unsure whether fingerprints are required on an application/petition, they should consult their supervisors and/or SOP for the processing requirements of that specific application. Many of the requirements are found online or in the instructions of the application/petition at [www.uscis.gov](http://www.uscis.gov).

## 3. Results of FBI Fingerprint Check



### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



**D. TECS/Interagency Border Inspection System (IBIS)**

Ultimately, it is the adjudicator's responsibility to ensure that prior to final adjudication, the IBIS result is not expired and any hits have been resolved.

Inter-Agency  
Border Inspection  
System Standard  
Operating  
Procedures (IBIS  
SOP) dated March  
1, 2006.

1. Background

TECS, previously known as Treasury Enforcement Communications System, is an automated enforcement and inspection lookout system that USCIS personnel use to conduct manual IBIS queries. This system is maintained by U.S. Customs and Border Protection (CBP).

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

IBIS improves border enforcement and facilitates inspections of applicants for admission into the United States. It strengthens border security by identifying threats to national security and/or public safety, and other law enforcement violations as well as integrates computer resources to assist inspections, investigations, adjudications, law enforcement, and intelligence agencies.

IBIS combines information from many federal agencies into the TECS database and interfaces with other sources such as the NCIC.

In December of 1999, the Deputy Commissioner of Immigration and Naturalization Services (INS) directed the Adjudications Division to prepare a plan to conduct electronic lookout checks on applicants for immigration benefits, in particular those aliens seeking adjustment of status.

On August 21, 2001, Michael A. Pearson, Executive Associate Commissioner, Office of Field Operations, of INS signed a memo directing the adjudication division of INS to complete IBIS checks on all I-485s, I-90s, I-821s, and on I-765s filed by asylum seekers.

On November 13, 2002, Johnny N. Williams, Executive Associate Commissioner, Office of Field Operations, signed a memo concerning the responsibilities of adjudicators. Along with this memo was the first National IBIS Standard Operating Procedure (SOP). The IBIS SOP is a living document and is revised as USCIS policies and procedures are changed.

- USCIS conducts IBIS checks on every applicant, petitioner and beneficiary and in certain cases on businesses.
- USCIS conducts 33-35 million IBIS name checks per year & receives approximately 10,000 hits of a national security nature.
- Approximately 1,500 are Known or Suspected Terrorists (KSTs).

Note: USCIS personnel use the terms TECS and IBIS interchangeably.

## 2. National Crime Information Center (NCIC)

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- a. Database maintained by the Federal Bureau of Investigation (FBI).

LE

See page 13 of the IBIS SOP dated March 1, 2006, for a list of who to query by application and petition.

- c. USCIS personnel (e.g. FDNS officers and BCU staff) also have access to NCIC Interstate Identification Index (NCIC III). Authorized USCIS personnel are permitted only to query NCIC III when fraud is articulated, a national security concern has been identified, or there is an indication of a criminal record or criminal activity.

### 3. IBIS Usage

- a. “For Official Use Only (FOUO)”
- b. Must be marked accordingly
- c. Access is granted on a need-to-know basis for official use only.
- d. All IBIS users must be certified through an on-line security certification test and must be re-certified every two years.

**\*\*\*Abuse or misuse of IBIS could result in loss of access, termination of employment, and/or criminal prosecution.\*\*\***

### 4. Applications/Petitions Requiring TECS/IBIS

- a. Must be run on the following subjects age 14 and over:

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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



I-290B, and EOIR-29 cases only.)

**LE**

- b. Not only conducted on the applicant and beneficiary but also on the petitioner (individual, business, organization):
- i. Employment based petitions
  - ii. Religious worker petitions
  - iii. To deny immigration benefits to ineligible petitioners in accordance with the Adam Walsh Act

Note: IBIS queries are not required for the following:

Subjects under the age of 14

Employment-based petitioners that are business entities. Sole proprietorships are considered business entities and do not need to be queried. Individual persons are not considered business entities and must be queried.

Subjects who are deceased

**EXCEPTION:** Query IBIS on decedents on Forms N-644, Application for Posthumous Citizenship.

For businesses, it is not required but at the discretion of the officer an SQ16 query may be conducted. However, in accordance with USCIS memorandum dated 7/5/2006 entitled "Standard Operating Procedures for Religious Worker Petition Anti-Fraud Enhancements" there are certain requirements to query religious organizations petitioning for individuals on the I-360 or I-129.

## 5. Results from TECS/IBIS

- a. Immigration Services Officers primarily use the subject and business query in TECS.

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- b. TECS provides information relating to open and closed investigations, intelligence reports, wants and warrants, etc.
  - c. Results identify concerns such as: criminal, immigration violations, public safety, and national security
  - d. Queries available at discretion of local office, if not required
6. Validity of TECS/IBIS Checks
- a. Must be run on all new applications/petitions within 15 calendar days of initial receipt
  - b. For applications/petitions filed at a service center or a lockbox, this process is run automatically through a process called Batch Processing
  - c. The IBIS query must be valid at the time of final adjudication
  - d. The IBIS query is valid for 180 CALENDAR days. At the time of adjudication if the validity has expired, a manual IBIS query must be completed

Note: Discuss the results that can be obtained from more commonly used Subject Queries (SQ).

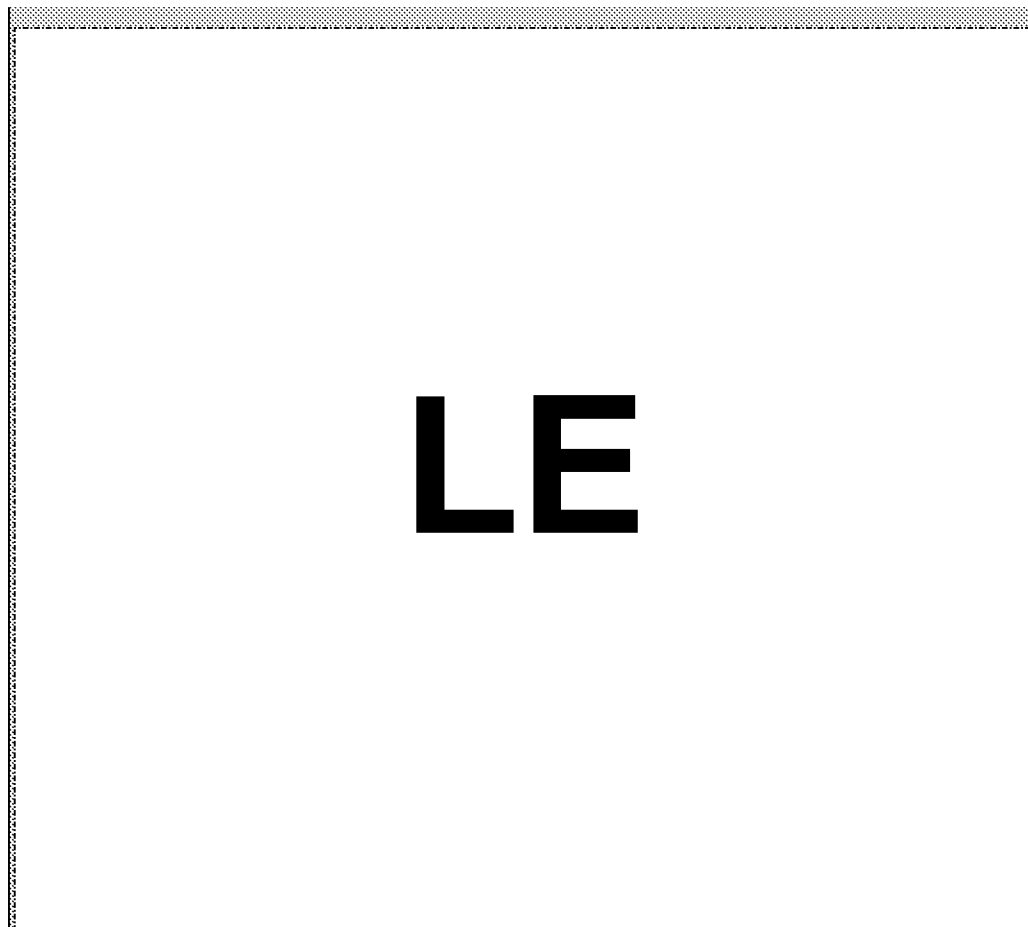
IBIS SOP requires **LE** be performed and details when those queries must be performed. Students will review IBIS SOP will be at NBC. The other SQ queries are not required but may provide information beneficial in the adjudication process. These queries are used regularly by FDNS Immigration Officers and BCU staff.

For example:

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



- i.
  - ii.
  - iii.
  - iv.
- 
- A rectangular area with a dotted border, containing the letters 'LE' in a large, bold, black font centered within the space.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

v.	
vi.	
vii.	<b>LE</b>
viii.	
ix.	
x.	

See USCIS Memorandum entitled “*Accessing National Crime Information Center Interstate Identification Index (NCIC III) Data*” dated June 3, 2005.

DHS Management Directive 11042.1 describes numerous additional caveats (e.g. “Law Enforcement Sensitive”) used by agencies to identify unclassified information as “Sensitive but

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Unclassified (For  
Official Use  
Only).”

#### **E. United States-Visitor and Immigrant Status Indicator Technology (US-VISIT)/Automated Biometrics Identification System (IDENT).**

- Used primarily by Asylum Branch
- Used by DOS, CBP, ICE
- Loads biographical and biometric information
  - Two Prints vs Ten Prints
- US-VISIT watchlist
  - Not same as Terrorist Watchlist

#### **F. Third Agency Rule**

1. The contents of an originating agency's report in possession of USCIS shall not be disclosed to another agency without the prior consent of the originating agency.
2. Third agency information includes but is not limited to information resulting from security checks such as information provided by FBI, DOS, U.S. Marshals Service (USMS), Drug Enforcement Administration (DEA) and information from TECS/IBIS.

#### **G. DHS Components**

- a. All DHS components are considered one agency.
- b. Information from these components is oftentimes “Law Enforcement Sensitive” (e.g. TECS/IBIS hit information) and must be protected regardless.
- c. Component information shall not be disclosed to another agency without the permission of the owning component.
- d. Includes but not limited to Immigration and Customs Enforcement (ICE), CBP, the U.S. Secret Service.

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

#### **DHS Policy for Internal Information Exchange and Sharing (2/1/07)**

- All DHS components are considered to be part of one "agency" for purposes of the Privacy Act, 5 U.S.C. § 552a(a)(1), (b)(1).

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- No DHS component should consider another DHS component to be a separate agency for information-sharing purposes.
- Absent any legal prohibitions as set forth by the Department's Office of 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, possesses the requisite security clearance, if one is needed, and assures adequate safeguarding and protection of the information.
- 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.

**Note:** When in doubt on whether the information may be released to the applicant, petitioner, or their representative, students should seek guidance from their supervisors and local USCIS attorney on how to "use" information without disclosing it as well as the proper steps for obtaining consent from the originating agency/component, if USCIS would like to disclose the third agency information.

## H. USCIS Fact Sheet on Immigration Security Checks

1. Created for distribution to the public to explain the importance and necessity of the security checks as well as possible reasons for delay in the security check process.
2. The fact sheet provides the following information:
  - a. Security checks are performed on every applicant regardless of ethnicity, national origin or religion;
  - b. Security checks enhance national security and ensure the integrity of the immigration process;
  - c. The fact sheet explains the FBI Name Check, FBI Fingerprint Check, and IBIS.

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)

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**EPO #5: Discuss the term “national security concern” and methods used to identify cases involving 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.

- May be identified at any stage of the adjudication process
- “Guidance for Identifying National Security Concerns” (Attachment A of CARRP Policy)
  1. Articulable Link determined by designated officer
    - 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

Note: Students should become very familiar with the reference tool “Guidance for Identifying National Security Concern”. This document is Attachment A to the Domestic Ops Guidance and is the focus of this EPO. It is also found in the other CARRP guidance for the different components within RAIO.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Identifying a NS concern is a three prong test

Are there NS indicators? Yes

Do they relate to the individual? Yes

Is there an articulable link to NS activity? Yes

If you answer yes to all, then there is an NS concern. If you answer no to any of the three then there is not a NS concern.

Once an NS indicator is identified, the designated officer will determine if an articulable link exists.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



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

Note: Prior to 9/11, there were at least 12 different watch lists. After 9/11, President Bush signed the Homeland Security Presidential Directive (HSPD-6) which consolidates these lists into one terrorist watch list.

The National Counterterrorism Center (NCTC), which is a multi-agency organization, was created to analyze all intelligence pertaining to terrorism and counterterrorism. The NCTC receives nominations for the watch list from many different government agencies (FBI, CIA, DOD) and foreign governments (Canada, Australia). The information is reviewed by NCTC and put in a classified database known as Terrorist Identities Datamart Environment (TIDE). If NCTC has enough information pertaining to an individual and that individual meets the criteria to be watch listed, NCTC forwards that information to the Terrorist Screening Center (TSC).

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

The TSC has been operational and running 24/7 since December 2003. **LE**

**LE****LE****LE****LE****LE**

**According to CARRP, designated officers will contact the TSC. The TSC should not be contacted unless there is a KST hit:** **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**LE**

The below information comes from the following website address on the FBI's website as of 3/31/08:

[www.fbi.gov/page2/august07/tsc083107.htm](http://www.fbi.gov/page2/august07/tsc083107.htm)

"Two days before the attacks on the World Trade Center and the Pentagon in 2001, a Maryland State Trooper stopped Ziad Jarrah for speeding near the Delaware state line. The trooper checked Jarrah's license and registration against a database of "wants and warrants," and it came back clean. The trooper later called the stop routine. He had no way of knowing that Jarrah was on a CIA watch list and that he was central to an unfolding plot to attack the U.S.

Fast forward to today: if Jarrah was stopped for speeding, a query of his information in the FBI's National Crime Information Center (NCIC) would automatically check him against a master list of known or appropriately suspected terrorists. The presence of Jarrah's name would raise a flag, and the trooper would be prompted to call the Terrorist Screening Center (TSC), where analysts would run more extensive checks to see if the Jarrah at the traffic stop is the same one of interest to the intelligence community. The screening center might guide the trooper through some questions to ask Jarrah or contact its operational unit to coordinate a response, such as dispatching agents from the Joint Terrorism Task Force to the scene."

**LE**

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

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

## 2. Terrorist Identities Datamart Environment (TIDE)

<http://www.whitehouse.gov/news/releases/2003/09/20030916-5.html>

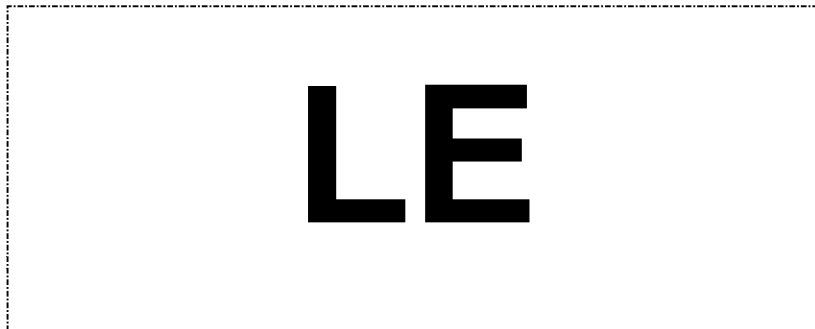
- a. U.S. Government's central repository of information on international terrorist identities.
- b. Supports the U.S. Government's various terrorist screening systems or "watch list" and the U.S. Intelligence Community's overall counterterrorism mission.
- c. Includes, to the extent permitted by law, all information the U.S. government possesses related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of Purely Domestic Terrorism information.
- 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. Known or Suspected Terrorist (KST) Hit:

- Has been nominated and accepted for placement in the Terrorist Screening Database (TSDB)
- Remains on the Terrorist Watch List until a nomination for removal has been approved

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

## a. TECS/IBIS:



**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**LE**

- CLASS
  - DOS results from overseas processing/Refugees

Note: USCIS identified Known or Suspected Terrorists (KST) hits primarily via TECS/IBIS and NCIC. These individuals are on the Terrorist Watch list and identified by **LE**

The can also be identified through National Crime Information Center (NCIC) Lookouts:

- Identified by **LE**
- Indicates the subject is a "Possible Terrorist Organization Member" or an "International Extremist" and request contact with the TSC.

**LE**

Consular Lookout Automated Support System (CLASS)

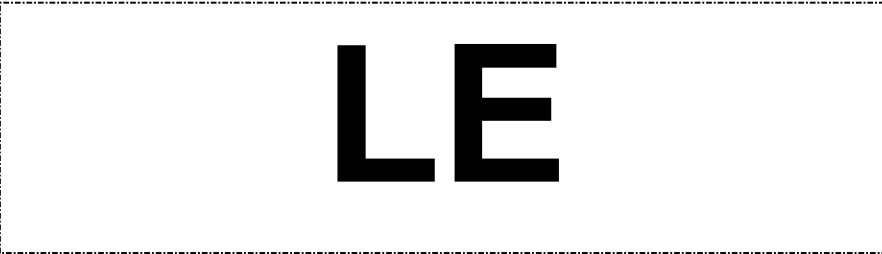
- CLASS may indicate that the subject is on the Terrorist Watch List. Information from CLASS is used by State Department Officials as well as USCIS Officers overseas.

#### 4. Terrorist Screening Center (TSC)

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- a. Operational and running 24/7 since December 2003.
- b. Designated Officers contact the Terrorist Screening Center to confirm whether a KST lookout is a match to a USCIS subject.

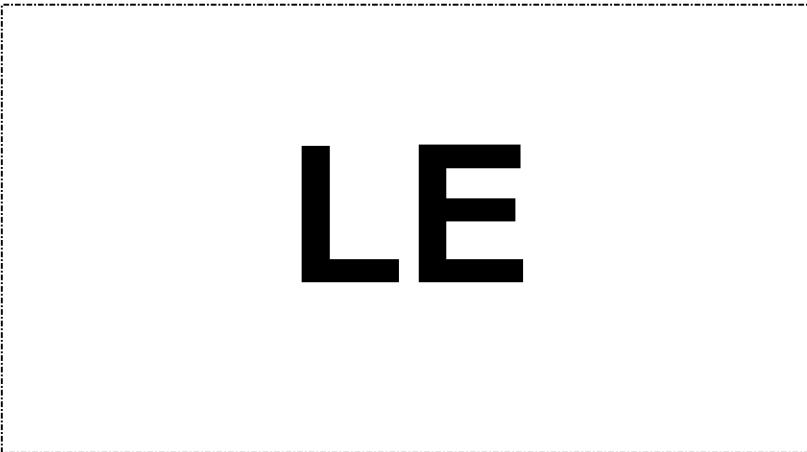
c. 

e. Do **NOT** contact Richard Kopel, Deputy Director at the TSC.

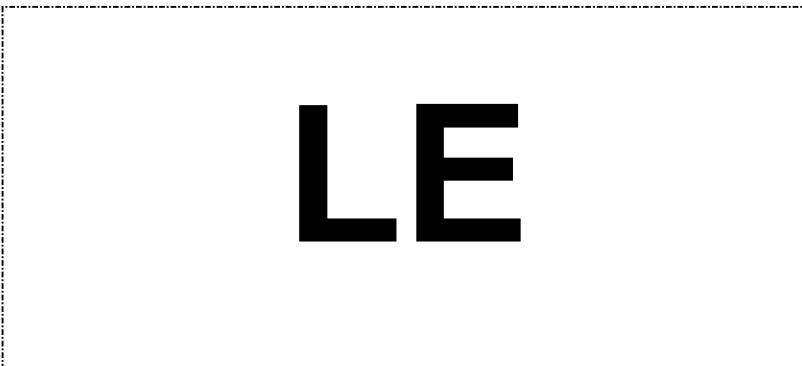
f. TSC **does not** give adjudicative advice,

g. TSC Contact: 866-872-

h. TSC personnel confirm the match

i. 

**What will TSC need to confirm the match?**

m. 

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Non-KST NS Concerns

All of the remaining NS concerns

- Associates of KST(s),
- Unindicted co-conspirators,
- Persons involved with providing material support to terrorists or terrorist organizations,
- Agents of foreign governments

**Non-KST ≠ Not Dangerous**

**KST + Non-KST = Terrorist Cell**

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**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:

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

**LE**

- 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.
- “Guidance for Identifying National Security Concerns”
- Use as a Reference Tool
- Also known as Attachment A

**Statutory Indicators**

- 212(a)(3)(A), (B), or (F)
- 237(a)(4)(A) or (B)
- Other

**Non-Statutory Indicators**

- Employment, Training, Government Affiliations
- Other Suspicious Activities
- Family Members or Close Associates

**Security Check Results****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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

\*\*\*\*Officers must look at the whole picture and consider the facts of each individual case.\*\*\*\*\*

Note: Non-KSTs are the population that will be primarily encountered via security checks and through other sources.

**LE**

KST + non-KST = Terrorist cell means a KST needs support to accomplish his/her ultimate goal of a terrorist act. And it is the Non-KSTs that are assisting him/her accomplish the goal.

Non-KSTs also include those who are involved in foreign intelligence activities and sabotage.

Remember Non-KST does not mean not dangerous.

## 1. Statutory Indicators

Sections found in the Immigration and Nationality Act (INA)

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

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



## Counterintelligence vs. Foreign Intelligence

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

Definitions for Foreign Intelligence and Counterintelligence found at:

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

<http://www.dod.mil>

Note: 212(a)(3)(A) covers espionage, sabotage, and illegal transfer of goods, sensitive information outside of the U.S.

Espionage includes but is not limited to activities of foreign powers and their agents that adversely affect national security such as obtaining inside information on our government's policies and intentions towards other countries; details on U.S. military plans and weapons systems; or our nation's scientific and technological innovations and research, both public and private. Being an unregistered foreign agent is sufficient for this ground even without doing anything directly contrary to the U.S. Government

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

Note:

While the terrorist activity grounds of inadmissibility at 212(a)(3)(B) are identical to the deportability grounds at 237(a)(4)(B), there is a difference with the "in general" grounds (which includes espionage and unlawful exportation of goods and sensitive information). The inadmissibility ground at 212(a)(3)(A) applies to current and future activities while the deportability

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

ground at 237(a)(4)(A) refers to past activities. Though when speaking about Non-KST NS concerns we are focusing not on the statute but the activity, individual or organization listed in the statute.

USCIS Officers should understand the scope of the following terms defined in section 212(a)(3)(B) of the INA: "Terrorist Activity", "Engage in Terrorist Activity", and "Representative".

Interesting to note that the words "terrorist" and "terrorism" as nouns are not found in "3B" of the INA. Congress intended for the term "terrorist activity" to be very broad. With the enactment of the USA PATRIOT Act (enacted 10/26/2001) and the REAL ID Act (enacted 5/11/2005), the definitions relating to "terrorist activity", "engaging in terrorist activity", and "terrorist organization" became even broader. "3B" of the INA covers more conduct than over 20 other federal legal definitions.

A summary of key changes that were implemented as a result of the REAL ID Act by USCIS Attorney, Nick Perry, can be found in the students' reference material:

- Expanded the inadmissibility ground to include representatives of both designated and undesignated terrorist organizations. Previously, only representatives who were members of a Foreign Terrorist Organization (designated by DOS under section 219 of the INA) and those of "a political, social, or other similar group whose public endorsement of acts of terrorist activity the Sec of State determined undermines the US effort to reduce or eliminate terrorist activities" were inadmissible.
- An alien who endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization is inadmissible. Previously it was limited to aliens who have a position of prominence in any country to endorse/espouse terrorism and the Secretary of State had to determine that it undermines the US effort to reduce or eliminate terrorist activities.
- A new ground of inadmissibility was added which reads, an alien who "has received military type-training from or on behalf of any organization that at the time the training was received was a terrorist organization". This includes both designated and undesignated terrorist organizations.

## Other Sections of the INA:

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

208(b)(2)(A)	Ineligibility for Asylum
219	Designation of Foreign Terrorist Organizations
235 (c)	Removal of Aliens Inadmissible
236A	Mandatory Detention of Suspected Terrorists
237(a)(2)(D)	Grounds of Deportability –Misc. Crimes
212(a)(2)(l)	Inadmissible Aliens – Money Laundering
221(i)	Issuance of visas- Revocation of visas/other docs

i. Terrorist Activity Defined

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:

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

- 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 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.
- 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

Internationally  
protected person as

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

---

**Participant Guide**

individuals or to cause substantial damage to property.

defined in section 1116(b)(4) of title 18, United States Code

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

ii. Engage in Terrorist Activity Defined

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 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 as described in INA 212(a)(3)(B)(vi)(I) & (II) (Tier I or II terrorist organization); or an undesignated terrorist organization as defined at INA 212(a)(3)(B)(vi)(III) (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;
- F. To commit an act that the actor knows, or reasonably should know, affords material support, including a safe house, transportation,

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

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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

Note: Food, housing, and money (war tax, ransom, extortion, donations) would also be considered material support.

The material support provision applies: 1) when the individual afforded material support for the commission of a "terrorist activity;" 2) when an individual has committed or plans to commit a terrorist activity; or 3) to a "terrorist organization", even if the individual was forced to provide the material support.

When handling material support claims and Tier III undesignated terrorist organizations, officers should refer to the USCIS Policy memorandum 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"

### iii. Inadmissibility for Terrorist 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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 at INA 212(a)(3)(B)(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;
- 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
- I. is the spouse or child of an alien who is inadmissible under this subparagraph, if the activity causing the alien

INA 212(a)(3)(B)

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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 with 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:

Abu Sayyaf  
 Al-Qa'ida  
 Basque Fatherland and Liberty (ETA)  
 Continuity Irish Republican Army  
 HAMAS  
 Hezbollah  
 Jemaah Islamiya Organization  
 Mujahedin-e Khalq Organization  
 Palestine Islamic Jihad  
 Revolutionary Armed Forces Colombia (FARC)

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

See [www.state.gov](http://www.state.gov) for full listing:.

B. Tier II – Terrorist Exclusion List (TEL)

1. An organization otherwise designated, upon

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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. There are over 60 designated organizations and companies:

Asbat al-Ansar  
 Babbar Khalsa International  
 Japanese Red Army  
 Lashkar-e-Tayyiba (Army of the Righteous)  
 Eastern Turkistan Islamic Movement  
 Libyan Islamic Fighting Group  
 Revolutionary United Front

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

See [www.state.gov](http://www.state.gov) for full listing.

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

### 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.
3. For handling of individuals involved in or having supported Tier III organizations, see
  - USCIS Memorandum 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”*

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



**No Official List**

Note: The definitions of “engaging in terrorist activity” and “terrorist activity” contained in the INA, include illegal use of explosives, firearms or other weapons (other than for mere personal monetary gain), with intent to endanger the safety of individuals or to cause substantial damage to property and under circumstances indicating an intention to cause death or serious bodily injury. This broad definition would include most armed resistance groups as Tier III terrorist organizations.

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

**Executive Order 13224  
Terrorist Financing List**

On September 23, 2001, the President issued Executive Order 13224, which provides the means to disrupt terrorist support networks. Under this order, the US Government may block the assets of individuals and entities providing support—financial and otherwise—to designated terrorists and terrorist organizations. This authority has been used on numerous occasions to target individuals actively engaging in terrorist-related activities, including providing false documentation to illegal aliens to facilitate travel.

- 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)
- h. Mandatory detention of suspected terrorists; habeas corpus;  
judicial review  
236A

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/enforce>

Deportable Aliens – Miscellaneous crimes

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

237(a)(2)(D)

ment/ofac/

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

## 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.

Note: General NS indicators may be equated to general fraud indicators. In short, they are red flags. Just because there are fraud indicators does not mean that fraud is being committed. In the same manner, just because there are NS indicators, does not mean the applicant or petitioner is a terrorist or spy. But when fraud or NS indicators are present, the totality of the circumstances of the case should be considered to determine whether the facts and indicators rise to the level of a national security concern. Further exploration of the case may be required such as running additional systems checks or establishing a more thorough line of questioning for the interview.

When reviewing security check results, testimony and documents provided in support of a benefit, and/or any other source material, 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Services Officer should consider:

This information is oftentimes obtained during the interview or in the application/petition. **LE**

**LE**

Criminal Activity--different types of criminal activity such as money laundering, manufacturing fake documents, and human trafficking or smuggling are activities that may be used to fund terrorist activities/organizations. Criminal activities like these fall into the category of material support if assisting a designated or undesignated terrorist organization.

Intelligence gathering--was the person encountered by law enforcement or was there a lead sent in on the individual because he/she was gathering intelligence. **LE**

**LE**

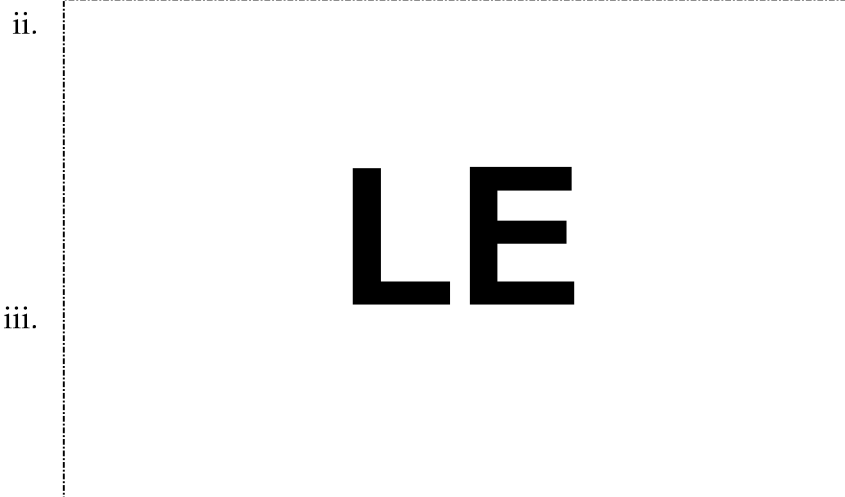
BREAKING NEWS

**LE**

- a. Employment, Training, or Government Affiliations
  - i. Certain types of employment, training, government affiliation, and/or behavior may (or may not) be indicators of a NS concern, depending on the circumstances of the case, and require additional scrutiny to determine whether a NS concern exists.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



i. State Sponsors of Terrorism

Countries whose governments the Department of State has determined have repeatedly provided support for acts of international terrorism are designated as state sponsors of terrorism under provisions in the Foreign Assistance Act, Arms Export Control Act, and Export Administration Act.

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

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

**Note:** State Sponsors are countries determined by the Secretary of State to have repeatedly provided support for acts of international terrorism and are designated pursuant to three laws: section 6(j) of the Export Administration Act, section 40 of the Arms Export Control Act, and section 620A of the Foreign Assistance Act.

Sanctions taken against these countries include but are not limited to restrictions on U.S. foreign assistance, a ban on defense exports and sales, certain controls over exports of dual use items, and miscellaneous financial and other restrictions.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Iran is known to financially back terrorist organizations such as Hezbollah, HAMAS, and the Palestinian Islamic Jihad (PIJ).

Libya was removed from the list.

The below excerpt was retrieved from

<http://www.state.gov/r/pa/prs/ps/2006/66244.htm> on April 14, 2008.

Countries whose governments the U.S. has determined have repeatedly provided support for acts of international terrorism are designated as state sponsors of terrorism under provisions in the Foreign Assistance Act, Arms Export Control Act, and Export Administration Act. The Secretary of State can rescind Libya's designation as a state sponsor, if the President submits a report to Congress at least 45 days before the proposed rescission. The report needs to justify the rescission and certify that the government of Libya has not provided any support for international terrorism during the last six months and has provided assurances that it will not support future acts of international terrorism. After careful review, the President submitted a report on Libya to Congress on May 15, 2006. In conjunction, Secretary of State Condoleezza Rice announced her intention to rescind Libya's designation as a state sponsor of terrorism after the 45-day period expires. Libya was designated a state sponsor of terrorism in 1979. Relations deteriorated further during the 1980s, particularly in the aftermath of Libya's role in the destruction of Pan Am flight 103 over Lockerbie, Scotland in December 1988, killing 270 people. In 1999, Libya began seriously to address our terrorism concerns and began the process of fully meeting the requirements to distance itself from terrorism by transferring the suspects in the Pan Am 103 case for trial by a Scottish court sitting in the Netherlands. Beginning in 2001, the United States and the United Kingdom initiated three-way direct talks with Libyan representatives to secure Libya's compliance with the remaining international terrorism requirements. Based upon these discussions, on August 15, 2003, Libya sent a letter to the United Nations Security Council confirming its commitment "not to engage in, attempt, or participate in any way whatever in the organization, financing or commission of terrorist acts or to incite the commission of terrorist acts or support them directly or indirectly" and to "cooperate in the international fight against terrorism." Libya also accepted responsibility for the actions of its officials in the Pan Am 103 incident, agreeing to pay over \$2 billion in compensation to the families of the victims of Pan Am 103 and pledged to cooperate in the investigation. On December 19, 2003, after intense discussions with the United States and the United Kingdom, Libya announced its decision to abandon its programs to develop weapons of mass destruction (WMD) and MTCR Category I missile delivery systems. President Bush responded that the United States would reciprocate Libya'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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

good faith in implementing this change of policy. At the same time, Libya moved forward in implementing its pledge to cooperate in the fight against international terrorism. Since September 11, 2001, Libya has provided excellent cooperation to the United States and other members of the international community in response to the new global threats we face. Based on this cooperation, Secretary Rice also announced on May 15, 2006, that, for the first time, Libya will not be certified this year as a country not cooperating fully with U.S. antiterrorism efforts. The United States has responded to Libya's actions through a careful step-by-step process designed to acknowledge Libya's progress, but still allow review at each stage. Libya has responded in good faith not only in the area of international terrorism but also in the related field of weapons of mass destruction. Libya is an important model to point to as we press for changes in policy by other countries (such as Iran, North Korea, and others), changes that are vital to U.S. national security interests and to international peace and security.

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:

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**LE**

**LE**

c. Suspicious Financial Activities

Evidence of certain financial activities may also require additional scrutiny to determine if there is a link to a national security concern.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**LE**

d. Hawala

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**LE**

**LE**

3. Security Check Indicators.

a. FBI Name Check

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



i. Indicators

LHM may likely involve a NS concern if the individual is the main or referenced subject in one or more of the following types of investigations or if the LHM includes language that suggests an investigation of a similar nature:



In some instances, a LHM may indicate that upon completion and closure of the FBI investigation, the FBI case agent made a definitive finding of no nexus to national security in relation to the USCIS applicant. If the LHM indicates a definitive finding of no nexus to national security to the USCIS applicant, and no other indicators of a national security concern are present (e.g. resulting from a thorough review of the security checks and file), the case would not be considered to have a national security concern.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

## b. FBI Fingerprint Check

## i. Indicators

- A. Classified by the Attorney General as a known terrorist;
- B. Charged in immigration court with an inadmissibility/removability ground in sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Act;
- C. Arrested/detained by the U.S. military overseas (e.g., detainees in Iraq or Guantanamo);

D.



Note: Officers will not often encounter information on the Rap sheet that indicates a national security concern.

The following slide is an example of the FBI RAP sheet with the NS indicator for a Guantanamo detainee. It has been redacted for identifiable information.

Furthermore, officers will not often deny based on inadmissibilities relating to the security grounds (other than material support related). Officers should remember that lodging a Notice To Appear (NTA) charges on security – related grounds requires ICE-Office of Principal Legal Advisor (OPLA) approval.

Due to the breadth of activities that fall under “Terrorist Activity” as defined in the INA some explosives, firearms or weapons charges may be considered terrorist activity. The definition clearly states that “terrorist activity” in relation to use of explosives, firearms, or other weapons or danger devices must be **for other than mere personal monetary gain AND** with intent to endanger, directly or indirectly, the safety of one or more individuals or to

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

cause substantial damage to property.

c. TECS/IBIS

LE

A.

B.

LE

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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

LE

D.

LE

1.

2.

LE

E. Evaluate for articulable link:

1.

2.

3.

4.

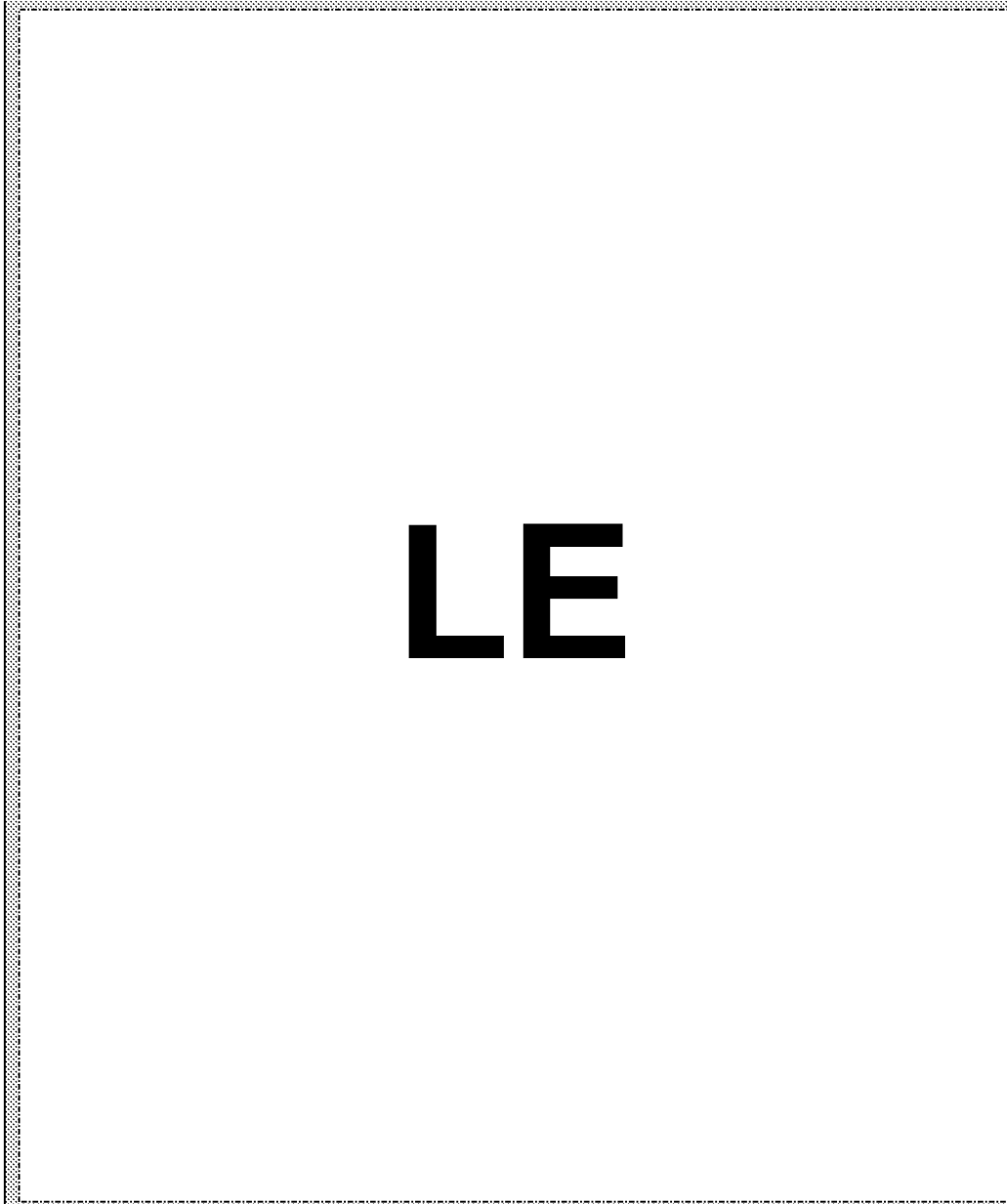
LE

Note:

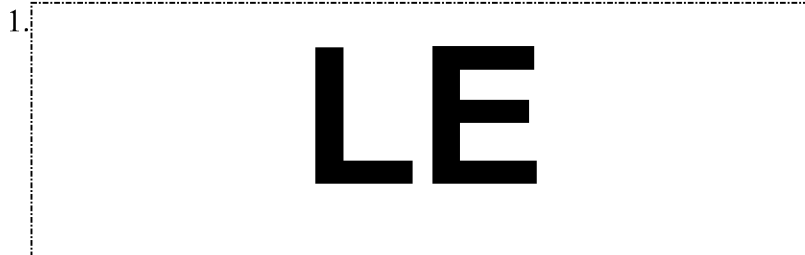
LE

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



F. CBP's National Targeting Center (NTC)



**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



LE

Note: NTC enters different types of lookouts. When lookouts require contact with the NTC, the officer will first determine if it [REDACTED] LE if so, TSC must be notified. If it is [REDACTED] LE, the officer will follow the above instructions regarding [REDACTED] LE [REDACTED] LE which will be discussed later.

See IBIS SOP dated March 1, 2006.

d. INTERPOL

- i. INTERPOL is the International Criminal Police Organization
- ii. Created in 1923
- iii. 187 Member countries
- iv. Each country has a National Central Bureau (NCB) staffed by national law enforcement officers.
- v. Facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.
- vi. INTERPOL does not give adjudicative assistance.
- vii. Personnel are only deployed in a major crisis.

See IBIS SOP.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Note: You might come across INTERPOL Lookouts in TECS/IBIS – the slides in this section provide a brief overview of INTERPOL. It is important to understand that INTERPOL is not a regular police force and will not deploy personnel to make an arrest. Their role is to confirm if the lookout is a match to our subject and verify the validity of the notice.

INTERPOL is the world's largest international police organization, with 187 member countries. Created in 1923, it facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.

INTERPOL aims to facilitate international police co-operation even where diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. INTERPOL's constitution prohibits 'any intervention or activities of a political, military, religious or racial character.'

INTERPOL (whose correct full name is "The International Criminal Police Organization – INTERPOL") comprises the following:

- General Assembly
- Executive Committee
- General Secretariat
- National Central Bureaus
- Advisers
- The Commission for the Control of INTERPOL's Files

Although you are unlikely to contact INTERPOL, as this will be done by a Designated Officer or FDNS Immigration Officer.

**LE**

See Attachment A, "Guidelines for Identifying National Security Concerns"

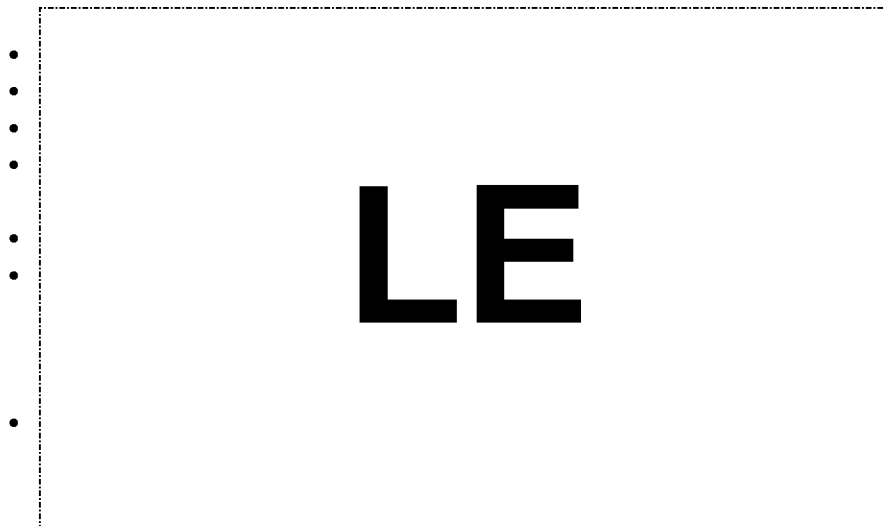
- When assistance is needed from INTERPOL, please email Officer Monda Lambert at [REDACTED] and provide the following information.

:

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



- It is not necessary to call INTERPOL unless subject is present or if there is an emergency.

e. US-VISIT/IDENT

i. Background

Various government agencies, including DHS Components (USCIS, CBP, and ICE), DOS, the FBI, and the National Ground Intelligence Center (NGIC), load biographical and biometric information into US-VISIT/IDENT.

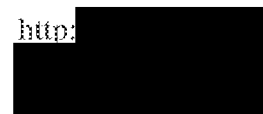
ii. Indicators

US-VISIT/IDENT Watch list includes, but is not limited to, biographic and/or biometric information for KSTs; fingerprints for military detainees held in Afghanistan, Pakistan, and Guantanamo; and individuals inadmissible or removable under sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Act.

f. Results of Security Checks states : Closed Investigations



***Find out Why it was Closed***  
Case was closed administratively



**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

LE



- **Examples of Closed Investigations as found in LHM**

LE



**D. Identifying a NS Concern – Determination**

Prior to making the final determination of National Security Concern – the officer should consider:

- Does the derogatory information relate to the subject?
- The totality of the circumstances (for Non-KST's)
- Does the information in the referral meet the NS concern threshold?

**E. 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.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**EPO #6: Identify the process for eligibility assessment, internal vetting, deconfliction, and external vetting of cases involving national security concerns.**

**A. Deconfliction**

Note: We will watch Deconfliction Video 2 min 30 sec

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.
  - Deconfliction and CARRP Workflow Stages 2 and 3
  - Stage 2: Eligibility Assessment
  - Deconfliction
  - Internal Vetting
  - Stage 3: External Vetting
  - Not required if legally sufficient grounds of ineligibility and decision issued
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 under CARRP
  - a. Primarily FDNS Immigration Officer in the field and asylum offices
  - b. BCU or FDNS staff at Service Center
  - c. Consider including designated Immigration Services Officer on discussions with record owner
5. Ensures that record owner is aware that the individual has a benefit pending with USCIS

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

6. Provides USCIS with opportunity to ask about
  - a. Aliases;
  - b. Family relationships;
  - c. Residence within or outside the U.S.;
  - d. Membership or involvement with organizations;
  - e. Military Training; and
  - f. Foreign Travel
  - g. Criminal activity to include fraud and immigration violations:
7. Provides record owner with opportunity to consider additional information that may initiate further action or investigation of the case.

#### Deconfliction Guidance

8. Request by Law Enforcement Agency for Abeyance or Expedited Processing during Deconfliction -
  - Designated officers in receipt of LEA requests to grant, deny or place in abeyance the issuance of immigration benefits must refer the request to the USCIS chain of command.
  - Request must be in writing, in accordance with the Operational Guidance.
  - Designated officer must prepare a written recommendation to Field Director requesting to place the case in abeyance or for expedited processing.
  - On a case-by-case basis, the Field Director will determine whether the request comports with the requirements for abeyance (8 CFR 103.2(b)(18)) or warrants expedited processing.
9. Case will be held in abeyance for **180 days** or until the investigation is completed, whichever is sooner.

**LE**

\*For more information see: *Additional Guidance on Issues Concerning*

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

*Vetting and Adjudication of Cases Involving NS Concerns* pg. 7-8 and 8 CFR 103.2(b)(8)

## B. 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. Further internal vetting may be required if no grounds of ineligibility are evident or grounds may be easily overcome
5. 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.
6. Designated Officers conduct eligibility assessment and
  - internal vetting on KSTs and non-KSTs
  - Primarily FDNS IOs and BCU vet
  - FDNS IOs do not adjudicate
7. Deconfliction must occur prior to decision

### Eligibility Assessment –

- Is a thorough review of the file, applicant’s history, and system checks results
- May occur at time of interview (e.g. for asylum)
- May occur more than once

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



- If ineligibility grounds are identified – DECONFLICT and ADJUDICATE
- **REMINDER:** Disclosure rules for use and sharing of classified and law enforcement sensitive information apply

Note: This section highlights techniques/best practices that Immigration Services Officers use when handling national security cases and are techniques that can be employed for not only national security cases but for day-to-day adjudications. These techniques will ensure that the Officer conducts a thorough interview and/or review of the application/petition/file to determine eligibility. Use of these techniques will assist in identifying national security or fraud concerns.

**LE**

G-325 Biographical Form: Officers often overlook the G-325 but should make it a conscious effort to review the G-325 for accuracy, completeness, and consistency. The G-325 asks for residential and employment history for the last five years.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

LE

1. Look at the whole picture and from different angles. Review all prior petitions, applications and Biographic Information Forms (G-325). Do not focus solely on the pending application or petition but consider the applicant's/petitioner's entire immigration history.
2. Review the pending application, petition, and supporting documents for completeness and accuracy. Review every page of the application or petition and Form G-325. Ensure phone numbers and addresses claimed are current.

3. Look for consistency in testimony and documentation to establish credibility.

LE

LE

4. Clearly document changes made to the application or petition during the interview.

LE

LE

5. Ask questions in the same order, being sure to use follow-up questions for unexplained answers.

LE

LE

- 6.

LE

7. Ask about membership in all political, social and religious organizations.

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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

# LE

8. Ensure that all biographical data is current and accurate to include current contact information.

### Internal Vetting/Eligibility Assessment

- Consider: *What do Designated Officers Need?*
- Information regarding eligibility, admissibility, credibility
  - Inconsistencies
  - Misrepresentation and fraud
  - Illegal, suspect or unusual activity
  - Civil infractions
  - Unexplained financial activities
- What systems will need to be checked?
- For Official Use Only (FOUO)/Law Enforcement Sensitive information cannot be disclosed without permission from the record owner
- Classified information cannot be disclosed

### C. Internal Vetting cont'd

1. Completed by Designated Officers
2. Prior to initiating internal vetting, the designated officer considers:
  - 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.
  - b. Does the information in the referral meet the criteria for a NS concern?

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- 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? Officers document information that identifies inconsistencies; misrepresentation and fraud; illegal, suspect or unusual activity; civil infractions; and unexplained financial activities.
  - i. Biographical Information
    - A. Aliases, various spellings, maiden names
    - B. Marital status
    - C. Children
    - D. Location of family members (immediate, siblings, parents, ex-spouses)
  - ii. Immigration History
    - A. Dates of and status at entry
    - B. Purpose of stay
    - C. Type of visa
    - D. Applications/petition filings
    - E. Previous denials
    - F. Suspected immigration fraud
  - iii. Education
    - A. Institutions
    - B. Degrees
  - iv. Work history
    - A. Current and past occupation
    - B. Business or professional licenses
    - C. Tax information/sources of income
    - D. Business associates
  - v. Address History
    - A. Immigration forms
    - B. Taxes
    - C. School Records
    - D. Outside sources
    - E. Check for roommates

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- vi. Military Service
  - A. Dates
  - B. Rank
  - C. Military training
  - D. Active combat
  - E. Compulsory service
  - F. Weapons training
  - G. Flight training
  
- vii. Affiliations, Associations
  - A. Position in group?
  - B. Solicit funds?
  - C. Speak on behalf of group?
  - D. Voluntary or automatic?
  - E. Clubs, Unions, or Organizations
    - 1. Political
    - 2. Social
    - 3. Religious
    - 4. Professional
    - 5. Educational
  
- viii. Travel History
  - A. Frequency and length of trips
  - B. Reason for each trip
  - C. Countries of interest
  - D. Travel companions
  - E. Taking money overseas for self or others
  - F. Travel documents used
  - G. Contacts

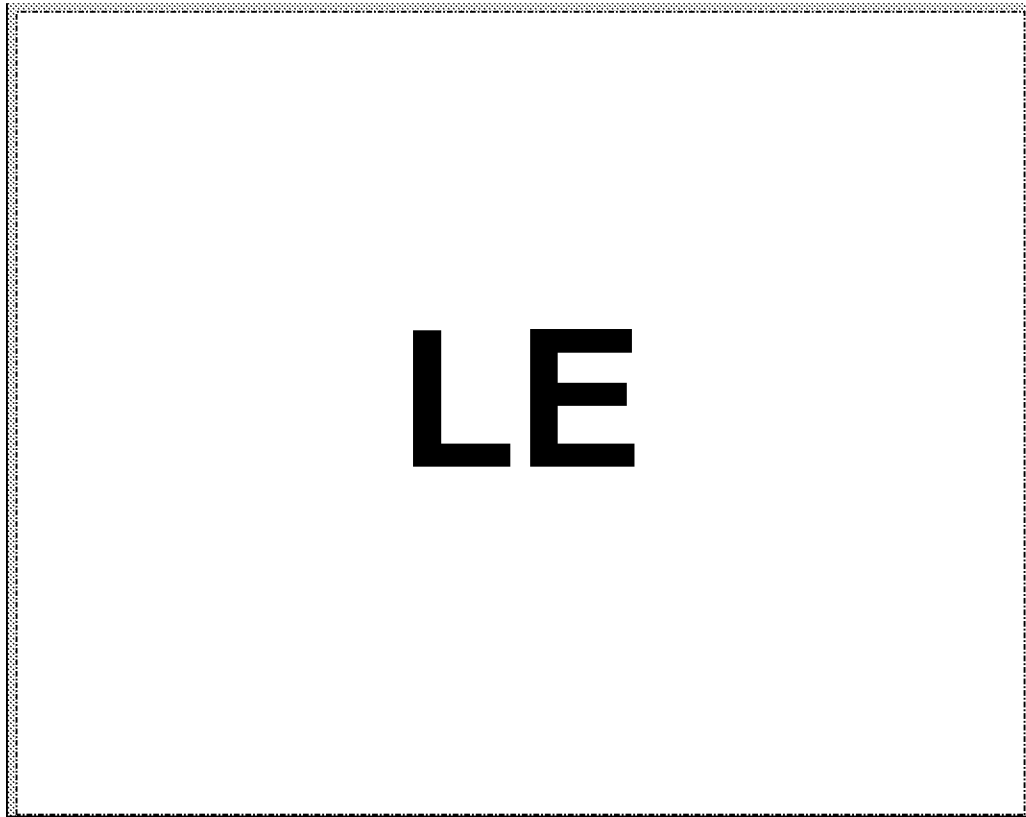
3. Internal Vetting: Systems Checks

For example:

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



FDNS-Data System (FDNS-DS) USCIS System	Provides information on suspected and confirmed fraud, national security and public safety concerns
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
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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

---

**Participant Guide**

TECS	criminal or NS concern
<b>LE</b>	
Choicepoint/LexisNexis Commercial Databases	Associated addresses, social security numbers, businesses, relatives and other close associates
Arrival and Departure Information System (ADIS)	Travel History
<b>LE</b>	
Consular Consolidated Database (CCD) Department of State System	Non-immigrant, immigrant, and DV visa queries
ENFORCE	Query by name, FINS or Biometric information to obtain immigration violations
Image Storage Retrieval System (ISRS) USCIS System	Provides photograph and signature of aliens who have obtained travel documents, employment cards, and permanent resident cards
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) Televue	Used by Asylum Branch
Deportable Alien Control System (DACs) Televue	Detention & Removal docket management system which is to be replaced by ENFORCE Alien Removal Module (EARM)

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Student and Exchange Visitor Information System (SEVIS)	Student status
Open source/Internet Queries	Google, Yahoo, Ask.com, Dogpile, Youtube, MySpace, LinkedIn, Facebook, Twitter, etc.

- **Must be clearly articulated and based on objective facts**
- **Analyze all relevant documents and the circumstances**
- **Not based on a “gut feeling” or the person’s appearances**

### C. External Vetting :

- Conducted when no grounds of ineligibility identified or grounds easily overcome
  - Need to know
  - To determine nature and extent of concern
  - To obtain information about eligibility
  - KSTs – HQFDNS
  - Non-KSTs- Designated Officers in the Field
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

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



- i. Generally BCU and FDNS IOs
  - ii. For Overseas Offices, IO HQ
- 5. Designated Officer reviews information gathered from external vetting and determines whether the NS concern remains or whether there is no longer
  - i. Determination-Not NS, results in routine adjudication
  - ii. Determination-NS, results in adjudication by a designated officer (CARRP Adjudication)

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**EPO #7: Identify 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.

**Note:** Adjudication of national security cases is a process which requires a solid knowledge of the law, great attention to detail, the ability to conduct research, the ability to clearly articulate ideas verbally and in writing and communication skills in order to coordinate with internal components of USCIS and external agencies.

The process is meant to ensure that USCIS does not grant a benefit to an individual who poses a threat to national security and is not eligible for the benefit. Oftentimes the adjudication process is time intensive and laborious due to the sensitivity and complexity of the nature of the concern.

Of utmost importance, is that the Officer does not disclose third agency, sensitive or classified information without the express permission and/or appropriate authority to release that information. When there is an ongoing national security or criminal investigation, close coordination with the respective investigating agency for deconfliction purposes is required so as not to disrupt or impede the investigation.

- Meant to ensure that USCIS does not grant a benefit to an individual who poses a threat to national security and is not eligible for the benefit
- Process is time intensive and laborious due to the sensitivity and complexity of concern
- Requires a thorough review of all pertinent and available documents to determine eligibility

**A. Adjudicative Steps Completed By Designated Officers****Note:**

Steps in adjudicating a case with national security concerns. These steps do not differ much from those that occur during routine adjudication; however, the adjudication of cases with national security concerns generally takes much more time.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

Prioritize NS Case. Notify OCC in federal litigation cases. Federal litigation, congressional inquiries, and management directives?

Timeline? A step-by-step history of the subject's filings, immigration history, and any other event that could impact eligibility, admissibility, removability.

Authenticity of documents/visa information? DOS Reciprocity Tables, CCD, official request to DOS consular office

Adjudication strategy? Discuss with management, OCC and/or NSAU, as appropriate.

Note: Reciprocity refers to the agreements that the US has with each country regarding length of visa issuance. The reciprocity tables provide a list of the different non-immigrant visa types and how long they should be issued for depending on the nationality of the individual. In addition and more importantly for us, the tables list by country the availability of different registry records (birth, marriage, death certificate) or police/military records and tells where they can be obtained. In some instances it tells whether military service is voluntary or not. This is a very good resource for Immigration Services Officers to go if they have doubts about the validity or genuineness of a document as well as its availability. For example, if an applicant says he cannot get a document, the reciprocity tables will advise whether that is true or whether the applicant just hasn't tried hard enough. See below excerpt for the country of Benin.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



Interview or RFE Prep? Detailed line of inquiry for interview and/or RFE, Notice of Intent to Deny (NOID) or Notice of Intent to Terminate (NOIT).  
 Deconfliction? Required prior to USCIS action.  
 Interview? Consider need to audio or video tape.  
 Adjudication Decision – review with supervisor, OCC, obtain concurrence.  
 Issue Notice to Appear (NTA)? Coordinate with OCC, law enforcement agency, and ICE Counsel.

### **TIMELINES ARE VERY IMPORTANT!**

Provide a brief immigration history timeline to include immigration status at entry; listing of all previous immigration forms filed and the outcome of those applications/petitions, history of any exclusion/removal proceedings and/or immigrations violations; current immigration status; any additional pertinent information extracted from the A-file.

### **Ineligibility Findings**

Officers cannot disclose classified or law enforcement sensitive information, so they look at other ineligibilities in the case when drafting a decision.

### **GMC vs 6(C)(i) Inadmissibility**

Good Moral Character (GMC)

Naturalization

False Testimony Sections 101(f) & 336(d) of the INA

8 CFR 316.10(b)(2)(vi)

False testimony under oath for the purpose of obtaining an immigration benefit constitutes a bar to a finding of GMC

Case law supports the idea that a misrepresentation need not be material for a finding of poor moral character

Misrepresented fact must be given for the purpose of obtaining an

### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

immigration benefit

Misrepresented facts other than those given orally under oath are not an automatic GMC bar but can support a finding of lack of GMC

[http://www.travel.state.gov/visa/frvi/ reciprocity/reciprocity\\_3532.html](http://www.travel.state.gov/visa/frvi/ reciprocity/reciprocity_3532.html)

## B. Application of 212(a)(6)(C)(i) Inadmissibility and Good Moral Character (GMC) Bar at 101(f)(6)

Note: This explain that when dealing with national security cases, the law enforcement sensitive or classified information cannot be disclosed, so Immigration Services Officers may identify issues pertaining to Good Moral Character (GMC) or inadmissibility under 6ci in their decision.

Students should understand the difference between an inadmissibility finding based on 212(a)(6)(C)(i) of the INA and a finding that an individual lacks Good Moral Character under 101(f)(6). Many officers, even journeyman officers do not have a clear understanding of the differences between the two.

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.

### GMC vs 6(C)(i) Inadmissibility

#### 212(a)(6)(C)(i)

##### 1. Inadmissibility for Permanent Residence

- a. Anyone 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
- b. Does not need to be under oath
- c. Can be written or oral
- d. Material fact is information that is necessary for the alien to

INA  
212(a)(6)(C)(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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

- be eligible for the benefit or shuts off a line of inquiry relevant to the alien’s eligibility
- e. May be eligible for a waiver
- 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
- a. False testimony must be under oath **and** given orally.
- b. 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.

Example:



INA 101(f) and 336(d)

Other false statements, such as on an application, can lead to a conclusion that a person GMC, but the automatic bar only applies to false testimony.

8 CFR 316.10(b)(2)(vi)

*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**

See DHS Memorandum

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**Note:**

Information about a national security concern may be classified. If not classified it is likely "For Official Use Only" and "Law Enforcement Sensitive". Immigration Services Officers must not disclose this information to the public, to third agencies, or to any other individuals who do not have the proper access/clearance and "need to know".

"Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings", dated October 4, 2004 and signed by Tom Ridge.

**Ridge Memo**

- DHS Memorandum "Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings", dated October 4, 2004 and signed by Tom Ridge
- Department policy precludes the use of classified information, as the basis for denial of a benefit, without (formal) authorization by the Secretary and permission of the owning agency.

**Declassification**

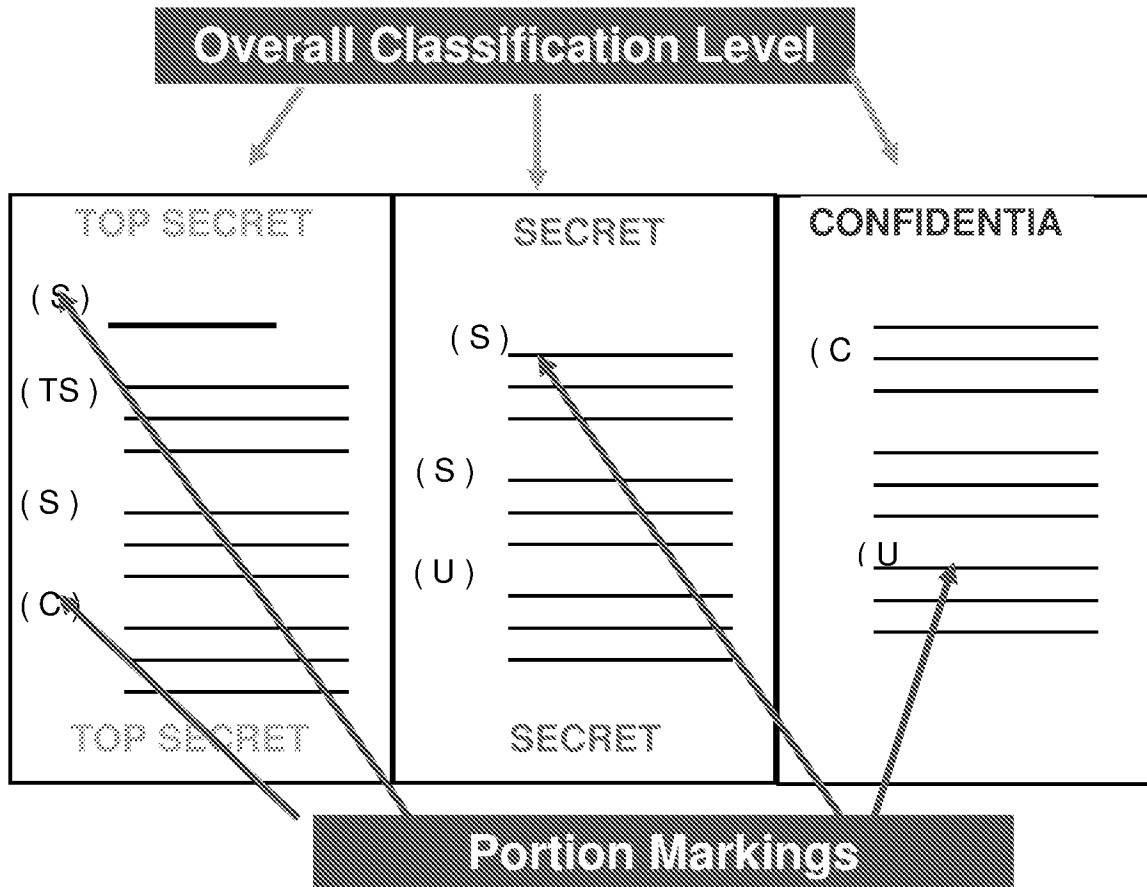
- Declassification of pertinent information, or obtaining approval for use of unclassified but sensitive information contained in investigative reports, is a time-consuming process.

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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

**Classification Markings**



Officers must NOT compromise ongoing investigations by divulging availability or knowledge of Sensitive But Unclassified (e.g. FOUO) or classified information.

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

Note: To be used as a last resort. Requires multiple steps and high level concurrence (e.g. permission/approval by owning agency and sign of by the Secretary of DHS)

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



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.


**Note:** While it is a separate lesson on classified information, it should be emphasized that everyone needs both the clearance and the need to know to review classified. Classified cannot be revealed without both regardless of how strong the need to know or how high the clearance.

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

When sharing information -

- Need to know?
- Proper clearance?

Verify clearance through:

- Local Security Officer
- Office of Security and Integrity (OSI) Personnel Security Customer Service
- Email to
  - **USCIS-OSI-PERSEC-Customer Service** (in Outlook) OR
  - 

### Situations To Remember

If there is any indication that information is classified, assume it is classified.

Don't ever leave classified unattended outside of an approved locked container.

Promptly mark w/appropriate cover sheet A-files containing classified information.

•No processing classified information on an unaccredited computer or e-mailing on DHS e-mail. DO NOT PARAPHRASE. • No discussion or transmission of classified information on nonsecure telephone or fax. DO NOT PARAPHRASE. No mailing of classified information using private, commercial couriers. Classified package must be properly addressed, packaged and marked. Contact intended recipient of classified package before sending it.

#### **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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.



**Who has the first .....QUESTION?**

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**IV. APPLICATION**

**A. In-Class Laboratory**

- None

**B. In- Class Practical Exercises**

- 15 Scenarios for Applying Referral Criteria

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**V. REFERENCES**

- A. INA §§ 101(a)(43), 101(f)(6), 212(a)(3), 212(a)(6)(C)(i), 219, 237(a)(4), 237(c), 240(b)(4)(B),
- B. 8 C.F.R. §§ 103.2(b)(16)(i)-(iv), 235.8
- C. Nutshell Chapter 8 §§ 8-1.2(c), 8-2.2(d)  
Chapter 9 § 9-1.1(d)(2)  
Chapter 13 § 13-4.6

**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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

**VI. Appendix**

- A. USCIS Operational Memorandum, “*Policy for Vetting and Adjudicating Cases with National Security Concerns*” dated April 11, 2008
- B. USCIS Memorandum, “*Revised National Security Adjudication and Reporting Requirements*,” dated February 4, 2008.
- C. USCIS Operational Memorandum, “*FBI Name Check Process and Clarification for Domestic Operations*,” dated December 21, 2006.
- D. USCIS Fact Sheet, “*Immigration Security Checks—How and Why the Process Works*,” dated April 25, 2006.
- E. DHS Secretary’s Memorandum, “Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings,” dated October 4, 2004.
- F. Guidance for Identifying 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.