

**EXHIBIT 61**  
**FILED UNDER SEAL**

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

---



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

***FDNS OFFICER  
BASIC TRAINING***

**NATIONAL SECURITY  
INSTRUCTOR GUIDE**

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

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

---

**August 2008**

---

**SYLLABUS**

**COURSE TITLE:** National Security

**COURSE NUMBER:** 701

**COURSE DATE:**

**LENGTH AND METHOD OF PRESENTATION:**

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

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

Instructor's note: This national security training module has been designed to last approximately 7.5 hours. Below are suggested time guidelines for each Enabling Performance Objective (EPO) to assist instructors pace themselves during the course of the training.

In addition, the instructor's notes found in the gray text boxes throughout the Instructor's Guide provide speaking points that the instructor may wish to incorporate into the training presentation. Instructors are encouraged to include pertinent anecdotes relating to on-the-job experiences or examples which will help to illustrate and reinforce the material.

Introduction: 15 minutes  
 EPO#1: 15 minutes  
 EPO#2: 15 minutes  
 EPO#3: 45 minutes  
 EPO#4: 1.5 hours includes 17 practical exercises  
 EPO#5: 30 minutes (includes 3 minute video clip)  
 EPO#6: 1 hour includes 2 practical exercises  
 EPO#7: 45 min includes 10 practical exercises  
 EPO#8: 30 minutes

Multiple practical exercises have been incorporated into the training.

**1) Practical Exercises- CARRP Case?**

5 Scenarios to discuss whether based on the information presented the case should be adjudicated under CARRP.

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

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

**2) Practical Exercise - Identifying NS Concerns**

17 scenarios are presented to the students on slides. This exercise should promote class discussion about whether there is sufficient information available to make a determination if a NS concern exists, whether it is a KST or non-KST NS concern, whether to refer the case as a national security concern, whether they should review the file closer for additional information, or whether they should develop a line of inquiry to be asked at the time of the interview. These scenarios were generated from actual national security referrals. The scenarios and discussion topics are found at the end of the Instructor Guide. Estimated time 20 minutes.

**3) Practical Exercises – Considering Classified Information**

2 scenarios. Students are asked to explain how they would consider the information without divulging knowledge of it or disclosing it. Do's and Don'ts included in the slides. Estimated time: 15 minutes.

**4) Practical Exercises- External Vetting**

After reviewing the scenario in each slide, students should answer the following questions

- 1-Identify the NS indicators and do rise to level of NS concern
- 2-Determine what internal vetting steps should have been taken
- 3-Determine if there is enough information to determine whether the NS concern has been resolved or the NS concern remains

**DESCRIPTION:**

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

**TERMINAL PERFORMANCE OBJECTIVE (TPO):**

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

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

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

**ENABLING PERFORMANCE OBJECTIVE (EPOs):**

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

**STUDENT SPECIAL REQUIREMENTS:**

**METHOD OF EVALUATION:**

Written Examination – Multiple Choice

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

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

---

**TABLE OF CONTENTS**

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

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

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

Instructor's note: The material for this course has been labeled "For Official Use Only (FOUO)/ Law Enforcement Sensitive," and should be handled accordingly.

## Presentation

## References

### I. INTRODUCTION

Instructor's note: Security Check vs. Background Check— Security checks include the FBI Name Check, FBI Fingerprint Check, TECS/IBIS and US-VISIT. Background check refers to the analysis of the results of the security checks or any other identified concern relating to national security or public safety and the actions required to resolve the concern such as reaching out to a third agency for additional information on the applicant, requesting a site visit, conducting a re-interview, etc.

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

#### **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).

security hits requiring intensive review and resolution.

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

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

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

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



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

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

**Instructor’s note:**

The terms defined below are found in the USCIS policy memorandum entitled, “Policy for Vetting and Adjudicating Cases with National Security Concerns” dated April 11, 2008.

These terms are primarily found in the footnotes of the memorandum and should not be overlooked. It will be essential for students to understand the difference between KST NS Concern and Non-KST NS Concern as well as the differences among the terms: internal vetting, external vetting, and deconfliction.

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

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

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

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

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

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

System (CLASS), as used by the Department of State.

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

1. A category of the remaining cases with NS concerns including but not limited to:
  - a. Associates of KST(s)
  - b. Unindicted co-conspirators
  - c. Terrorist organization members
  - d. Persons involved with providing material support to terrorists or terrorist organizations, and
  - e. Agents of foreign governments

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

### **D. Security Checks**

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

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

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

### **E. Internal Vetting**

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

### **F. External Vetting**

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

- (a) fact or fact patterns necessary to determine the nature and relevance of the

#### **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).

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.

### **G. Deconfliction**

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

Instructor's note: The term "Designated Officer" is used in this lesson but has a different connotation depending on the operational guidance. The Domestic Operations guidance (which likely applies to the majority of the students) defines "designated officer" on page 5. Look to footnote number 5 for the following definition: "For purposes of this memorandum, a **designated officer** is an 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."

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

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

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

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

Instructor's note: This section provides a brief overview of the three directorates in USCIS (NSRV, Domestic Operations, and Refugee, Asylum, International Operations). In the next section, the CARRP policy and different components' operational guidance are discussed so students should understand how all the offices relate.

The slide presentation has three organizational charts, one for each directorate.

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

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

Instructor's note: The National Security Branch was previously composed of three units. As of July 2008, the NSB now has four units, all which will support the field in their vetting and adjudication of NS 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).

The Field Support Unit (FSU) is the most recent addition to the NSB. The FSU staff triages the requests for assistance sent from the field to HQFDNS via the FDNS-NSB mailbox (which replaced the FDNS-IBIS mailbox).

1. National Security Branch (NSB) at Headquarters FDNS
  - a. Field Support Unit (FSU)
    - i. Triages requests for assistance from the field
    - ii. Develops and provides training to the field and HQFDNS
  - b. Background Check Analysis Unit (BCAU)
    - i. Externally vets KST NS concerns
    - ii. Provides advice and technical assistance to the field
    - iii. Detailed to other agencies and DHS components
      - A. Terrorist Screening Center (TSC)
      - B. National Joint Terrorism Task Force (NJTTF)
      - C. FBI's National Name Check Program (NNCP)
      - D. Immigration and Customs Enforcement (ICE)
  - c. Adjudication Support Unit (ASU)
    - i. Formerly known as National Security Advisory Unit (NSAU)
    - ii. Develops and coordinates case resolution strategies relating to national security cases.
    - iii. Coordinates with Intelligence and Law Enforcement Agencies to declassify or use classified information when required
  - d. Policy Support Unit (PSU)

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

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

- i. Formerly known as National Security Policy and Strategy Unit (NSPS)
- ii. Provides policy analysis and guidance for the National Security Branch to help shape operations, procedures, and strategies.

## 2. FDNS Immigration Officers in the Field

- a. Located at each field office, asylum office and service center.
- b. Review, research, and analyze information relating to applications/petitions when there are national security, public safety, or fraud concerns.
- c. Do not adjudicate
- d. Document work in FDNS-Data System (FDNS-DS) a national database used by FDNS to monitor and track referrals and cases involving national security concerns, suspected and confirmed fraud, and egregious public safety concerns.
- e. Primary conduit for law enforcement coordination such as ICE, FBI, and members of the local JTTF to support the USCIS mission of ensuring the integrity of the immigration system and removing those who pose a threat to the U.S.

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

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

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

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

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

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

- a. Service Centers
  - i. Have established procedures to review all IBIS, FBI fingerprint & FBI name check results when the initial response is received; this includes the immediate review of Rap sheets.
  - ii. All national security concerns and concerns are referred to local Background Check Units (BCU)

Instructor's note: Note that at service centers, Background Check Units (BCU) primarily handle cases with NS concerns not FDNS IOs. All FDNS IOs regardless of location need to be familiar with this policy and process because at any time local management could designate them as a "designated officer" depending on workload.

Furthermore, FDNS IOs may encounter NS indicators or concerns when handling their workload of fraud cases or may be presented a NS case with suspected fraud, so they need to be fully familiar with this NS module.

- iii. FDNS Immigration Officers do not handle the national security cases.

- b. Field Offices
  - i. Have established procedures to ensure all IBIS, FBI Fingerprint & FBI Name Check results have been received, reviewed, and are current prior to the granting of an immigration benefit.
  - ii. Each Field Office has an established referral process to the local FDNS Immigration Officer for cases identified as having national security concerns.

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

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

Instructor's note: Explain to students that Refugee Affairs Division provides the Refugee Officers who regularly travel overseas to interview and adjudicate refugee applications. The Asylum Division has 8 offices throughout the U.S. and handle credible fear claims at the ports-of-entry as well as affirmative asylum applicants. International Operations has 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).

personnel stationed at U.S. embassies and consulates throughout the U.S. These officers may adjudicate waivers, orphan and other relative petitions, and refugee applications.

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

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



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

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

##### Instructor's notes:

Determine which components the students are from: Domestic Operations, Refugee, Asylum, International Operations. Advise that the training is meant to encompass all components therefore it is fairly broad; however, since the majority of students are from Domestic Operations, there will be more emphasis on their procedures in certain sections. Those sections should indicate that the information is from the Domestic Operations guidance.

Prior to the issuance of the USCIS policy memo entitled "*Policy for Vetting and Adjudicating Cases with National Security Concerns*" on April 11, 2008, the national security case load was centralized at Headquarters Office of Fraud Detection and National Security. The Background Check Analysis Unit (BCAU) vetted the cases with NS concerns and the National Security Adjudications Unit (NSAU), now known as National Security Advisory Unit (NSAU) developed adjudicative strategies for the cases.

The NS policy issued on April 11, 2008 is significant in that it provides agency wide NS policy. Previously, Refugee and International Operations had separate policies. The policy also allows for the decentralization of the NS caseload to the field and takes HQFDNS out of the operational role it has been playing for the past several years. HQFDNS will now take on a more advisory role under the new policy.

In addition to the NS policy, Domestic Operations (includes Field and Service Center Operations) and the 3 components within the Refugee, Asylum, and International Operations Directorate (RAIO) – Refugee Affairs Division, Asylum Division, International Operations Division, issued their own separate operational guidance in order to implement the policy. The operational guidance focuses on the details of adjudicating the various types of applications/petitions under each component.

Advise students that policy is dynamic and students must keep abreast of policy changes. USCIS broadcasts announce new policy and the intranet

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

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

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

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

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

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

posts the policy for reference purposes.

1. Provides agency-wide national security policy
2. Decentralizes the authority to vet and adjudicate cases with national security concerns – from HQFDNS to field offices
3. Establishes the Fraud Detection and National Security Data System (FDNS-DS) as the primary system for documenting activities (vetting, deconfliction, resolution activities) of national security cases
4. Distinguishes between two types of national security concerns
  - a. Known or Suspected Terrorist (KST)
  - b. Non-KST
5. Applies to all applications and petitions that convey immigrant or non-immigrant status
6. Rescinded specific previous USCIS national security policy memoranda
7. Effective upon the issuance of operational guidance from the Directorate of Domestic Operations and each component within the Directorate of Refugee, Asylum, and International Operations (RAIO)

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

Instructor's notes: All students must refer to their appropriate guidance to determine the requirements for their specific position. The 4 separate guidance documents are provided electronically.

8. Policy memorandum and Operational Guidance is For Official Use Only (FOUO)
9. Establishes a standard CARRP workflow consisting of four stages in order to identify, record, and complete applications/petitions with a national security concern
10. Completed by Designated Officers as outlined in each component's individual guidance

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

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

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

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

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

Instructor’s notes: The operational guidance also provides for “Attachment A: Guidance for Identifying National Security Concerns”. All components are using this same tool for standardization purposes.

The Background Check and Adjudicative Assessment, which replaced the National Security Record (NSR) is no longer used. It is to be replaced by FDNS-DS but in the interim, officers must complete one or more worksheets that are outlined in the 7/18/08 memo about interim procedures for tracking NS cases. Additional guidance will be forthcoming. This course will not focus on completing these documents. Upon return to their offices, if students require assistance completing the worksheets, they should look to their supervisor and seek assistance through the chain of command if required. Designated worksheet(s) terminology used throughout the class refers to this 7/18/08 memorandum.

## B. Four Stages in the CARRP Workflow

### 1. Identifying National Security Concerns

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

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

### 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).

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, owner, partner, affiliate, or friend.

## 2. Eligibility Assessment/Internal Vetting

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

## 3. External Vetting

Outreach to record owner of national security information:

- a. To obtain information that may be relevant in determining eligibility
- b. To obtain information regarding the nature and extent of the national security concern

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

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

- c. For KST, HQFDNS maintains sole authority for KST external vetting
  - d. For Non-KST NS concerns, the Field conducts external vetting
4. Adjudication of National Security Cases (CARRP Adjudication)

Evaluation of results of internal and external vetting to make eligibility determination.

- a. For KSTs, seek HQFDNS assistance
  - b. For Non-KST NS concerns, Senior-level official has authority to approve or discretion to seek HQFDNS assistance. See operational guidance for definition senior-level official.
5. At any stage of the process, any of the following actions may occur:
- a. Deconfliction
  - b. Request for Assistance to HQFDNS
  - c. Determination that the case is not national security and is released for routine adjudication
  - d. A KST becomes a non-KST NS Concern or non-national security
  - e. A non-KST becomes a KST

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

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

- 1. Petitions that do not convey immigrant or non-immigrant status are not vetted and adjudicated under CARRP. Adjudication of these petitions establishes eligibility for the visa category not admissibility.
- 2. Regardless, certain steps are required if a national security concern should arise:

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

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

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

- a. National security concern must be documented. (designated worksheet(s)/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

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.

Instructor's Note: page 40 of the Domestic Operations Operational Guidance lists the petition 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

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 designated worksheet(s). 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.

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

1. If an exemption is granted under INA § 212(d)(3)(B)(i) of the Act, AND no other NS concern is identified, no further vetting is required and the application/petition may continue through routine adjudication.
2. If an exemption is available but will not be granted under INA §

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,

#### **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).

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 documentation is required.

“Implementation of Section 691 of Division J of the Consolidated Appropriations Act, 2008, and Updated Processing Requirements for Discretionary Exemption to Terrorist Activity Inadmissibility Grounds”

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

AND

Dated May 24, 2007 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

**E. Special Considerations**

- 1. Specific guidance on these applications and cases may be found in the

**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).

respective operational guidance.

- a. Application for Employment Authorization (Forms I-765)
- b. Application for Travel Authorizations (Form I-131)
- c. (Forms I-765 and I-131)
- d. Application for Replacement Permanent Resident Card (Form I-90)
- e. Santillan Cases
- f. Appeals/Motions to Reconsider or Reopen
- g. Application for Naturalization

for Vetting and Adjudicating Cases with National Security Concerns” dated April 24, 2008, signed by Don Neufeld.

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

Instructor’s Note: These cases fall under the CARRP process; however, if vetting is not concluded within a specific period of time named in the guidance then the application may be adjudicated. Remembering deconfliction prior to a decision. Since the two May 11, 2007 memos were rescinded (regarding ancillary benefits and I-90s), parts of the memos had to be restated such as how to handles public safety concerns with these applications.

Santillan cases refer to the cases when the Immigration Judge grants permanent residency. The individual presents to USCIS the IJ grant at an InfoPass appointment and if eligible is processed for issuance of a permanent resident card. There are specific timelines for the issuance of the document (30 to 60 days) depending on the grant date.

Instructor’s Note:

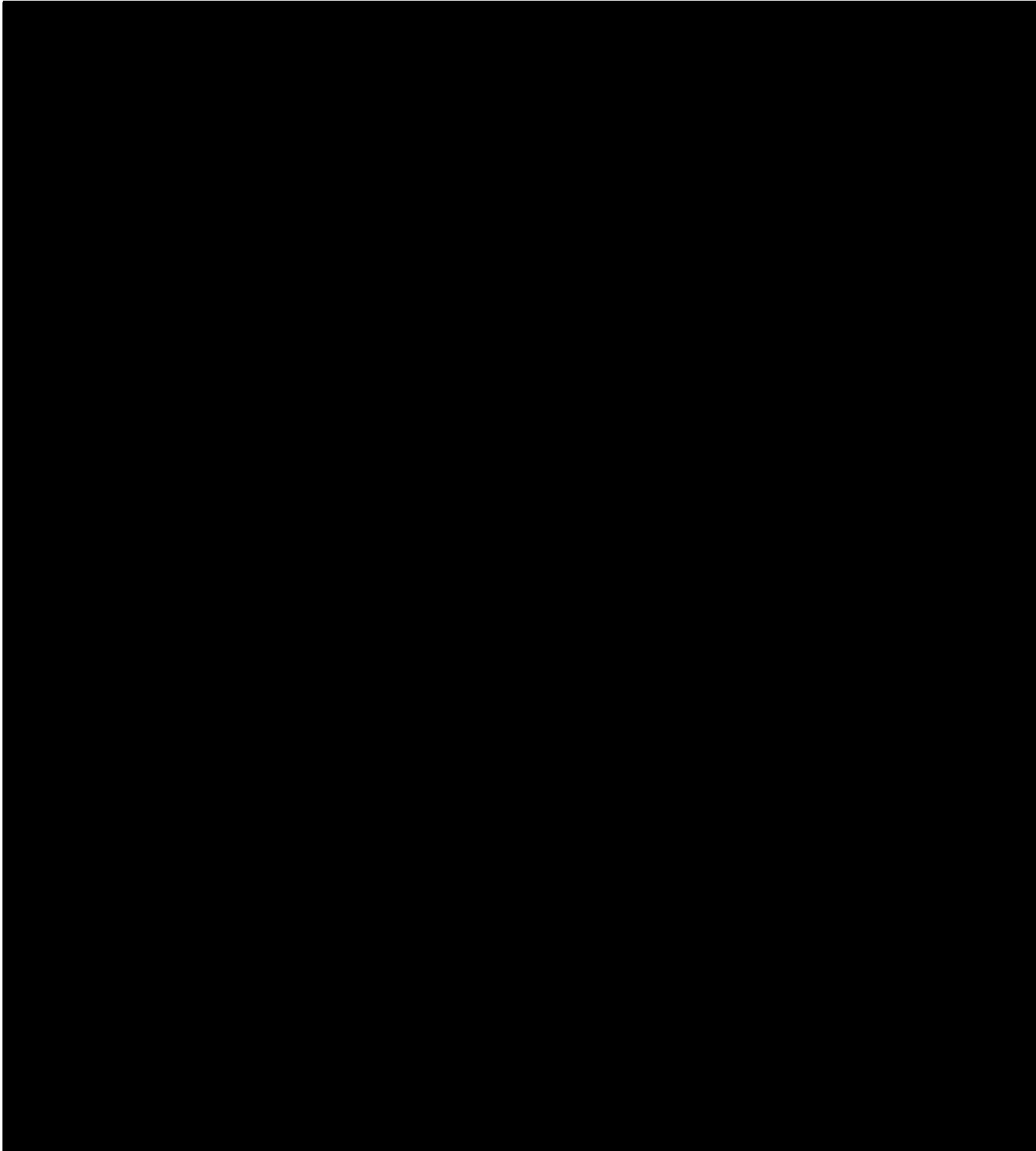
**Practical Exercises on Slides 58-63**

This exercise is meant to discuss how these different applications/petitions would be considered under CARRP. Discussion points are **in bold** below each scenario.

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

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



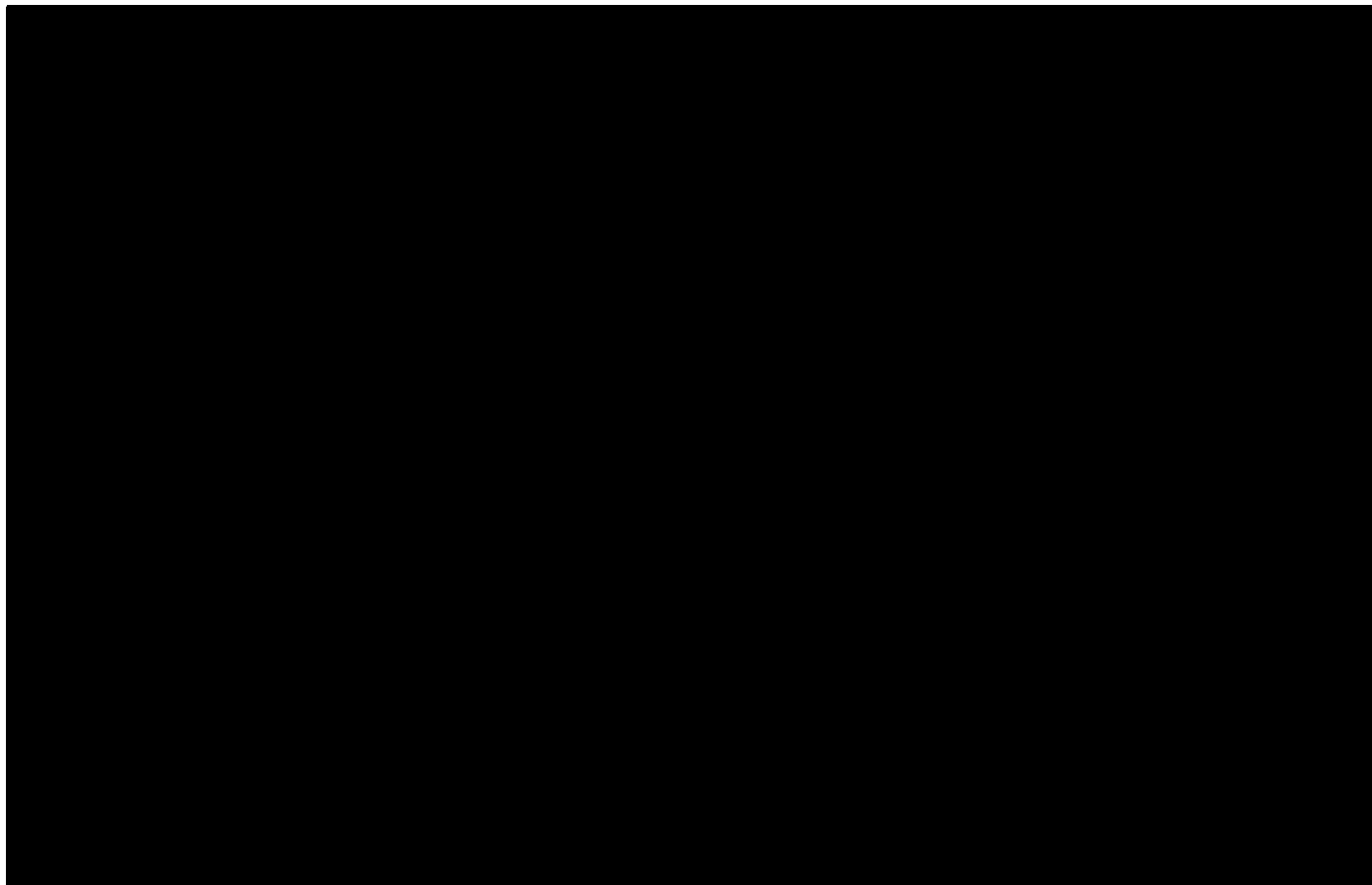


**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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

**USCIS**  
**NATIONAL SECURITY**

**23**  
**August 2008**



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

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

**USCIS  
NATIONAL SECURITY**

**24  
August 2008**

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

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

**1. Articulable Link**

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

**Instructor's note:**

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.

**2. Two Types of NS Concerns**

- a. Known or Suspected Terrorist (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).

## b. Non-KST

Instructor's note:

**Emphasize the importance of understanding the distinction between a KST and a non-KST. Students must understand whether they are dealing with a KST or a non-KST before they can properly apply the policy and operational guidance.**

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

Instructor's 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).

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.

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

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

- d. Directs federal agencies to provide appropriate terrorist information to the National Counterterrorism Center (NCTC), which in turn provides the TSC access to all appropriate terrorist information or intelligence.
2. Terrorist Identities Datamart Environment (TIDE) [http://www.nctc.gov/docs/Tide\\_Fact\\_Sheet.pdf](http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf)
- a. U.S. Government's central repository of information on international terrorist identities.
- b. Supports the U.S. Government's various terrorist screening systems or "watch list" and the U.S. Intelligence Community's overall counterterrorism mission.
- 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. Terrorist Screening Center (TSC)

Instructor's notes: The TSC has been operational and running 24/7 since December 2003. The TSC is much like a call center in that it responds to inquiries from state, local, and federal agencies who encounter individuals who are a potential match to a watch listed subject. In addition to USCIS, CBP regularly contacts TSC (via the National Targeting Center-NTC) for encounters at POEs or on the border with KSTs.

The TSC will forward the information provide by USCIS to the Terrorist Screening Operations Unit (TSOU) who will then contact the primary case agent or originating agency. The TSC, TSOU or case agent may or may not

**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).

contact USCIS in response.

The TSC generally requests a copy of the application or petition be faxed to them. This information may assist in establishing whether there is a definitive match and it may assist the originating agency in their review of the case. USCIS Officers may comply with this request; however, USCIS Officers must NOT forward asylum applications to the TSC.

The TSC should not be contacted unless there is a KST hit: IBIS **LE** hit directing contact with the TSC.

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."

Instructor's note:

**LE**

**LE**

accompanied by "CIO" hits (generally TSA Selectee hits). If there is no

**LE**

and no **LE**

" but only a "

**LE**

contact with TSC may be required

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

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

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

- b. Confirms matches for KST hits and forwards pertinent information provided by USCIS to the Terrorist Screening Operations Unit (TSOU) who contacts the primary case agent or originating agency.
- c. The TSC, TSOU or case agent may or may not contact USCIS in response.
- d. The TSC generally requests a copy of the application or petition be faxed to them. This information may assist in establishing whether there is a definitive match and it may assist the originating agency in their review of the case. USCIS Officers may comply with this request; however, USCIS Officers must NOT forward asylum applications to the TSC.

e.

**LE**

Instructor's note: USCIS identifies Known or Suspected Terrorists (KST) hits via IBIS, NCIC, or CLASS. These individuals are on the Terrorist Watch List.

**LE**

Remember, we have been instructed not to fax an asylum application (I-589). You can ask the student if they know why we are not to fax asylum applications. The reasoning is due to the confidentiality provision for those that apply for asylum. Information about an asylum applicant and his/her claim is confidential and must be authorized. There are certain law enforcement and administrative clauses that allow for disclosure.

**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).

## 4. Known or Suspected Terrorist (KST) Hit

## a. TECS/IBIS

- i. Identified in IBIS with a record number beginning with **█**
- ii. Record should indicate the individual is a Known Terrorist or Suspected Terrorist and to contact NTC.
- iii. USCIS Officers should not contact the NTC in such cases but instead are required to contact the Terrorist Screening Center (TSC) in order to confirm whether the KST hit is a match.

## b. National Crime Information Center (NCIC)

- i. Identified by **LE** followed by a number.
- ii. Indicates the subject is a “Possible Terrorist Organization Member” or an “International Extremist” and requests contact with the TSC.
- iii. Note: The Terrorist Watch List information in NCIC is

**LE**

number. If the record indicates the individual is a gang member, the gang is not considered a terrorist organization, and there are no additional indicators that the individual is a NS concern, the hit would not rise to the level of a national security concern but should be resolved according to standard operating procedures for individuals who are a risk to public safety.

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

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

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

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



### C. Non-KST National Security Concern

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

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

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

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

Non-KSTs are not on the watch list. Just because they are not on the watch list, doesn’t mean they are not dangerous and do not pose a threat to our national security.

Non-KSTs may be associates of KSTs or unregistered foreign agents. These individuals may be supporting KSTs by providing material support such as funds transfer services, housing or accommodations for meetings, providing travel services to include fake documents and transportation.

Non-KSTs may be applicants who are living in the U.S., have an association with a business, organization, or individual who is an identified NS concern and law enforcement is unaware of that association.

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.

#### 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).

Remember Non-KST does not mean not dangerous.

## 1. Statutory Indicators

Sections found in the Immigration and Nationality Act (INA)

Instructor's note: The slide presentation does not provide the detailed sections of the INA so the instructor should discuss these and reference the availability of these in the participant guide and the INA.

### a. Security related inadmissibility grounds

212(a)(3)(A)

#### i. Espionage

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

Definitions for Foreign Intelligence and Counterintelligence found at:

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

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

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

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

Espionage also known as 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;

### 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).

or our nation's scientific and technological innovations and research, both public and private.

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

Instructor's 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 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.

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

**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).

- An alien who endorses or espouses terrorist activity or persuades others to endorse or espouse terrorist activity or support a terrorist organization are 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.

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:

- 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

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

**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).

weapon or device, or

- G. explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property.
- H. A threat, attempt, or conspiracy to do any of the foregoing.

ii. Engage in Terrorist Activity Defined

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

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

- A. To commit or to incite to commit, under circumstances indicating an intention to cause death or serious bodily injury, a terrorist activity;
- B. To prepare or plan a terrorist activity;
- C. To gather information on potential targets for terrorist activity;
- D. To solicit funds or other things of value for a terrorist activity; a Tier I or II terrorist organization; or a Tier III organization unless the solicitor can demonstrate by clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization;
- E. to solicit any individual--to engage in conduct otherwise described in this subsection; for membership in a designated terrorist organization (Tier I or Tier II); for membership in an undesignated terrorist organization (Tier III) unless the solicitor can demonstrate by

**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).

clear and convincing evidence that he did not know, and should not reasonably have known, that the organization was a terrorist organization;

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

Instructor's 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.

**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).

Indicate that there are certain exceptions and an exemption may apply.

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”

Section 212(a)(3)(B)

iii. Inadmissibility for Terrorist Activity

In general, any alien is inadmissible who-

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

**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).

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 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.

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

iv. Terrorist Organization Defined

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

A. Tier I – Foreign Terrorist Organization (FTO)

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

1. An organization designated under section 219 of the INA by the Secretary of State a finding that the organization engages in terrorist activities or terrorism.
2. These organizations threaten U.S. nationals or the national security of the U.S.

**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).



3. Over 40 different organizations are currently designated and include such organizations as HAMAS, Al Qaeda, Hizballah, and Revolutionary Armed Forces of Colombia (FARC).

B. Tier II – Terrorist Exclusion List (TEL)

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

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

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.

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

Instructor's 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.

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

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

- c. 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
  - i. Deportable Aliens – Miscellaneous crimes  
237(a)(2)(D)
2. Non-Statutory Indicators

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

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.

Instructor's 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

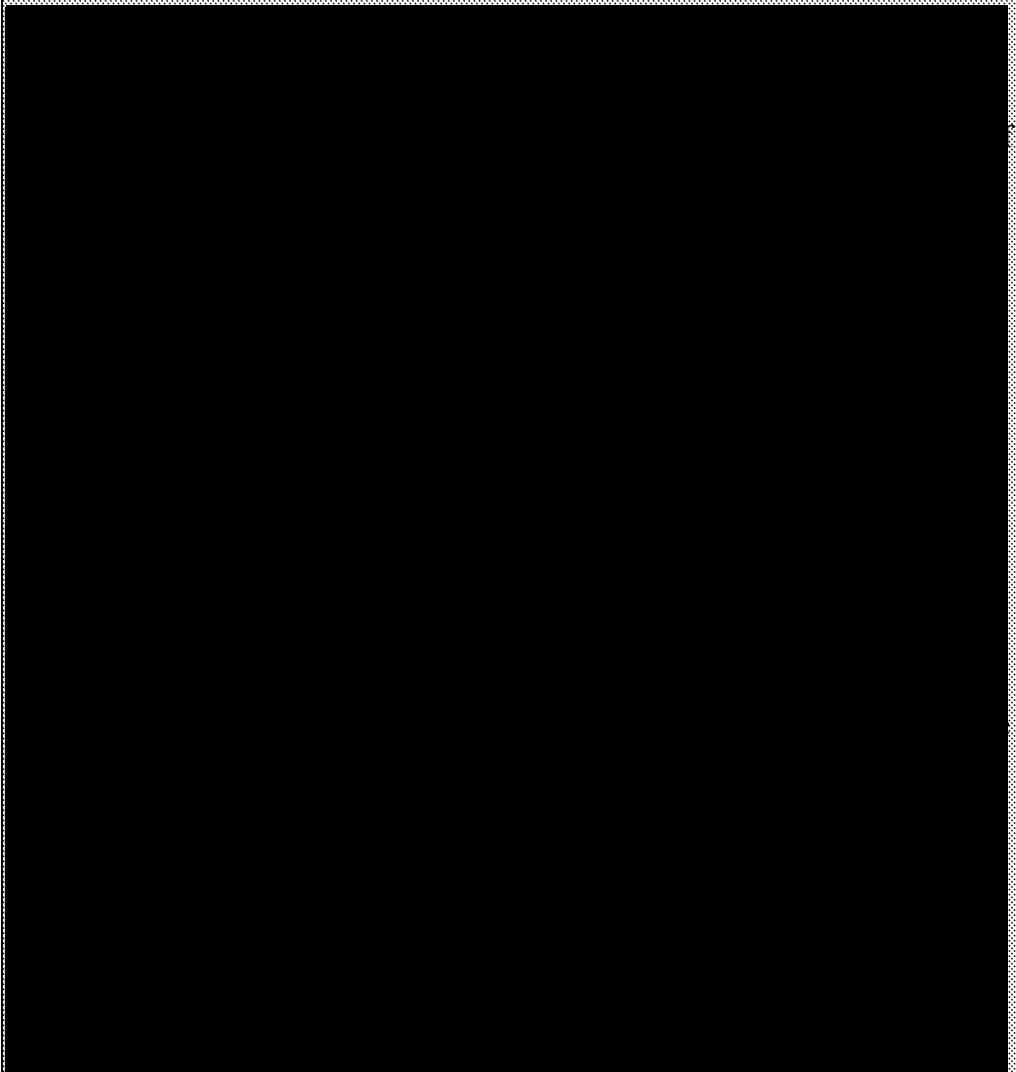
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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).

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 Adjudications Officer should consider:

This information is oftentimes obtained during the interview or in the application/petition. Encourage the Adjudications Officer to consistently ask questions about military history which is found on both the I-485 and N-400.



**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).

Encourage the Adjudications Officer to review the G-325 for completeness, accuracy, and employment history.

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.
- ii. For example, an individual may have been employed by a foreign government to engage in espionage or intelligence gathering, may have received training in such activities, or may have served as an official or diplomat in a hostile foreign government.

A. 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.

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

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

Instructor's note: State Sponsors are countries determined by the Secretary of State to have repeatedly provided support for acts of international terrorism are designated pursuant to three laws: section 6(j) of the Export Administration Act, section 40 of the Arms Export Control Act, and section

**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).

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.

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

Note: Libya was removed from the list.

The below excerpts were 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."

**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).

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 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.

■ [REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

**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).

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

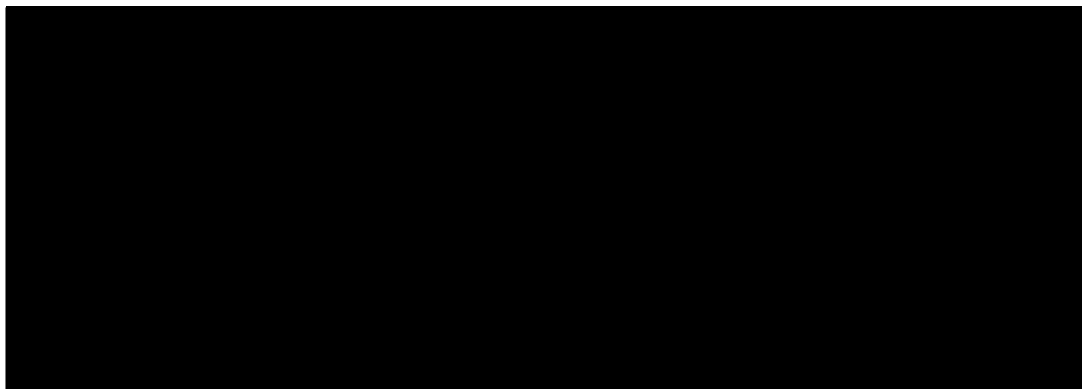
[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

**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).

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]



**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).



Hawala is also known as hundi.

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

**Instructor’s note:**

In accordance with the USA PATRIOT Act, Hawala in the U.S. is illegal if not registered as Money Service Business.

White vs Black Hawala –terms used to describe the difference in the source

**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).

of the money.

Allegedly white hawala dealers would use white smoke to indicate their business whereas black hawala dealers would use black smoke.

White Hawala can be used to send legitimate funds overseas such as migrants sending money home but it can also be used to funnel dirty money out of or into a country.

Black Hawala refers to transferring dirty money, money obtained through illicit means.

Pros of hawala:

- Don't need a bank account therefore don't need identity documents, social security number, or driver's license.
- No record of transaction--so no paper trail
- Efficient 1-2 days
- Cheaper rate for transaction than traditional banks

Interpol has a detailed description of Hawala at <http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp>

The below notes are excerpts found at [http://www.cbp.gov/xp/CustomsToday/2002/April/custoday\\_hawala.xml](http://www.cbp.gov/xp/CustomsToday/2002/April/custoday_hawala.xml) as of 3/28/08.

"Financial investigators call hawala a "system of remittance" - in this case, an ancient, record-less, international method of transferring money that is based upon trust. Hawala originated in southern Asia and today is practiced largely in that area, the Middle East, and by émigrés from those regions. Since September 11, American law enforcement has been trying to pull back the rocks under which it hides because federal investigators believe hawala is underwriting no small part of Middle Eastern terrorist operations.

The word *hawala* is Hindi for trust; these days, however, it has taken on a more nefarious meaning.

It didn't start out that way; it developed long before there were banks, wire transfers, Western Union, or even checks. Although it is still not necessarily

**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).

used for illegal purposes - there aren't many ways to wire money to Afghanistan or Somalia, for instance - it remains one way that folks with money to hide can jump the national, legal, and financial barriers inherent in conventional banking.

Stopping the dollars that support terrorism is hard enough to do under Western banking systems, which keep records of transactions. In fact, banks in the entire Western Hemisphere must, by law, report to their national treasuries any transfers larger than \$10,000. But with hawala, thousands, even millions of dollars at a time can crisscross the globe in a matter of hours, tracked only by a secret code and disposable scraps of paper, making hawala investigations a shell game of global proportions.

Even at its most benign, hawala cheats governments of legally owed taxes, customs duties, and other fees that are the rightful income of nations - money desperately needed, especially in the countries where it is practiced, to improve those countries' economic conditions.

#### **How it works**

Say a Pakistani immigrant living in Baltimore wants to send \$5,000 home to his parents. He contacts a local *hawaladar*, as dealers are called, known to him through cultural or ethnic ties, and gives him or her \$5,000 plus a small fee for the latter's efforts. The dealer then phones another hawaladar in Karachi. The Karachi dealer delivers \$5,000 worth of rupees to the man's parents. End of story.

Sort of. Isn't the Karachi dealer now out \$5,000? Yes, but only temporarily. As stated earlier, the key to hawala is trust: the Karachi dealer knows that the \$5,000 will be returned to him - his outlay will be remitted - in the future, when he initiates a similar deal.

Hawala dealers give money out and take money in, not necessarily from the same client, so that in the end, their books balance. The remitted funds may follow a course as circuitous as that taken by Laurel and Hardy's rent money, but with hawala, what appears to be invisible accounting, isn't.

Written accounts of transactions, if they are done at all, are done in code on scraps of paper that are destroyed when the transaction is over. The code may be a combination of serial numbers taken from currency notes and known only to the hawaladar and the recipient."

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

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

“The USA Patriot Act, passed in October 2001, expanded the federal government’s investigative powers and created important new criminal offenses. One of them makes failure to register with FinCEN a felony for money-remitting businesses. (Before recently issued Treasury regulations mandated this registration, 45 states had such laws; now it is a felony to violate the federal registration requirement).”

e. Closed Investigations

Reference to a “closed” investigation does not mean that there is no national security concern or that the concern was resolved during the course of the investigation. Law Enforcement Agencies (LEA) close investigations for a variety of reasons, some substantive and others administrative. For instance, investigations may be closed due to a lack of resources available to pursue the investigation, relocation of the subject to another office’s jurisdiction, subject’s departure from the U.S., or exhaustion of available leads. Furthermore, investigations may be closed if the U.S. Attorney does not accept the case for prosecution. Officers need to gather additional information to determine whether a NS remains despite the closure of a formal investigation.

Instructor’s note: Annually, USCIS receives approximately six million applications and petitions for immigration benefits. USCIS policy requires the completion of one or more security checks prior to granting immigration benefits as part of the background check process. The background check process allows USCIS to conduct a comprehensive review of the facts of the case. 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 or public safety nature, because of the large number of applications filed each year, a significant number result in national security or public safety hits requiring intensive review and resolution.

A thorough review of the pending application or petition, supporting documents, file(s), and the results of the required security checks is necessary to determine whether an individual poses a threat to national security. The Adjudications Officer must analyze the facts of the case, considering the

**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).

totality of the circumstances, to determine whether the concern exists.

This section provides information to help officers recognize when the issue of a national security concern may arise as a result of the security checks. This section does not provide an exhaustive list of criteria or methods for identifying national security concerns but should serve as a reference tool for Officers when evaluating potential cases.

### 3. Security Check Indicators

#### a. FBI Name Check

**Instructor's Note:** The results of the FBI Name Check do not necessarily reveal the same information as do the results of the FBI Fingerprint Check or TECS/IBIS.

The FBI got into the "name check" business in 1953, when President Eisenhower asked us to start running the names of federal job seekers applying for national security positions through our files to make sure these individuals didn't pose a threat to our country.

*Agency/entity submission to the FBI's NNCP: Submissions are accepted via magnetic tape, hard copy, telephone, or fax.*

**LE**

**LE**

indicates that the UNI database contains no identifiable information regarding a particular individual. A secondary  search of residuals from the batch run identifies an additional number of names as a  response.

The remaining paper files and/or electronic files are reviewed to ensure they are germane to the name check request. Identifiable files are then analyzed for relevant or derogatory information that may be disseminated to the requesting agency/entity.

Sixty-eight percent (68%) of the name check requests are resolved within 48 hours as "No Records", an additional twenty-two percent (22%) return final

#### **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).

result within 30 to 60 days; the remainder (approximately 10%) are possible matches. There is no fixed response time to complete this last ten percent (10%). After all processing is completed, less than one percent of all cases submitted result in a confirmed match.

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

When a Positive response or unknown response is uploaded into CLAIMS3, CLAIMS4, or RAPS, the office with the pending application on which the name check request was based should receive a hard copy report. For positive responses it will be a Letterhead Memorandum (LHM) or a Third Agency Referral. For unknown responses, it may be a Letterhead Memorandum (LHM), Third Agency Referral, or a response to an expedited request which could be a "No Record" or a "Positive Response". An LHM typically has the FBI Letterhead at the top of the report. An LHM may be classified or unclassified, and provides USCIS with information from FBI's investigative files (information the FBI "owns").

#### i. Background

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

During the Name Check, CRS is searched for "main files", files where the name of an individual is the subject of an FBI investigation, and for "reference files", files where the name being searched is just mentioned in an investigation.

Instructor's notes: If an individual is referenced in an investigation, there may or may not be derogatory information relating to the individual. An individual could be referenced in an investigation for various reasons such as 1) the individual is of investigative interest to the FBI. For example, a referenced individual may have close ties to the main subject of an investigation but the FBI might not have enough derogatory information to make the individual into a main subject. OR 2) an individual could be mentioned as a neighbor, relative, employer with little to no additional information on that individual. For example, an individual could be listed in an investigation because he/she was interviewed as the neighbor or employer

*"Revised National Security Adjudication and Reporting Requirements", as of*

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

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

of the main subject.

February 4, 2008, signed by Michael Aytes, Associate Director, Domestic Operations.

ii. Responses

A. No Record

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

Instructor's notes: Positive responses result in LHMs or Third Agency Referrals.

LHMs

LE

LE

Third Agency Referral

LE

B. Positive Response

1. Indicates pertinent and/or derogatory information
2. Generates a hard copy report: Letterhead Memorandum (LHM) or Third Agency Referral
3. Must ensure that the information in the LHM relates to the applicant

LE

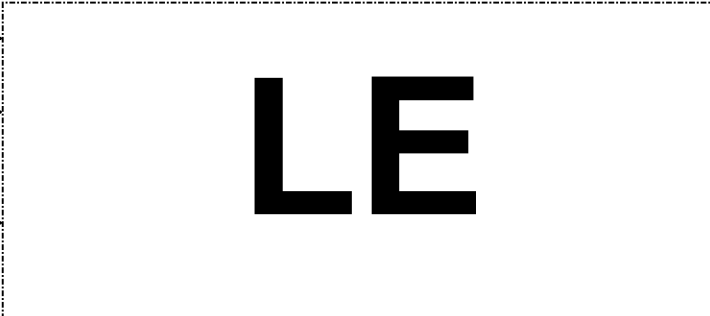
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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



LE

C. Unknown Response



1  
2  
3

LE

D. Pending Response

1. No adjudication unless pending over 180 days and otherwise approvable

Temporary and permanent residence  
(I-485, I-687, I-698)  
Waiver (I-601)

2. Must not schedule interview for N-400 applicant with pending response

Instructor's notes: Important policy memorandum relating to the FBI Name Check which are good resources for the students.

USCIS Operational Memoranda, "*FBI Name Check Process and Clarification for Domestic Operations*", dated December 21, 2006 answers many frequently asked questions regarding the FBI Name Check Process (e.g.

**Multiple Name Check Requests for the Same Application**

LE

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

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



**LE****Applicant's Date of Birth is Wrong in the System****LE**

*"Revised National Security Adjudication and Reporting Requirements"* dated February 4, 2008 allows for adjudication of certain applications if the name check has been pending for over 180 days and is otherwise approvable.

An interview should not be conducted on an N-400 application where the name check is pending due to section 336(b) of the INA which allows the applicant to request a hearing before a district court if there is a failure to make a determination under section 335 of the INA before the end of 120 day period after the date on which the examination is conducted. Previously, naturalization applicants were interviewed while their name check was pending. After 120 days, their name check remained pending and they were then eligible to file a lawsuit under section 336(b). See Memorandum entitled, "FDNS Processing of Positive FBI Responses to G-325 Name Checks, dated October 21, 2004.

## iii. Validity

- A. A definitive (No Record, Positive or Unknown Response) name check response is valid indefinitely for the application for which it was conducted.
- B. If a definitive name check response is used to support other applications, the name check response is only valid for 15 months from the FBI process date.

## iv. Indicators

Instructor's notes: The LHMs also have standard verbiage for the different classifications of investigations. The list of classifications of investigations, depending on the content of the LHM, are indicators of a NS concern.

LHM may likely involve a NS concern if the individual is the main or referenced in one or more of the following types of investigations or if the LHM includes language

**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).

that suggests an investigation of a similar nature:

- A.
- B.
- C.
- D.
- E.
- F.
- G.
- H.
- I.
- J.
- K.

**LE**

In some instances, a LHM may indicate that upon

**LE**

Instructor's notes: The LHM in the PowerPoint was obtained on the internet. It has been redacted from a secret document to an unclassified document and relates to Omar Al Bayoumi who allegedly assisted two of the 9/11 hijackers (Al-Hazmi and al-Mihdar) upon their arrival in the U.S.

The LHM is meant to be a sample and to illustrate the heading of LHMs and the portion markings. Ask the students what (U) stands for? Unclassified. Ask them what (S) stands for? Secret. What should they do if they have a secret document? Ensure they have the proper clearance, the document is properly marked, and properly stored.

Remind them that even if a tiny portion of a document is marked classified.

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

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

the whole document becomes classified.

b. FBI Fingerprint Check

i. Background

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

ii. Responses

Results are transmitted electronically in the Integrated Automated Fingerprint Identification Systems (IAFIS) to the FBI's Criminal Justice Information Services (CJIS) and returned electronically as one of the following:  
Non-IDENT, IDENT, Unclassifiable.

Instructor's note: A Non-IDENT response does not mean that the applicant was never arrested in the U.S. If the arresting agency does not provide the FBI with the fingerprints of the arrested individual, an IDENT response will not be returned from the FBI.

iii. Validity

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

iv. 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);

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

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

- D. Note: A criminal charge of “terroristic threats” is not necessarily an indicator of a NS concern. For example, the “terroristic threats” offense is often used by local prosecuting authorities to charge a domestic violence crime. A request for additional documents such as certified police reports or court dispositions may be required to determine if the charge or conviction is an indicator.

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

Furthermore, adjudications 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 cause substantial damage to property.

c. TECS/IBIS

See IBIS SOP dated March 1, 2006.

i. Background

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

ii. Responses

- A. **LE** – indicating possible ties/nexus to terrorism or other NS activity

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

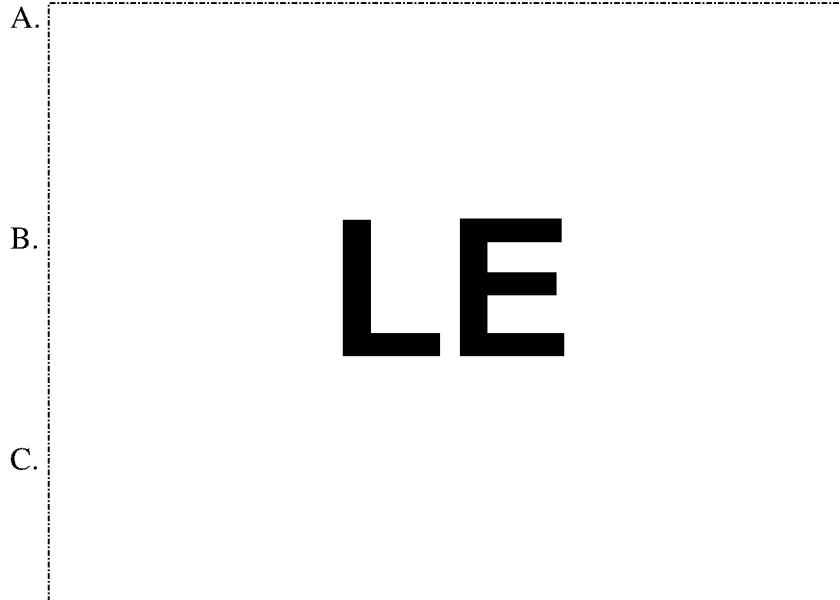
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

B. **LE** – e.g. Public Safety, Interpol

iii. Validity

Must be valid before a decision can be rendered on a benefit. An IBIS query is valid for 180 days.

iv. Indicators



D. The following hits are not considered indicators of a national security concern unless there is a specific Department of State (DOS) record or sub-record that identifies a national security concern

1. National Security Entry Exit Registration System (NSEERS)
2. The following “Visa Animals”:  
 Visa Mantis  
 Visa Bear  
 Visa Condor  
 Visa Donkey  
 Visa Eagle

Note: The “Visa Animals” refer to the DOS Security Advisory Opinion (SAO) clearance process, which is mandatory for DOS cases of name check-based hits, nationality-

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

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

E. Evaluate for articulable link:

1.

2.

3.

4.

**LE**

based requirements, or an alien's background and/or intentions while in the U.S. (See 9 DOS Foreign Affairs Manual Appendix G, 500)

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

**Instructor's Note:**

Lookouts noted in section E were determined not to be NS concerns by HQ USCIS. A USCIS memo issued on February 16, 2007, indicated that these hits by themselves did not require referral for NS vetting and resolution. This memo was rescinded. It is planned that the information will be specifically restated in the revision of the IBIS SOP (which will be much more expansive to cover other security checks as well). For the time being, the officers must apply the three prong test to determine if there is an NS concern. Most times there will not be an articulable link to NS activity because many of these are computer generated or targeting hits which result in secondary inspection, no derogatory information as a result of the inspection, and the person is admitted into the U.S.

**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).



d. 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:

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

Instructor's Note: Conduct 17 practical exercises to reinforce this EPO. The Instructor's answers to the practical exercises are found at the end of the lesson. Ask each time whether the example falls into the KST or non-KST NS concern category. Only #5 is a KST. All the others are non-KST NS 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).

## D. Initiating a Referral

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

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

Instructor's Note: Each office/service center has its own local standard operating procedures on how to refer a national security concern. Emphasize that if they are uncertain as to whether a case should be referred, they should consult with their supervisor and may request vetting assistance from HQFDNS.

### 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).





to the current criminal investigation)

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

Instructor's Note:  
FAQs

Can I ask what NS information the record owner has available? No. But in some instances, the LEA will share without you asking. That is OK.

What if there is no record owner? If there is NS information for which there is no record owner, USCIS should notify ICE of this information. Current procedure is by Request for Investigation (RFI). It might also be an instance where the Officer requests assistance for vetting from HQFDNS.

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

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

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

**A. Eligibility Assessment**

Instructor's note: Remind students that the eligibility assessment is stage 2 of the CARRP process and includes internal vetting activities.

When vetting and adjudicating cases with NS concerns, some may require minimal internal vetting because there is a legally sufficient ground of ineligibility which will not be easily overcome. Other cases will require that the full range of internal vetting activities be conducted to include multiple adjudicative activities (e.g. RFE, interview, re-interview). It is case-by-case. Officers must be flexible and communicate well with all interested parties (e.g. in Field Offices, the FDNS IO and the designated adjudicator will work very closely on these cases).

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

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

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

- ii. FDNS IOs do not adjudicate
- iii. For Overseas Offices, IO HQ

**B. Internal Vetting**

1. Prior to initiating internal vetting, consider:
  - a. Does the derogatory information relate to the subject?
    - i. Confirm identity.
    - ii. Do not assume that the information in the security check relates to your applicant.
  - b. Does the information in the referral meet the criteria for a NS concern?
    - i. If not, or if information comes to light that the concern no longer remains, the case may be returned to the routine adjudication process.
  - c. What types of systems checks should be run to support the determination for eligibility, admissibility, credibility?

Officers should 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. Attorneys
      - G. Suspected immigration fraud

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

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

- iii. 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
  
- 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

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

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

- C. Countries of interest
- D. Travel companions
- E. Taking money overseas for self or others
- F. Travel documents used
- G. Contacts

2. Internal Vetting: Systems Checks

Instructor's note: 1) Discuss the results that can be obtained from each system. 2) Advise that different results may appear depending on how you query and the different systems. 3) Remind that information that you get out is just as good as what was put in. 4) Facilitate discussion among officers so that they can share their knowledge and experience using the systems and describe what information they have found to be useful when running queries.

**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).

Officer does not have access to CCD. Note the memo from June 2008 entitled, "Access to the DOS' Consular Consolidated Database (CCD); Use of CCD Visa Data Safeguards Regarding Disclosure of Visa Data in Immigration Adjudications". Provides a thorough explanation of when information from CCD may be disclosed to the applicant or his/her representative.

CCD and the Text Search function.

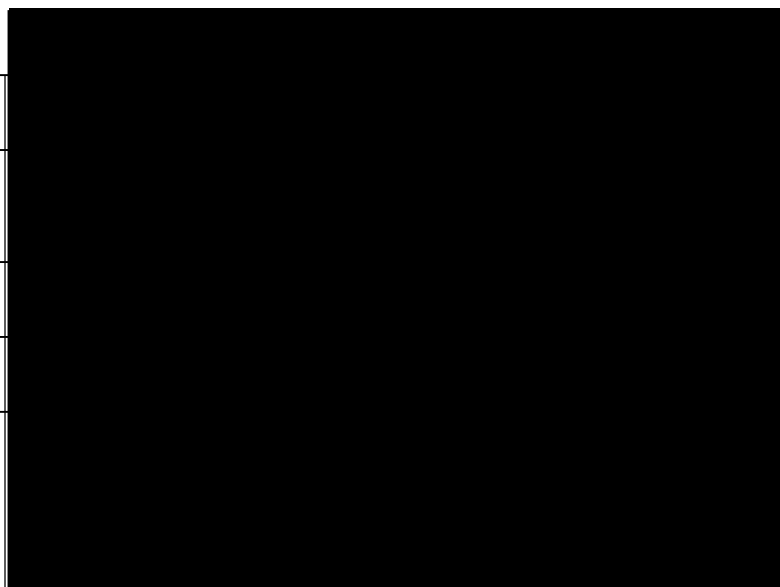
Gathering addresses of subject from open source (Zaba Search), commercial databases, CIS systems (old I-765 or H31s), and Afile (G-325, all previous applications) and run in FDNS-DS, SQAD, SCCLAIMS.

FDNS-Data System (FDNS-DS) USCIS System	Query people, organization, and addresses for fraud and NS links
National File Tracking System (NFTS) USCIS System	Search for unconsolidated A/T/Receipt files
Central Index System (CIS)	Search for unconsolidated A/T/Receipt files Search for Aliases
Computer Linked Application Information Management System (CLAIMS) 3 & 4 USCIS Systems	Obtain filings as beneficiary and petitioner Obtain addresses
<b>LE</b> TECS	<b>LE</b>
<b>LE</b> TECS	Due to NS concern
AVALANCHE	<b>LE</b>
<b>LE</b>	
Choicepoint/LEXISNEXIS Commercial Databases	Results of street addresses, businesses, & associates can be queried in FDNS-DS and in <b>LE</b>
Arrival and Departure Information System (ADIS)	Travel History

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

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

LE TECS
LE TECS
LE TECS
LE TECS
Consular Consolidated Database (CCD) Department of State System



<b>LE</b>	
ENFORCE	Query by name, FINS or Biometric information to obtain immigration violations
Image Storage Retrieval System (ISRS) USCIS System	Assists in determining identities (photo/fingerprint)
Benefits Biometric Support System (BBSS)	Assists in determining identities (results of fingerprint checks to include availability of RAP sheet)

<b>LE</b>	
AR11 Televue	Provides address changes submitted to USCIS on Form AR11
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)
Student and Exchange Visitor Information	Student status

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

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



System (SEVIS)	
Open source/Internet Queries	Google, Yahoo, Ask.com, Dogpile, Youtube, MySpace, LinkedIn, etc.

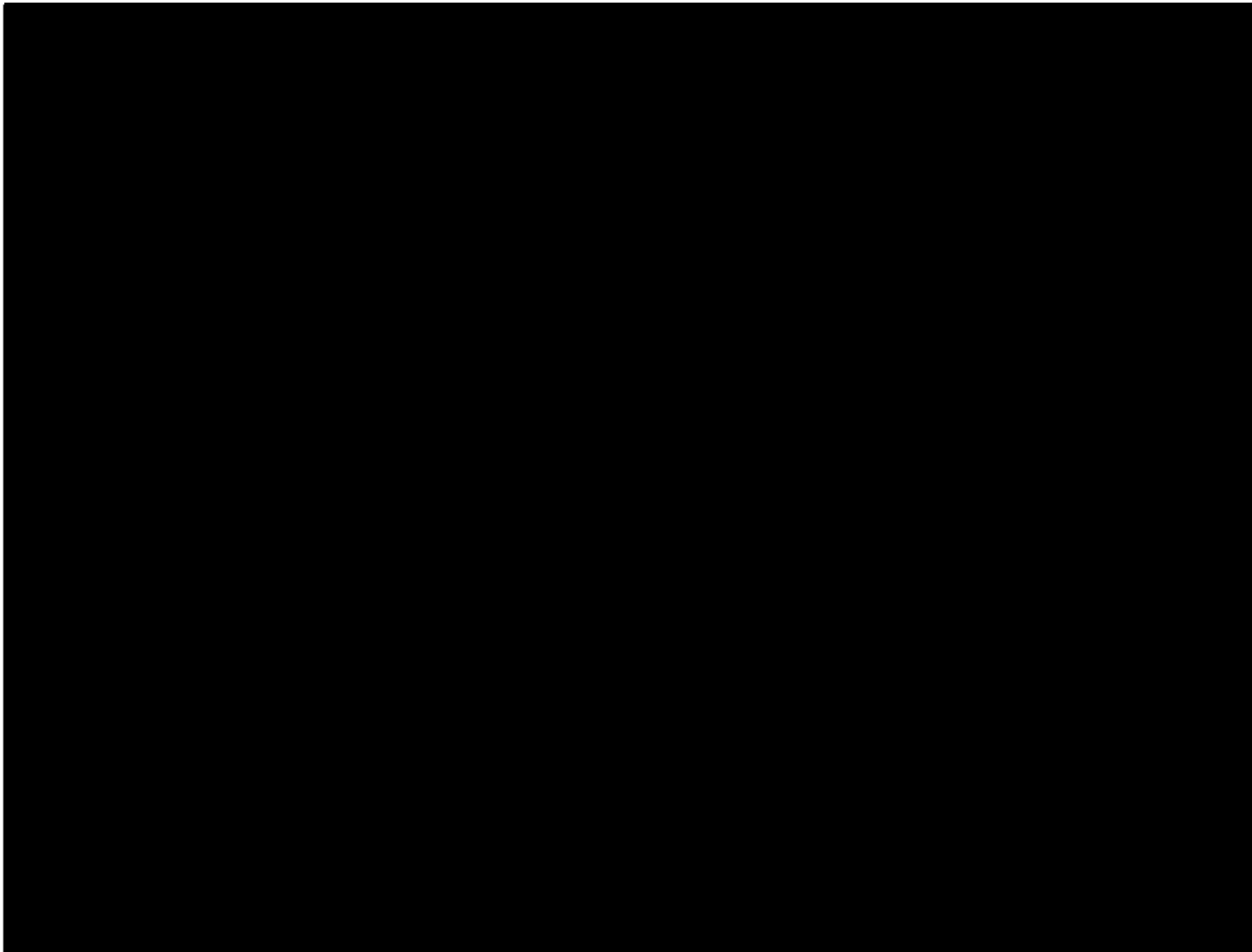
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

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

<http://dockets.justia.co>

**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).



o. USPER

- A. Citizens of the U.S.;
- B. Aliens lawfully admitted to the U.S. for permanent residence;
- C. Any unincorporated associations, a substantial of which are comprised of U.S. citizens or aliens lawfully admitted for permanent residence;
- D. U.S. corporations.

Foreign Intelligence  
Surveillance Act  
(FISA) of 1978, Title  
50 U.S.C. 1801

**Instructor's note:**

Students may encounter an LHM, TECS or NCIC record, 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).

report that indicates an individual or organization is a USPER.

Under the statute for Foreign Intelligence Surveillance Act (FISA) of 1978, Title 50 U.S.C. 1801 foreign power, agent of foreign power, and U.S. Person is defined. Permits law enforcement and intelligence agencies to domestically gather foreign intelligence information without requiring probable cause for a crime.

USPER would indicate that the individual may be fall into any of the four categories listed above and as defined in FISA. A USPER does not automatically mean the individual is US citizen and in some cases the individual may have been erroneously categorized as a USPER.

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

Instructor's note: Included in the slide show are two practical exercises/class discussion to illustrate how to use/consider information without disclosing it or knowledge of it.

"Consider" vs. "Disclose" Officers may "consider" or "use" sensitive and classified information as pointers to open source information or to create a line of inquiry for an interview but they must be extremely careful that the manner in which they "use" this information does not indicate that classified information is available and must under no circumstance disclose classified information.

"Disclose" refers to openly providing the information to the public such as during an interview or in a written decision. All Officers require permission from the originating agency to disclose third agency information to include law enforcement sensitive information. For classified information, there are additional requirements that will be discussed in EPO#8.

- i. Must have need to know And must have appropriate clearance for classified information
- ii. Construct parallel lead
- iii. Do NOT paraphrase
- iv. Do NOT compromise ongoing investigations or other interests by divulging knowledge of sensitive or classified information
- v. Do NOT compromise national security by disclosing classified information

**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).

- vi. Coordinate site visits, RFEs, and interview questions with appropriate agencies
- vii. Remember Third Agency Rule!

**Instructor's note: Third Agency Rule**

Records of other agencies either loaned to USCIS or a part of the USCIS files must be protected from unauthorized disclosure. 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.

Third agency information includes but is not limited to information resulting from security checks such as information provided by FBI, Department of State (DOS), U.S. Marshals Service (USMS), and Drug Enforcement Administration (DEA).

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

Contact Office of Security and Integrity (OSI) Personnel Security Customer Service at USCIS-OSI-PERSEC-Customer Service (in Outlook)

OR [REDACTED]@dhs.gov

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

#### 4. Documenting

- a. Outlines a set of facts that can be used to determine whether a national security concern exists, existed at one time but is no longer present or has not yet been eliminated to the satisfaction of the investigating agency.
- b. Provides a record of the status and results of security and systems checks, as well as results of inquiries to and responses from offices within USCIS, components within DHS and external agencies which provides information relevant to USCIS' determination of eligibility.
- c. Results of vetting and deconfliction must be documented in the designated worksheet(s) on the non- record side (right-side) of the file and in the appropriate tabs of FDNS-DS.
- d. No classified information can be entered into the designated worksheet(s) or FDNS-DS.

**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).

**Instructor's note:**

Be careful what you put in emails...they travel fast and to people you didn't intend.

Do not write CIA in emails or discuss on phone. Very sensitive information if not classified. Refer as OGA if must.

Do not write case agent, contact information in emails along with individual's names.

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

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

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

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

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

**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).

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

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

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

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

### **A. External Vetting Overview**

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

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

Instructor's Note: During the process of external vetting of Non-KSTs, the Vetting Officer must seek to obtain additional information that may be relevant to a determination of eligibility. Officers should note that actions that do not meet the threshold for criminal prosecution (e.g., indicators of fraud, foreign travel, and information concerning employment or family relationships) may be relevant to a benefit determination. The Officer must make every effort to clearly articulate these facts or fact patterns for final adjudication.

1. Preparation for Non-KST External Vetting
  - a. Be familiar with the individual's immigration status, pending applications
  - b. Be familiar to the extent the information is available (e.g.

#### **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).

results of IBIS hit);

- c. Develop lines of inquiry for case discussion with record owner

d.

**LE**

## 2. Outreach

- a. Be aware that the outside agency may not know who USCIS is or understand what USCIS does
- b. Be prepared to explain in layperson's terms why you are calling
- c. Avoid using immigration jargon when discussing the immigration history of the individual
- d. Elicit information regarding the nature of the concern, the extent of the concern, and the status of the investigation
- e. Ascertain from the outside agency any information that may affect the individual's eligibility for the benefit sought

f.

**LE**

g.

- h. Explain that evidence which may not support a criminal indictment or conviction may be legally sufficient to sustain a denial under immigration law.
- i. Be mindful that the information may be classified and if not it is likely Law Enforcement Sensitive and labeled FOUO or Sensitive but Unclassified (SBU).
- j. If classified information must be transmitted, the classified information must be transmitted over secure means such as over secure phone or fax.
- k. Remember that transporting classified information requires special permission and requirements as does mailing classified.

USCIS Office of  
Security & Integrity  
intranet site.

<http://osi.uscis.dhs.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).



Instructor's Note: The Officer must have a need to know for access to the FOUO or SBU information and must have a need to know AND the proper clearance for access to classified information.

Section 291 of the INA states in pertinent part, "Whenever any person makes application for a visa or any other document required for entry, or makes application for admission, or otherwise attempts to enter the United States, the burden of proof shall be upon such person to establish that he is eligible to receive such visa or such document, or is not inadmissible under any provision of this Act, and, if an alien, that he is entitled to the nonimmigrant, immigrant, special immigrant, immediate relative, or refugee status claimed, as the case may be."

### 3. Considerations for Information Sharing and Confidentiality

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

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

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

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

Instructor's Note: Much of the information contained in USCIS systems and

#### 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).

files is confidential and the disclosure and use of the information is governed by laws and regulations relating to sensitive but unclassified (i.e., For Official Use Only and/or Law Enforcement Sensitive (FOUO/LES)) information.

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

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

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

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

b. Confidentiality Provisions

- i. Sections 210 and 245A of the Immigration and Nationality Act limit the use and disclosure of information provided by “amnesty” applicants under the 1986 Immigration Reform and Control Act.
- ii. Section 384 of the 1996 Illegal Immigration Reform and Immigrant Responsibility Act, as amended, 8 U.S.C. 1367, limits the use and disclosure of information relating to aliens seeking protection under the Violence Against Women Act (VAWA), as amended, or as T or U non-immigrants.
- iii. Under 8 C.F.R. § 208.6, information regarding an individual’s status as an asylum seeker or asylee, information contained in or pertaining to his or her application, and records pertaining to any credible

See Memorandum entitled “Confidentiality of Asylum Applications and Overseas

**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).

fear or reasonable fear determination generally must not be disclosed without the written consent of the applicant or a waiver from the Secretary of DHS. By policy, the confidentiality provisions of 8 C.F.R. § 208.6 have been extended to information contained in or pertaining to refugee applications.

Verification of Documents and Application Information” dated June 21, 2001 and Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants dated June 3, 2005

c. Records Sharing

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

The Record Handbook can be found on the DHSONLINE Portal, at the USCIS Office of Records Services website:

[http://ors.uscis.dhs.gov/pol\\_imp/roh/index.htm](http://ors.uscis.dhs.gov/pol_imp/roh/index.htm)

m.  
1

4. Other Considerations when Externally Vetting Non-KSTs

- a. Understand the importance to law enforcement agencies of the chain of custody of evidence in criminal proceedings.
- b. Be aware that agencies post hits in TECS for a variety of reasons. The objective of the conversation with the record owner is to determine if the reason the hit was posted was based on an articulable concern.
  - i. Gather information and evidence for criminal prosecution
  - ii. Informational and historical purposes
  - iii. Intelligence collection which may support investigative initiatives or may be for targeting or pattern analysis.

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

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

## c. Note-taking

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

## 5. Liaisons with DHS Components

- a. In accordance with DHS policy, all DHS components are considered one agency. Information from these components is oftentimes "Law Enforcement Sensitive" and must be protected regardless.
- b. All DHS components are considered part of one "agency" for purposes of the Privacy Act 5 U.S.C. § 552a(a)(1), (b)(1).
- c. No DHS component should consider another DHS component to be a separate agency for information-sharing purposes.
- d. Absent any legal prohibitions as set forth by the Department's General Counsel, information shall be shared within DHS whenever the requesting officer or employee has an authorized purpose for accessing the information in the performance of his or her duties, possesses the requisite security clearance, and assures adequate safeguarding and protection of the information.
- e. From this point forward, information-access and -sharing agreements with outside entities will be negotiated and entered into on behalf of the Department as a whole, not on behalf of an individual DHS component.
  - U.S. Secret Service (USSS)
  - U.S. Coast Guard
  - U.S. Immigration and Customs Enforcement (ICE)
  - U.S. Customs and Border Protection (CBP)
  - Transportation Security Administration (TSA)

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

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

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

- U.S. Citizenship and Immigration Services (CIS)
- Federal Emergency Management (FEMA)
- Directorate for National Protection Programs
- Directorate for Science and Technology
- Directorate for Management
- Office of Policy
- Office of Health Affairs
- Office of Operations Coordination
- Office of Intelligence and Analysis
- Federal Law Enforcement Training Center (FLETC)
- Domestic Nuclear Detection Office

#### 6. Liaison with CBP's National Targeting Center (NTC)

Instructor's note: Advise students that each office has its own policy on who is responsible for conducting an IBIS query and who is responsible for resolving an IBIS hit. Service Centers often rely on the BCU to resolve IBIS hits and some field offices have IBIS Triage Units to resolve IBIS hits.

NTC enters different types of lookouts. The lookout may specify that CBP officers are required to contact NTC, regardless, when lookouts indicate contact with the NTC, the USCIS officer will first determine if it is a **LE** or **D/PLE** lookout, if so, TSC must be notified. If it is not a **LE** lookout, the USCIS Officer will follow the below instructions regarding NTC lookouts.

- a. Established on October 22, 2001.
- b. 24/7 operation with the centralized mission of coordinating anti-terrorism targeting and supporting all CBP Anti-Terrorism activities.
- c. Supports and responds to inquiries from the field, conducts tactical targeting to identify actionable targets, develops Automated Targeting System (ATS) rules, and supports Intelligence Driven Special Operations (IDSO).
- d. All Terrorist Watch list encounters by CBP are processed through the NTC.

#### **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).



Palm Beach, Florida; Bloomington, Indiana; Covington, Kentucky; Portland, Maine; Grand Rapids, Michigan; Helena, Montana; Erie, Pennsylvania; Providence, Rhode Island; Midland, Lubbock, and Plano, Texas; and Everett, Washington. **How do these JTTFs coordinate their efforts?** Largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs.

- a. JTTF was established in the 1980s.
- b. The FBI is the lead agency for terrorism investigations and the JTTFs.
- c. JTTFs serve three main purposes:
  - i. prevent terrorist attacks;
  - ii. respond to and investigate terrorist incidents or terrorist-related activity; and
  - iii. identify and investigate domestic and foreign terrorist groups and individuals targeting or operating within the U.S.
- d. The National JTTF (N-JTTF) located at FBI headquarters, includes representatives from a number of other agencies.
- e. The task forces are composed of federal, state, local agencies and are located in over 100 locations throughout the U.S.
- f. USCIS liaises with JTTF through the ICE representative on JTTF. The following list of agencies are full-time members of JTTFs:
  - Air Force Office of Special Investigations (AFOSI)
  - Bureau of Alcohol, Tobacco, and Firearms (ATF)
  - Central Intelligence Agency (CIA)
  - Customs and Border Protection (CBP)
  - Defense Criminal Investigative Service
  - Department of Interior's Bureau of Land Management
  - Diplomatic Security Service (DSS) (within DOS)
  - Federal Protective Service (FPS) (within ICE)
  - Immigration and Customs Enforcement (ICE)
  - Internal Revenue Service (IRS)

**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).

- Naval Criminal Investigative Service (NCIS)
- Postal Inspection Service
- Treasury Inspector General for Tax Administration
- U.S. Border Patrol (within CBP)
- U.S. Park Police
- U.S. Army
- U.S. Marshall Service (USMS)
- U.S. Secret Service (USSS)

Instructor's note: Officers should note that DHS has full-time members from ICE, CBP/Border Patrol, FPS, USSS

**LE**

**LE**

**LE**

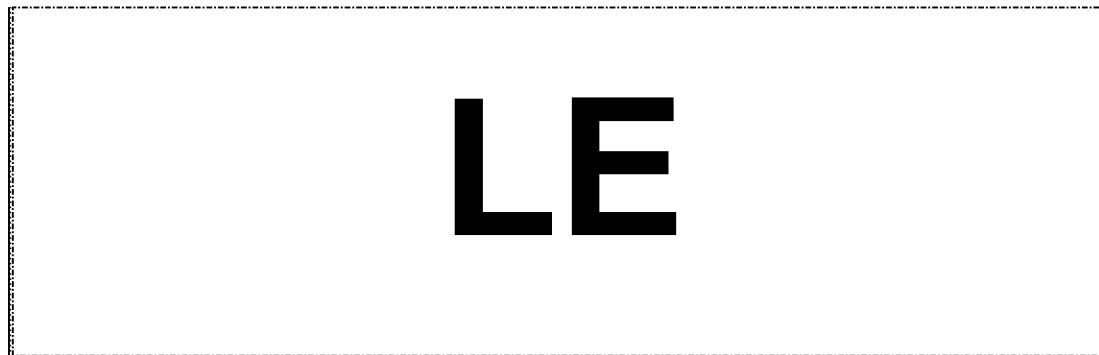
**LE** Remember that LEAs conducting an investigation are trying to obtain evidence that will be admissible to court and prove that a crime has been committed.

**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).





**C. External Vetting Decision Criteria**

Instructor's note: The vetting decision criteria is found only in the Domestic Ops Operational Guidance and is being presented considering the majority of the FDNS class falls under DomOps.

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

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

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

- a.
  - b.
  - c.
  - d.
  - e.
- 

**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).

- f.
- g.
- h.
- i.
- j.
- k.
- l.
- m.

**LE**

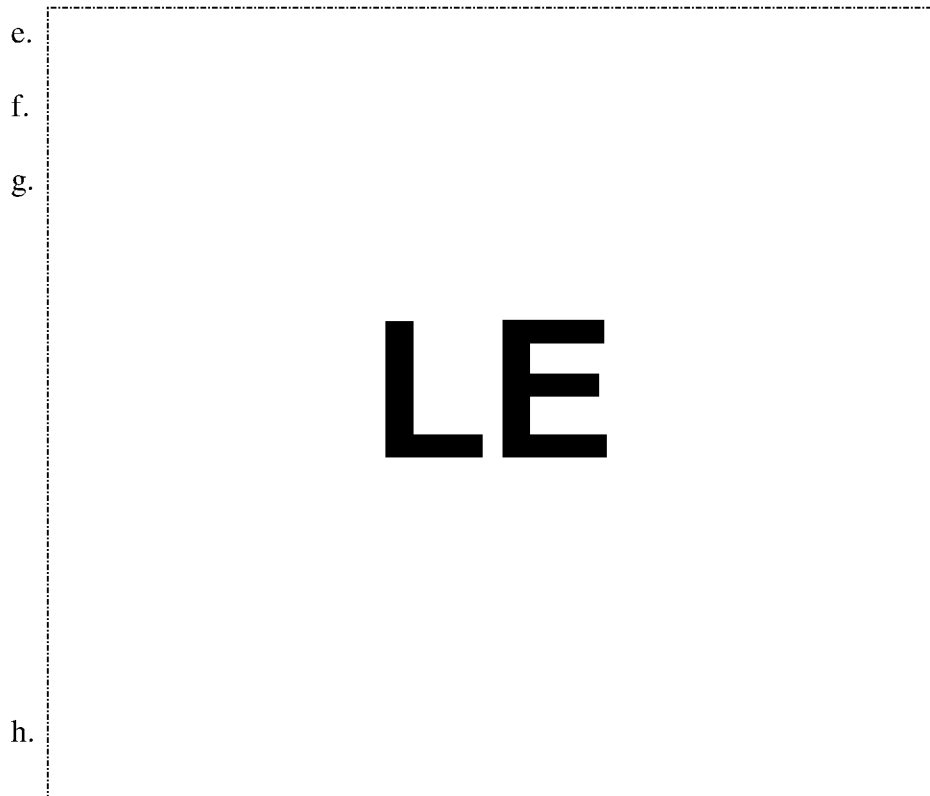
2. A National Security determination should be made if results of the external vetting fall into one or more of the following categories:

- a.
- b.
- c.
- d.

**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).



#### D. Request for Assistance to HQFDNS

Instructor's note: Operational questions should not come to HQFDNS but should go through the appropriate component's chain.

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

##### 1. General Types of Requests

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

#### **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).

- j. Assistance for declassification/use of classified information

## 2. Method of Request

- a. Update FDNS-DS AND designated worksheet(s)
- b. Send to [REDACTED]
- c. Ensure email is marked with "For Official Use Only" (FOUO) caveat
- d. Include the following information in the body of the email:
  - i. Subject: Request for Assistance (Vetting) or Request for Assistance (Adjudication)
  - ii. Full Name (Applicant, Petitioner, Beneficiary, Derivative or Company)
  - iii. A-Number
  - iv. Pending Application(s) and/or Petition(s) Form Type(s)
  - v. Nature of assistance requested
  - vi. Requesting Officer and Contact Information
  - vii. FDNS-DS NS Hit/Case #
  - viii. Litigation Case information if relevant\*

## 3. Intelligence Community (IC)

Requests for information from the intelligence community should be routed to HQFDNS.

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

Instructor's note: If the field requests KST external vetting (requires that a complete eligibility assessment including internal vetting has been completed, and the appropriate supervisory and senior level concurrence has been obtained), HQFDNS may conduct high side checks as part of KST external vetting or other requests for assistance.

This section explains some of the systems available to HQFDNS. These are classified systems which may result in unclassified and/or classified results. HQFDNS will review the results and provide an assessment to the field.

- a. High Side Checks

### 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).

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

i.



LE

- ii. TIDE (Terrorist Identities Datamart Environment)
- A. U.S. government central repository of information on international terrorist identities.
  - B. Includes all information the United States has related to individuals known or suspected to have been involved in international terrorism.

iii.



LE

b. Executive Order 12333

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

c. Executive Order 13354

**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).

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

d. Members of the IC include:

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

**Instructor's note: Practical Exercise for External Vetting**

Students should assume that an eligibility assessment has already been completed (to include external vetting) and that there is no additional derogatory information that was obtained during the systems checks. Instructor should ask based on scenario,

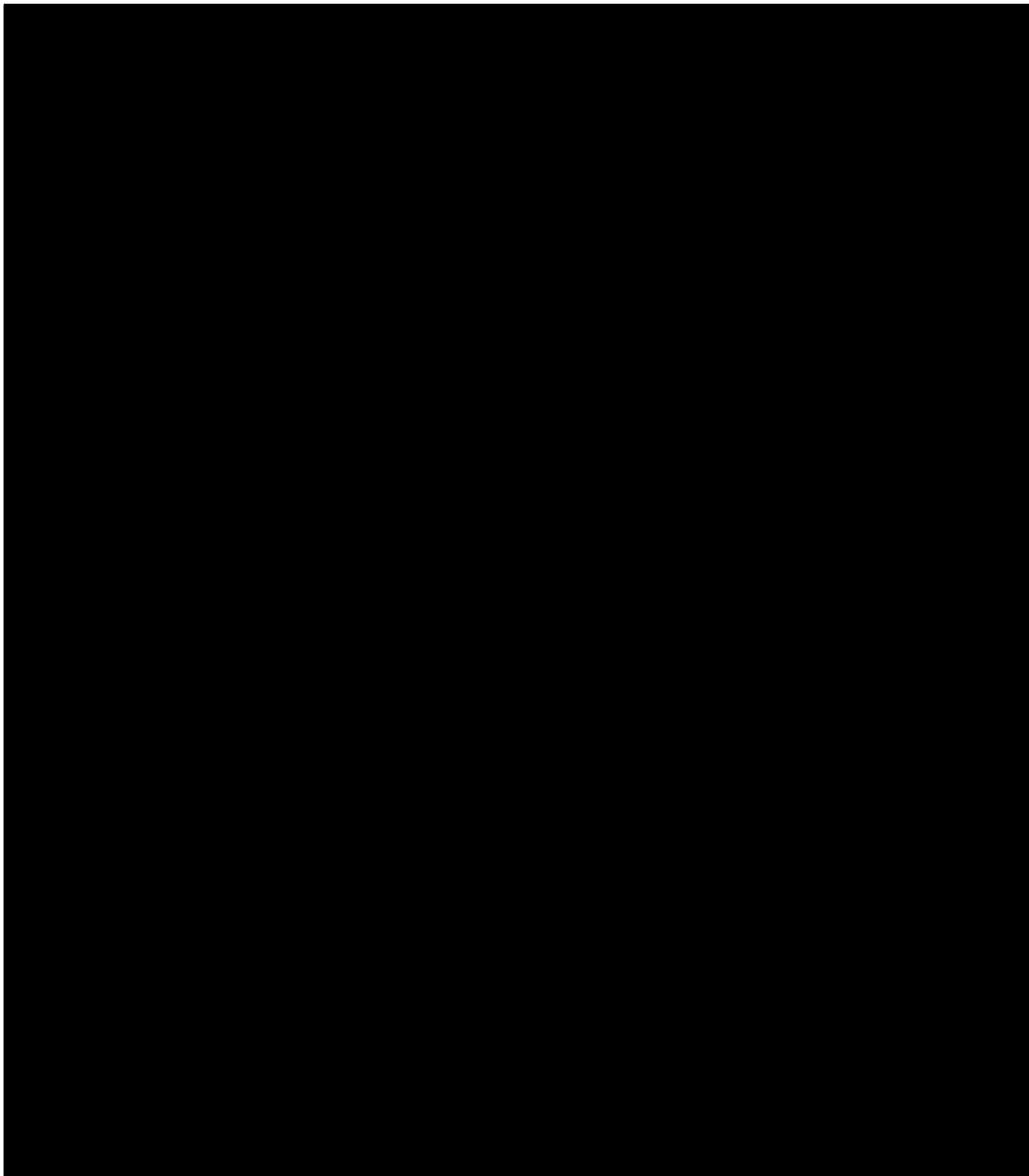
1-Identify the NS indicators and do rise to level of NS concern

2-Determine what internal vetting steps should have been taken

3-Determine if there is enough information to determine whether the NS concern has been resolved or the NS concern remains

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

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

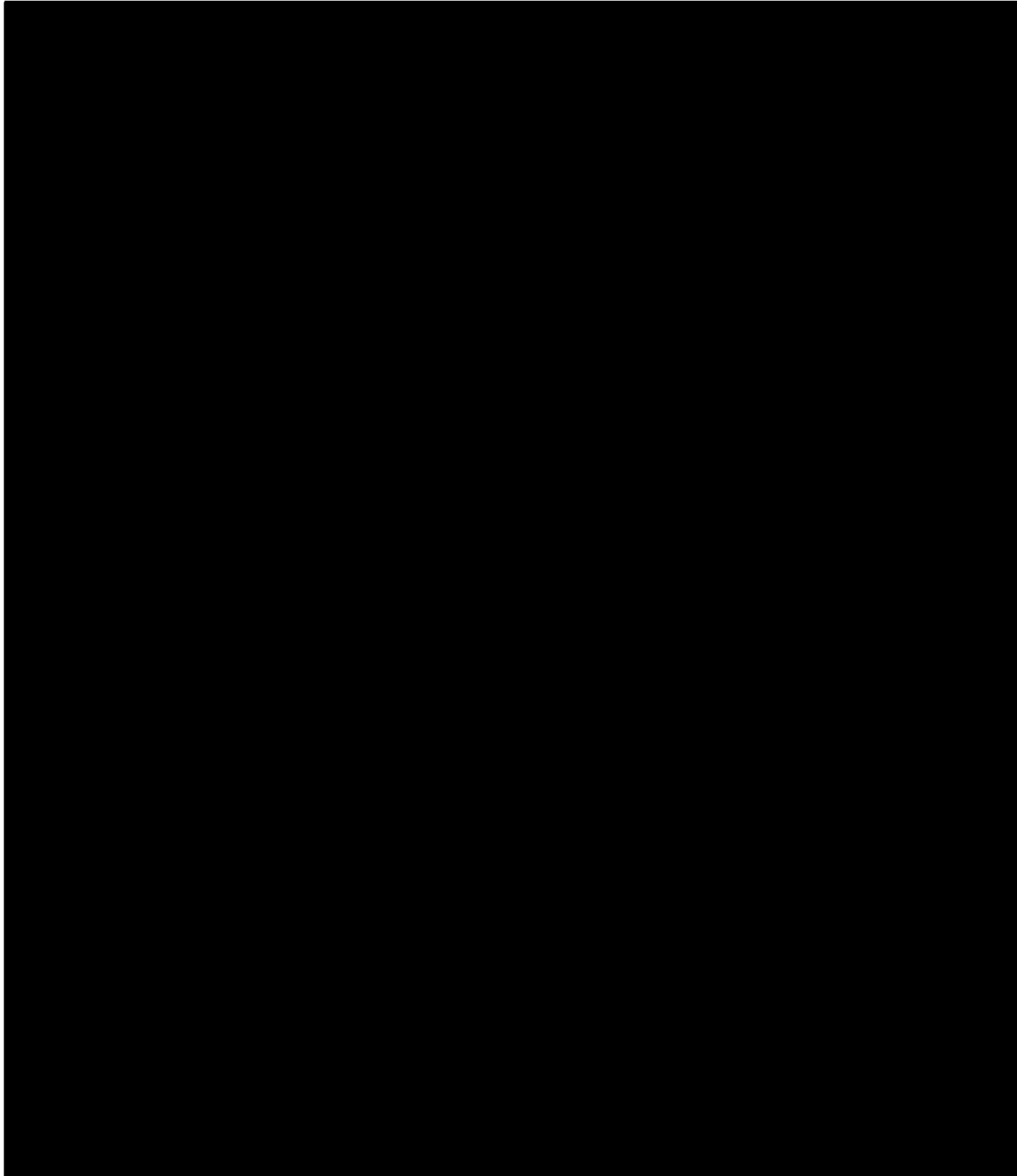


**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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

**USCIS  
NATIONAL SECURITY**

**93  
August 2008**



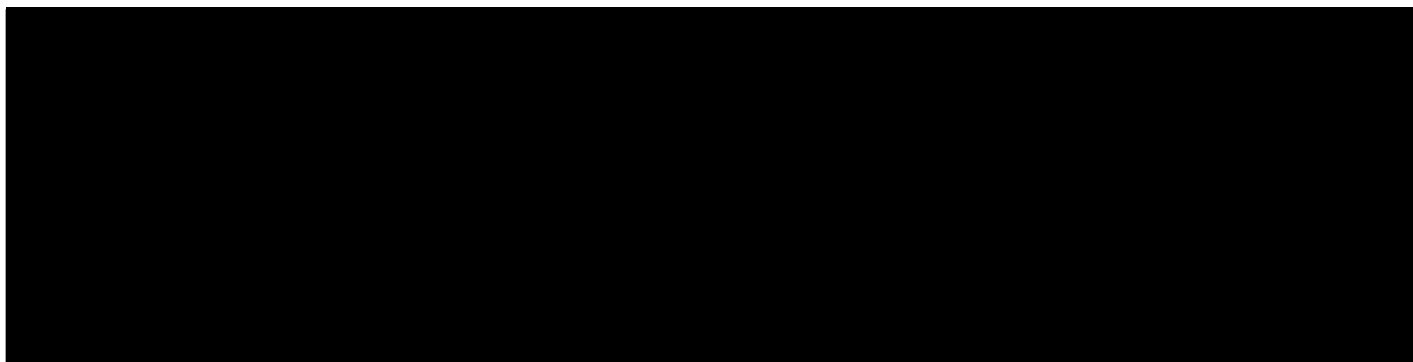
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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

**USCIS  
NATIONAL SECURITY**

**94  
August 2008**





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

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

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

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

Instructor's 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.

Adjudications Officers reviewing cases involving national security concerns must:

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

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

1. Ensure that if the file or a document is classified, the Officer has a "need to know" and the appropriate clearance to review the classified material. Ensure that the classified material is appropriately marked and properly stored.
2. Notify local USCIS Office of Chief Counsel (OCC) attorney if the

**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).

case is in litigation and determine due dates.

3. Check Central Index System and NFTS for relating files and charge file to Officer.
4. Check FDNS-DS to ensure case is up-to-date. Update adjudicative activities regularly in FDNS-DS.
5. Review the information gathered during internal vetting (and external vetting, if applicable) to understand the actions that have been taken. Review the designated worksheet(s) and any older versions of the national security document such as National Security Record (NSR), Case Resolution Record (CRR), the National Security Notification (NSN), the Significant Incident Report (SIR), and any other IBIS resolution forms.
6. Review file completely which includes ensuring that the required security checks (IBIS, FBI Fingerprint, FBI Name Check, IDENT/USVISIT for asylum cases) are complete and valid.
7. Establish a detailed timeline of the subject's immigration history, noting any and all discrepancies.
8. Verify the authenticity of documents and information provided by the subject with the Department of State (DOS) via DOS Reciprocity Tables, CCD, official request to DOS consular office where the subject and family members were born, lived, attended school, etc.
9. Perform open source searches and print out pertinent information.
10. Look for consistency in testimony and documentation to establish credibility. If there are inconsistencies, follow up questions or a Request for Evidence (RFE) may be required to explain the inconsistencies. The answers to the questions or RFE will assist the officer to make a credibility finding and determine how a negative finding of credibility may impact the eligibility for the benefit sought, as it relates to USCIS discretionary authority or Good Moral Character.
11. Clearly document changes made to the application or petition during the interview. Clearly note inconsistencies or irregularities as well as

**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).

responses to follow up questions relating to the inconsistencies or irregularities on the Adjudicator's Worksheet, in a Memorandum to File or in a sworn statement.

12. Formulate adjudication strategy and discuss with management, OCC and/or NSAU/HQFDNS, as appropriate.
13. Prepare a detailed line of inquiry for interview and/or RFE, Notice of Intent to Deny (NOID) or Notice of Intent to Terminate (NOIT).
14. Deconflict with law enforcement prior to interview or issuance of RFE, NOID, NOIT.
15. Interview or issue RFE, NOID, NOIT. In certain instances, the interview may be audio or video taped.
16. Draft decision. Among considerations when drafting are questions regarding who will sign the decision, legal sufficiency and anticipated court activity.
17. Deconflict with law enforcement prior to final decision.
18. Obtain supervisory concurrence for final decision and update designated worksheet(s).
19. Issue decision.
20. Issue Notice to Appear (NTA), if appropriate. Coordinate with law enforcement agency, OCC, and ICE Counsel.

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

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

1. Inadmissibility for Willful Misrepresentation or Fraud
  - a. An alien who either by fraud or willfully misrepresenting a material fact seeks to procure a visa, documentation, or admission into the United States or for any other immigration

#### **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).

benefit is inadmissible Section 212(a)(6)(C)(i) of the INA.

- b. Does not need to be under oath
  - c. Does not matter if given orally or in writing
  - d. Material fact is information that is necessary for the alien to be eligible for the benefit
  - e. Examples
    - i. Submitting a fraudulent birth certificate to establish a mother/daughter relationship for Form I-130, Petition for Alien Relative
    - ii. Using a fraudulent passport at time of entry
    - iii. Submitting fraudulent employment history to obtain an employment visa
  - f. Remember and consider the alien may be eligible to apply for a waiver of this inadmissibility under section 212(i).
2. Good Moral Character (GMC)

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

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

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

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

*In short:*

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

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

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

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

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

See 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.

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

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

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

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

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

#### **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).

Department.

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

## E. Federal Litigation

### 1. 336(b) Actions

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

### 2. Mandamus

- a. May be filed on any type of application or petition with federal court
- b. USCIS maintains jurisdiction
- c. The court will issue instructions to USCIS and other agencies to complete certain tasks within certain timeframes. For instance, a court may order the FBI to complete the FBI Name Check request within 45 days of the court's order with USCIS instructed to adjudicate the application within 45 days of the completion of name check.

### 3. Vetting and/or Adjudications Officer's Role

- a. Notify USCIS counsel and supervisor of litigation.
- b. Inquire about the next court deadline and expectations.
- c. Know the case and next steps.
- d. Don't make promises that cannot be kept. Be extremely frank with USCIS Counsel regarding issues, obstacles.
- e. Notify USCIS Counsel if USCIS cannot meet deadlines. It is better to ask for an extension than to be found in contempt of court.
- f. Anticipate court actions and respond appropriately
- g. Notify USCIS Counsel of contemplated actions (e.g. site visit, interview, RFE, decision). In some Federal Circuits, concurrent jurisdiction is observed – effectively giving USCIS the opportunity to interview and request evidence from an

#### **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).

applicant while the case is subject to court action. In other Circuits, courts hold that they have exclusive jurisdiction and that USCIS cannot take any action without the permission of the court, either through a remand or specific instructions.

- h. Know local basic court procedures.
  - i. Maintain custody of file, copy for USCIS counsel.
4. USCIS Office of Chief Counsel (OCC)
- a. Represents USCIS' interests.
  - b. Liaison between USCIS (e.g. Adjudications or Vetting Officer) and Assistant U.S. Attorney
  - c. USCIS Counsel works with the AUSA to address court inquiries and should notify the AUSA of any intended action.
  - d. Coordinates appropriate information-sharing activities with the AUSA and will identify appropriate parties to the discussion.
5. Assistant U.S. Attorney (AUSA)
- a. Represents USCIS in Federal Court
  - b. Employed by the Department of Justice
  - c. Familiar with court procedures and the preferences of individual judges.
  - d. May offer advice regarding decisions, to include review of the decision to determine legal sufficiency and/or risk of bad case law
  - e. Generally not very knowledgeable of immigration law
  - f. Third Agency rule prohibits the disclosure to the AUSA of any law enforcement sensitive information in the possession of USCIS which originated with another agency, unless that source agency has consented to such a disclosure to the AUSA.

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

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



## IV. APPLICATION

### A. In-Class Exercises

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

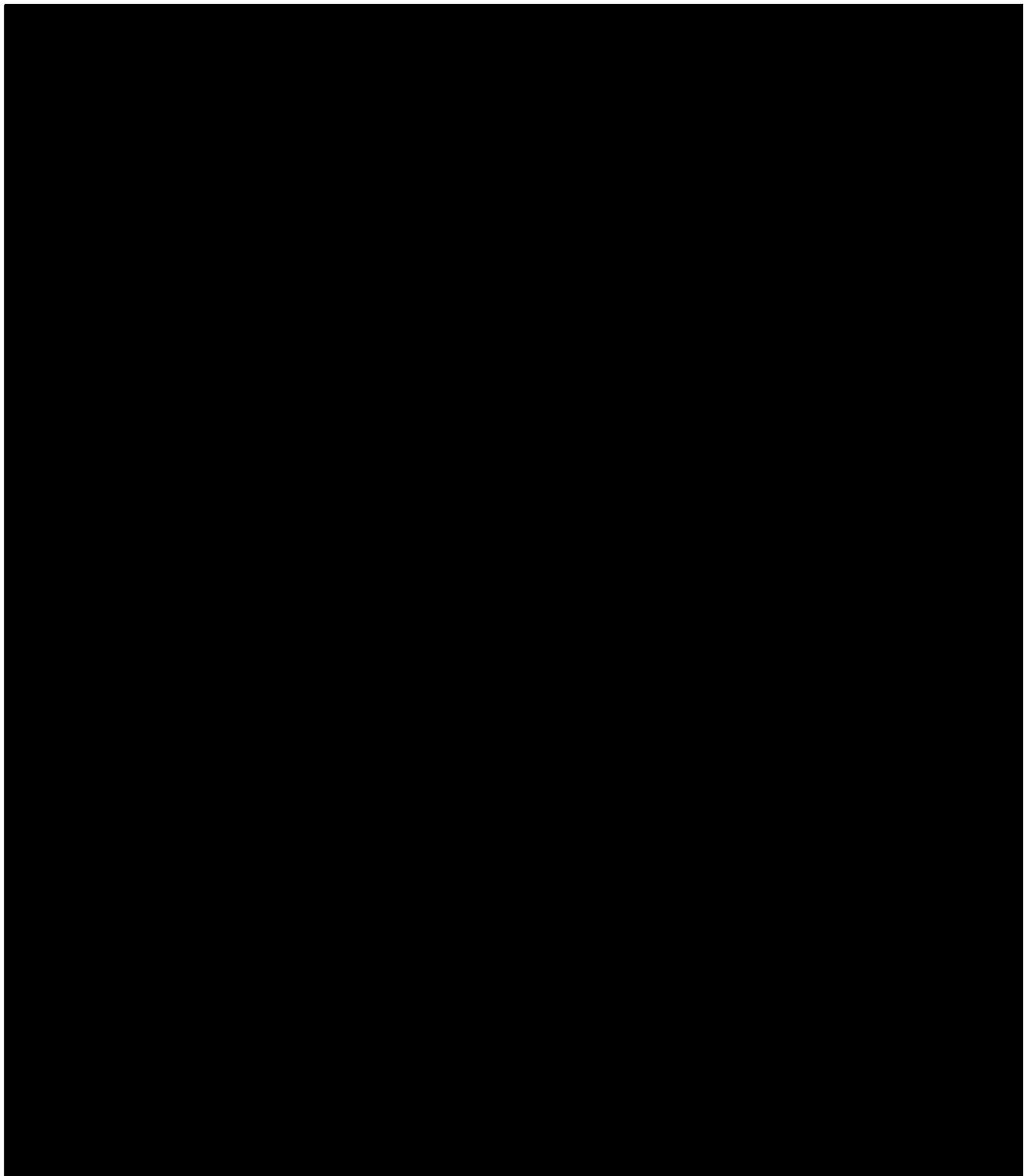
Instructor's Note: Once an NS indicator has been identified, which officer establishes the articulable link will depend on each individual office. Students should be most familiar with identifying NS indicators, realizing in some situations they might discover an indicator right before or in the middle of the interview. The discussion about the articulable links to NS Activity should give the students an idea of how the designated officer determines if there is a link.

Reminds students that what is identified initially as a NS concern, after further review of case/systems checks/discussion with record owner, may result in Not NS. That determination will be made by the designated officer and entered in to the designated worksheet(s).

The scenarios with answers & explanations (**in bold**) follow:

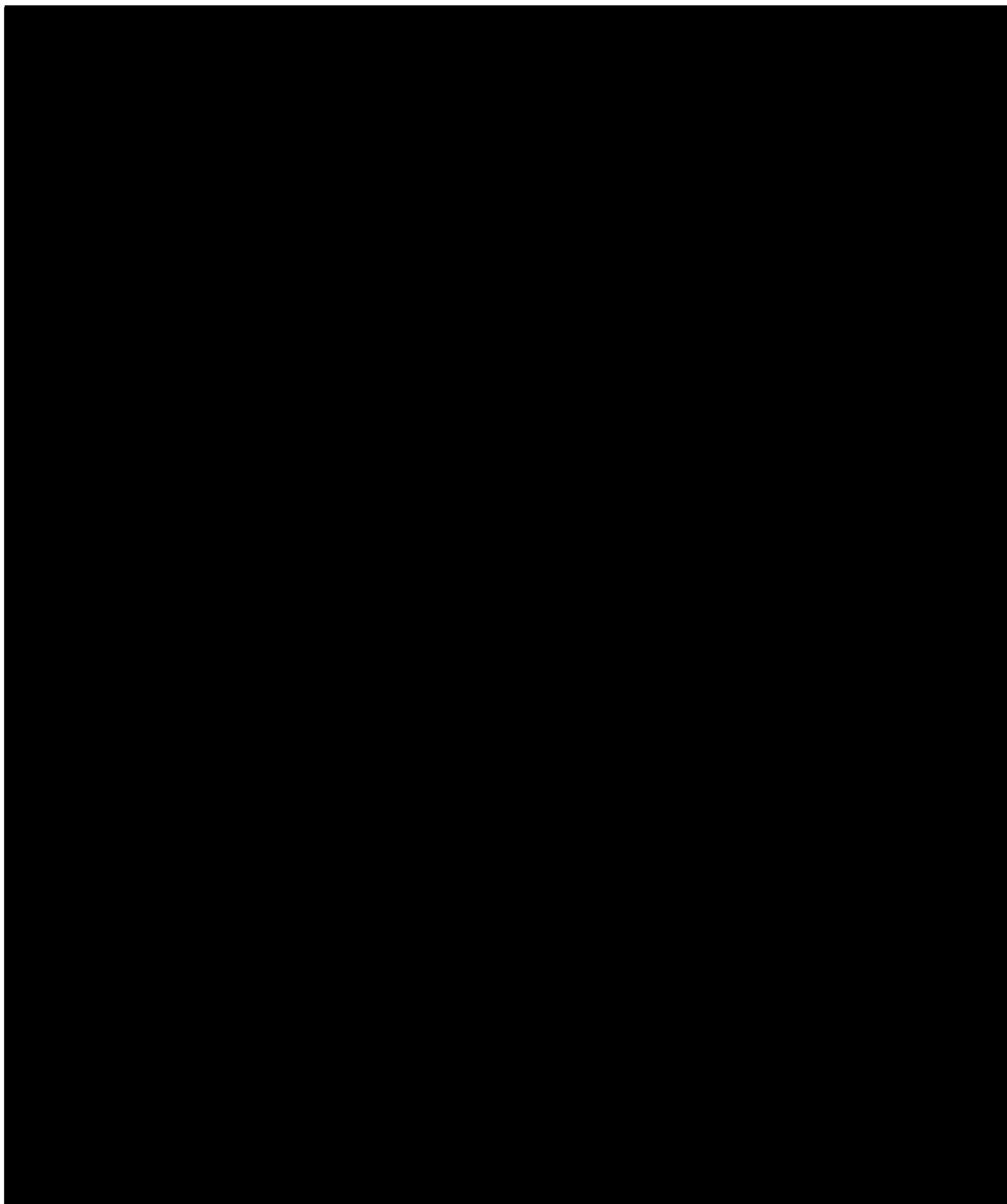
**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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



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

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

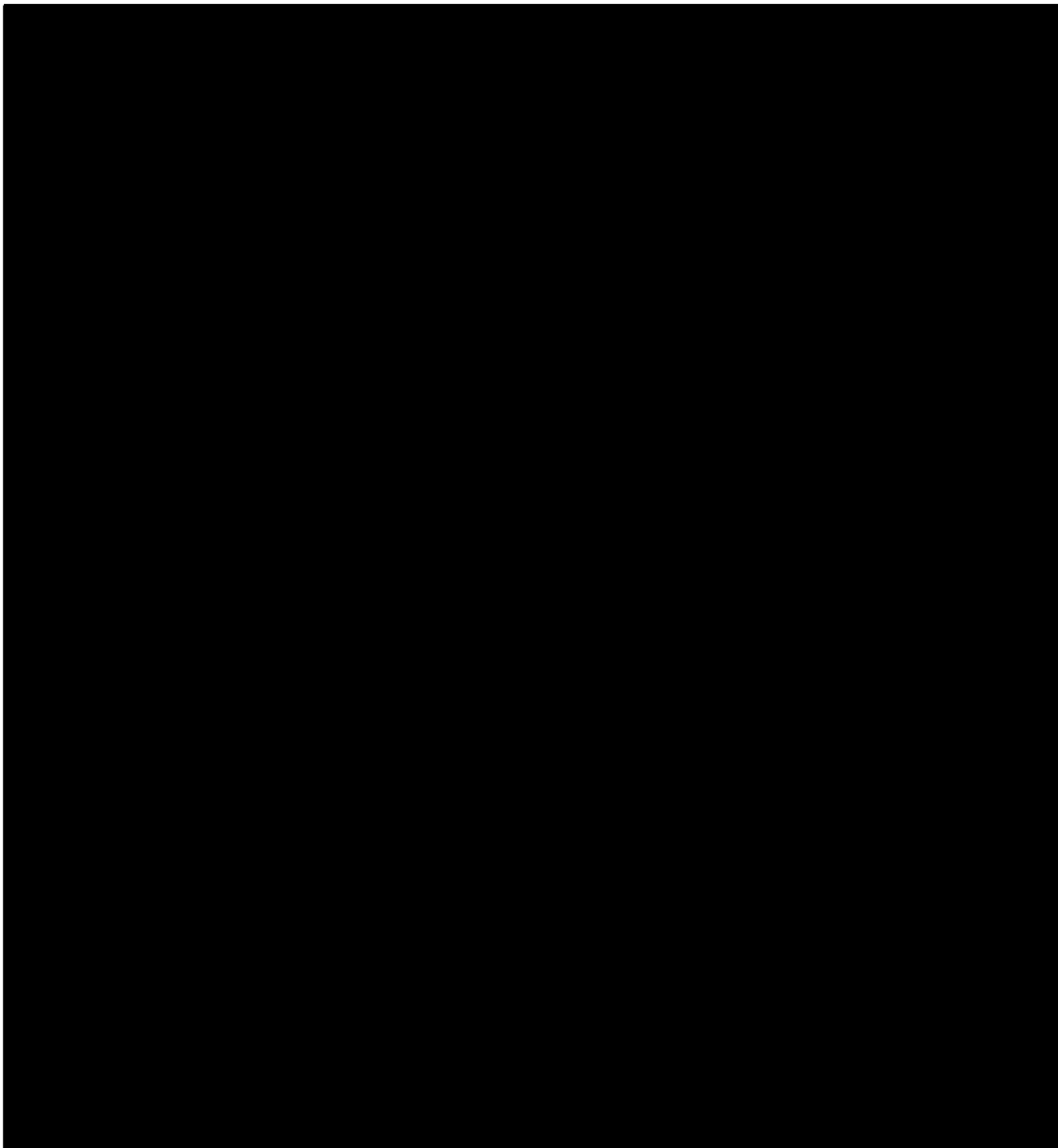


**FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE**

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

**USCIS  
NATIONAL SECURITY**

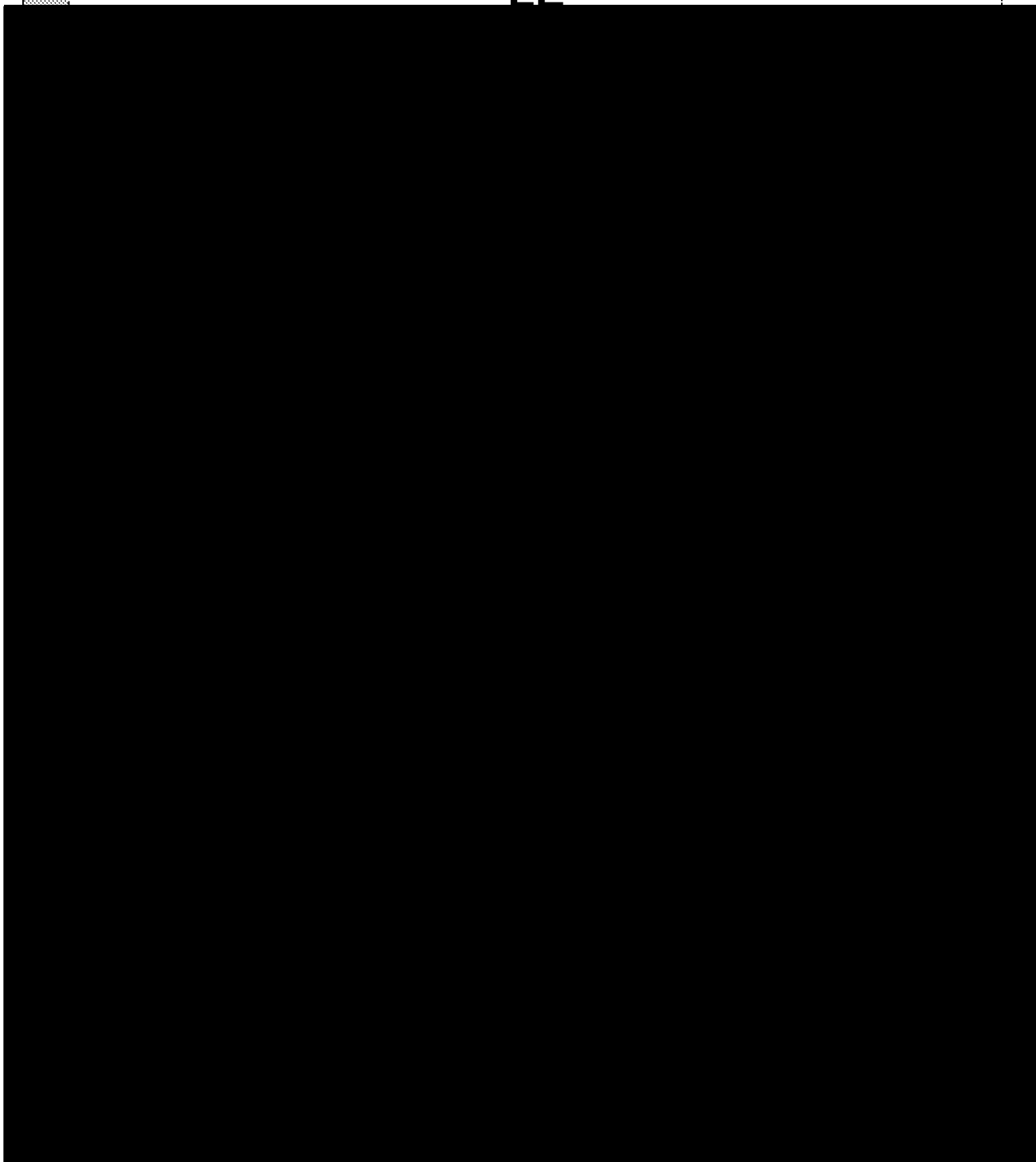
**105  
August 2008**



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

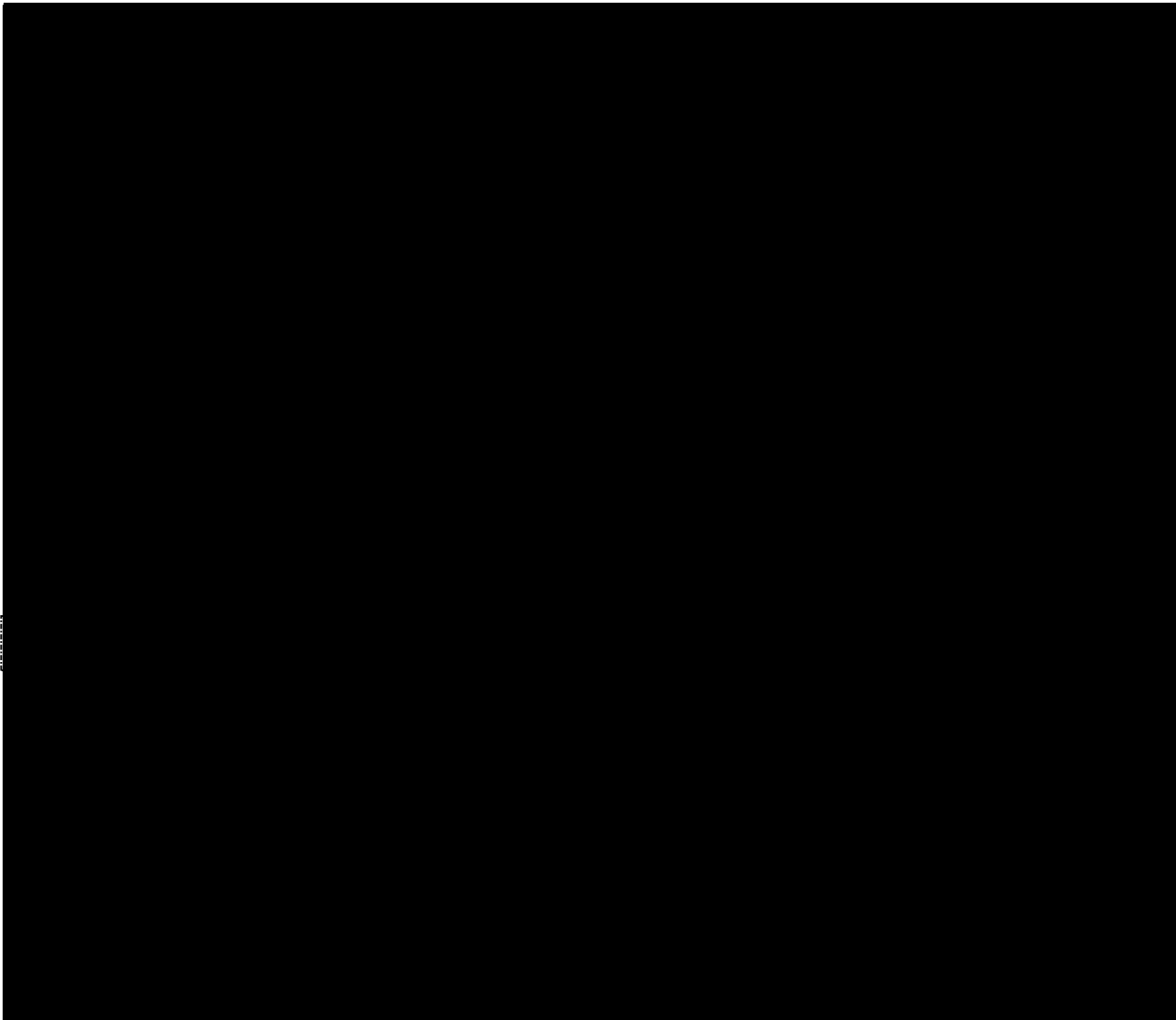
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552).

• Secondary inspection notes 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).



**V. REFERENCES**

- A. INA §§ 101(a)(43), 212(a)(3), 219, 237(a)(4), 237(c), 240(b)(4)(B),
- B. 8 C.F.R. §§ 103.2(b)(16)(i)-(iv), 235.8

**VI. POLICY MEMORANDA**

- A. National Security

**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).

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

#### B. FBI Name Check

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

#### C. Department of Homeland Security

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

#### D. Asylum-related

1. "*Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies*" dated April 18, 2007.
2. "*Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants*" dated June 3, 2005.
3. "*Protocols for Handling Asylee Adjustment Cases That May Warrant Initiation of the Asylum Status Termination Process*" dated July 19, 2004.
4. "*Confidentiality of Asylum Applications and Overseas Verification of Documents and Application Information*" dated June 21, 2001.

## VII. ADDITIONAL ELECTRONIC RESOURCES

- A. 2008 Customs & Border Protection Special Interest Alien Handbook
- B. Fraudulent Document Laboratory (FDL) Guides
  1. Middle Eastern Calendar Guide

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

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

- 
2. North African & Middle Eastern Stamp Guide (entry & exit stamps)
  - C. Al Qaeda Manual
  - D. A Guide to Naming Practices
  - E. National Security Terms of Reference Tables
  - F. USCIS Fact Sheet, "*Immigration Security Checks—How and Why the Process Works,*" dated April 25, 2006.
  - G. Statement of Mutual Understanding of Information Sharing with Dept of Citizenship and Immigration Canada
  - H. Websites for Basic and Supplemental Systems Checks
  - I. Department of Homeland Security For Official Use Only (FOUO) Coversheet
  - J. Sample Background Checklist
  - K. Sample Classified Notes Page

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

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