



U.S. Citizenship and Immigration Services

BASIC

NATIONAL SECURITY COURSE 235

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

SYLLABUS**COURSE TITLE:** National Security**COURSE NUMBER:** 235**COURSE DATE:** February 2013**LENGTH AND METHOD OF PRESENTATION:**

Lecture	Lab	P.E.	Total	Program
3:30	0:00	:30	4:00	BASIC

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

DESCRIPTION:

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

TERMINAL PERFORMANCE OBJECTIVE (TPO):

Given a field situation involving the adjudication of an application or petition, the Immigration Services Officer will be able to understand the security check process and specify criteria for identifying a national security concern. The Immigration Services Officer will have an understanding of the relevant USCIS components and processes associated with vetting and adjudicating cases with identified national security concerns.

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

ENABLING PERFORMANCE OBJECTIVE (EPOs):

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

EPO #2: Identify the organizational components responsible for reviewing the results of security checks, vetting and adjudicating cases identified with national security concerns.

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

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

STUDENT SPECIAL REQUIREMENTS:

Read pages 265 - 268 in *Immigration Law and Procedure in a Nutshell, 6th Edition*, by David Weissbrodt and Laura Danielson.

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

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

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

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

METHOD OF EVALUATION:

Written Examination – Multiple Choice (Open Book)

Handling for Official Use Only (FOUO) Material:

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

Directive does not appear to require such a high level of protection for FOUO materials. See J.M. Loy, ADM, Deputy Secretary of Homeland Security, Safeguarding Sensitive but Unclassified (For Official Use Only) Information, MD11042.1 (1.6.2005). For example, many A-files contain FOUO information. Nonetheless, MD11042.1 does not appear to prohibit leaving A-files on an officer's desk when the officer is away from the desk temporarily or even away overnight, provided the office area has sufficient physical access control measures. See MD11042.1, Section 6. I. Storage.

The practices which the text says to avoid use the word "should," apparently indicating that these are recommendations against certain practices, not prohibitions. If that is the intention, then the text should clarify that these are suggestions for methods to limit unauthorized access to FOUO information, but not absolute prohibitions.

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

TABLE OF CONTENTS

	<u>PAGE</u>
I. Introduction	6
II. Terms of Reference used in National Security Cases	7
II. B USCIS Organization and Functions in Processing National Security Cases	10
II. C USCIS Policies in National Security Cases	17
II. D Requirements for Security Checks	28
III. Summary	
IV. Application	44
V. References	45
VI. Appendix	A1

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

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

Presentation

INTRODUCTION

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

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

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

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

Only a small percentage of security checks reveal information related to national security, compared to the large number of applications filed each year, however all national security cases require intensive review and resolution.

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

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

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

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

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

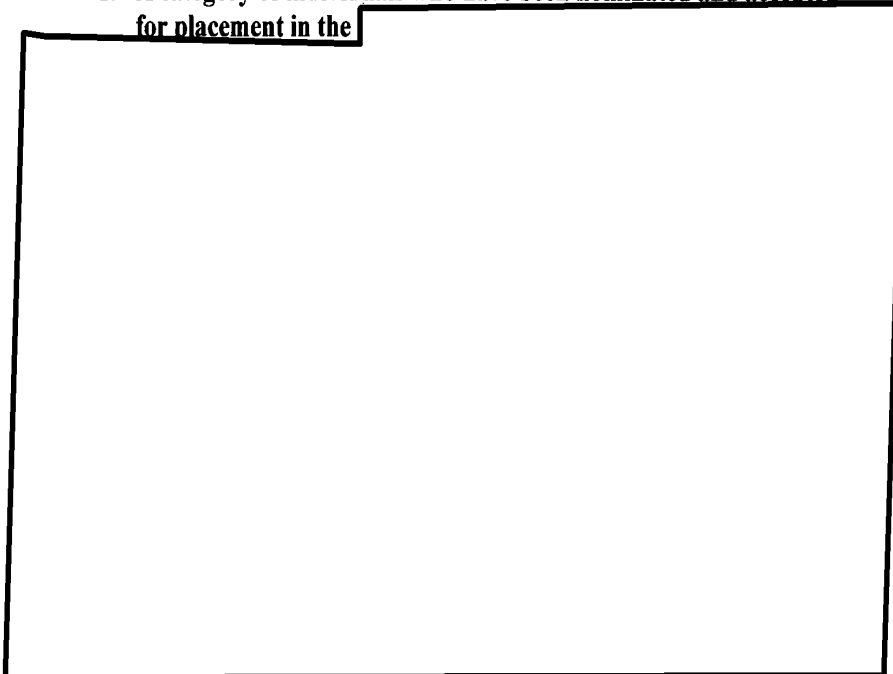
A. National Security (NS) Concern

1. Exists when an individual or organization has been determined to have an articulable link to prior, current or planned involvement in, or association with, an activity, individual or organization described in 212(a)(3)(A), (B), or (F), 237(a)(4)(A) or (B) of the Immigration and Nationality Act (INA).
2. Determination requires that the case be handled in accordance with Controlled Application Review and Resolution Program (CARRP) policy. **The Controlled Application Review and Resolution Program (CARRP) process provides a disciplined approach to identify, record, and adjudicate applications/petitions where a NS concern is identified. It involves four (4) distinct, yet not mutually exclusive, processing steps which will be explained in detail below.**

(b)(7)(e)

B. Known or Suspected Terrorist (KST) NS Concern

1. A category of individuals who have been nominated and accepted for placement 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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

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

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

D. Security Checks

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

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

NOTE: 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.

E. Internal Vetting

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

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

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

F. External Vetting

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

- (a) fact or fact patterns necessary to determine the nature and relevance of the NS concern, including status and results of any ongoing investigation and the basis for closure of any previous investigation; and
- (b) information that may be relevant in determining eligibility, and when appropriate, removability.

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.

H. Designated Officer

Domestic Operations Guidance:

For purposes of CARRP, a designated officer is an Immigration Services Officer, Immigration Analyst, Immigration Officer, Adjudications Officer, Asylum Officer or Refugee Officer who has been designated by local management to be trained, competent and knowledgeable in CARRP procedures. See Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns dated April 24, 2008, signed by Don Neufeld.

New – Updated Policy Memorandum - PM-602-0042

July 26, 2011: The field is now authorized to contact the record owner or nominating agency to vet and deconflict NS concerns involving KSTs. The field, however, is not authorized to approve applications or petitions with confirmed KST NS concerns; that authority continues to rest with the senior leadership of this Agency.

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

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

New – Updated Policy Memorandum - PM-602-0067

May 8, 2012: Policy guidance for the processing of certain cases related to the Immigrant Investor Program (EB5) which are now subject to the Controlled application Review and Resolution Program (CARRP).

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

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

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

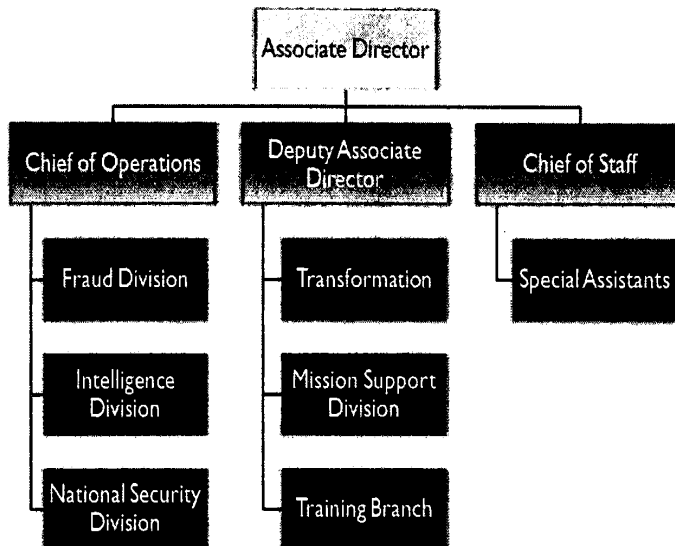
Today FDNS continues to lead the USCIS effort to ensure the integrity of the nation's immigration benefits processes.

The Office of Fraud Detection and National Security Division (FDNS) was created in 2004 and promoted to a Directorate, elevating the profile of their work in 2010. It was established to enhance the integrity of the legal immigration system by identifying threats to national security and public safety, detecting and combating benefit fraud and removing systemic and other vulnerabilities. FDNS Headquarters is composed of four separate divisions: National Security, Intelligence, Fraud, and Mission Support.

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



FDNS Immigration Officer

1. 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. See "Clarification and Delineation of Vetting and Adjudication Responsibilities for Controlled Application and Review and Resolution Program (CARRP) Cases in Domestic Field Offices, dated June 5, 2009, signed by Donald Neufeld.
 - 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.

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

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

- e. Primary conduit for law enforcement coordination such as ICE, FBI, and members of the local JTTF to support the USCIS mission of ensuring the integrity of the immigration system and removing those who pose a threat to the U.S.
- f. While FDNS IOs receive direction and oversight from HQFDNS, they report to and work for local management

HQ FDNS National Security Division

2. National Security Branch (NSB):

- a. One of four divisions in HQFDNS
- b. Provides support to USCIS officers in the field during the vetting and adjudication of cases with NS Concerns
- c. Works closely with law enforcement agencies and the Intelligence Community to facilitate the exchange of information with the field
- d. Develop nations security-related policies, programs and projects, including providing timely, effective training on related NS cases
- e. Facilitate interagency screening coordination: initiate, develop and implement screening projects to enhance security processes

3. National Security Division (NSD) at Headquarters FDNS

- a. Joint Program Coordination Branch (JPCB)
 - i. Over-site of all policies and procedures for National Security programs
 - ii. Liaison for all OGA activities
- b. Screening Coordination Office (SCO)
 - i. Over-site in maintaining NSD objective, quality, and effectiveness, including the NaBISCOP and ECN

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

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

c. Law Enforcement Support Operation Branch

- i. Adjudicate special benefits (S visas) and generates notional documents
- ii. Liaison for LEA and Intel agencies sponsored immigration benefit programs

d. Other Government Agency

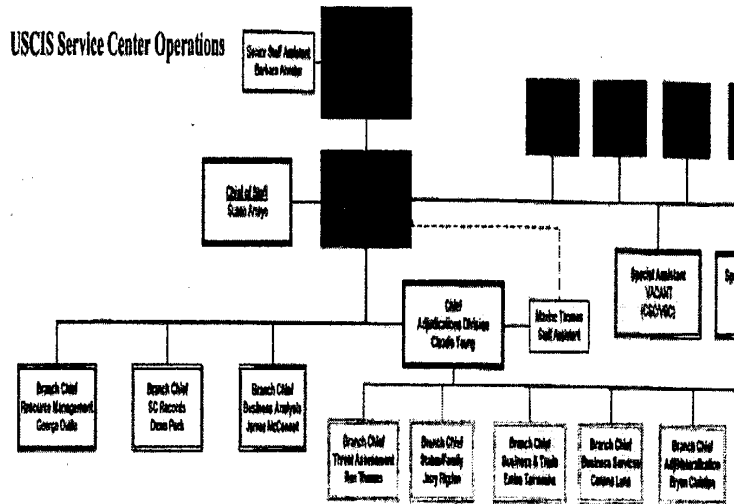
- i. Over-site for permanent presence of FDNS IOs at Other Government Agencies (INTERPOL, White House, TSC, NJTTF, NCTC, HSTC)

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

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

Field Operations and Service Center Operations Directorates:

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.

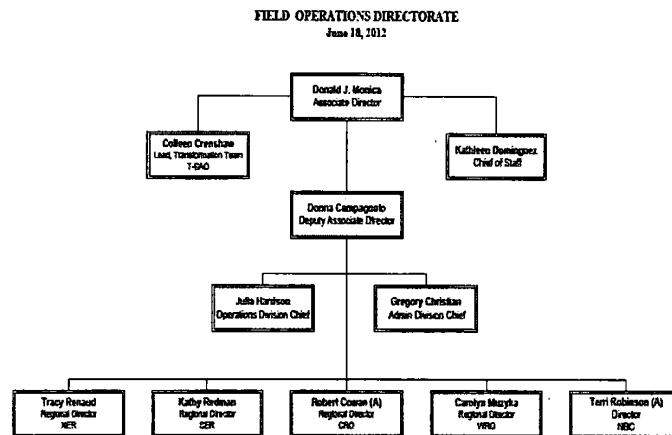
All national security concerns are referred to local Background Check Units (BCU)

- ii. FDNS Immigration Officers in the Center Fraud Detection Operation (CFDO) do not generally process the national security cases but may assist.

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

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

b. Field Offices

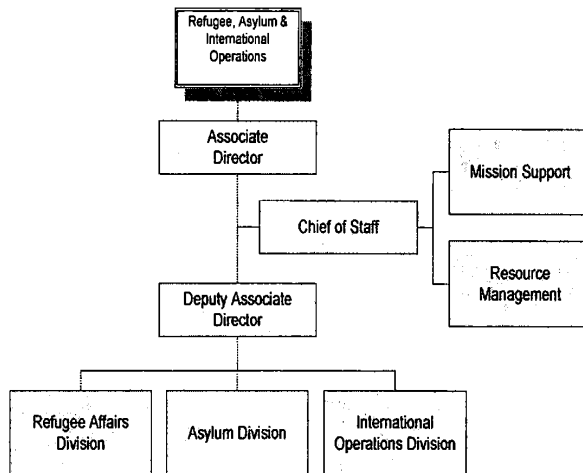


- i. Have established procedures to ensure all IBIS, FBI Fingerprint & FBI Name Check results have been received, reviewed, and are current prior to the granting of an immigration benefit.
- ii. Each Field Office has an established referral process to the local FDNS Immigration Officer for cases identified as having national security concerns.
- iii. National Benefits Center (NBC) falls under the Field Operations Directorate. FDNS staff at NBC handles 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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

c. Refugee, Asylum and International Operations Directorate:



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

~~FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE~~

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

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

A. Controlled Application Review and Resolution Program (CARRP)

Overview

1. USCIS policy memo entitled "*Policy for Vetting and Adjudicating Cases with National Security Concerns*" signed by Jonathan R. Scharfen, Deputy Director, on April 11, 2008
2. Provides agency-wide national security policy
 - Defines key terms so we (USCIS) are all on the same page
 - Rescinds multiple NS memos
3. Decentralizes the authority to vet and adjudicate cases with national security concerns
4. Effective with the issuance of operational guidance from the Directorate of Domestic Operations and each component within the Directorate of Refugee, Asylum, and International Operations (RAIO).
 - a. Domestic Operations - April 24, 2008
 - i. -Field and Service Centers
 - b. International Operations - April 28, 2008
 - c. Asylum - May 14, 2008
 - d. Refugee - May 14, 2008
5. 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.
6. Distinguishes between two types of national security concerns
 - a. Known or Suspected Terrorist (KST)
 - b. Non-KST
7. Applies to all applications and petitions that convey immigrant or non-immigrant status
8. Rescinded specific previous USCIS national security policy memoranda

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

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

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.
11. Introduces Guidance for Identifying National Security Concerns (Attachment A).
Used by all components
12. Introduced Background Check and Adjudicative Assessment (BCAA) located in FDNS-DS.

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

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

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

B. Updated CARRP Guidance

1. ***"Clarification and Delineation of Vetting and Adjudication Responsibilities for Controlled Application Review and Resolution Program (CARRP) Cases in Domestic Field Offices" signed by Donald Neufeld on June 5, 2009***
2. ***"Additional Guidance on Issues Concerning the Vetting and Adjudication of Cases Involving National Security Concerns" signed by Michael Aytes on February 6, 2009***
 - a. Cases with unresolved national security concerns need USCIS Deputy Director's concurrence for approval
 - b. Processing of CARRP cases where lookout (B10) has been removed from system
3. ***"Revised Guidance Pertaining to the Adjudication of Form I-90, Application to Replace Permanent Resident Card" signed by Donald Neufeld on February 6, 2009***
 - a. Addresses both Egregious Public Safety and National Security cases
 - b. Issuance of I-551 will not be delayed due to any pending resolution
4. ***"National Security Adjudication and Reporting Requirements Update" signed by Donald Neufeld on February 9, 2009***
 - a. Rescinds February 4, 2008 guidance to approve certain applications if Name Check is pending for over 180 days
 - b. All applications need a definitive FBI Name Check Response and IBIS resolution prior to final adjudication
5. ***"Uniform Instruction for Standardized CARRP File Identification and Movement of CARRP Cases within the USCIS" signed by Donald Neufeld, DOMO, Gregory B. Smith, Associate Director, NSRV on March 26, 2009***
 - a. CARRP File Identification with specific coversheet
 - b. Creation of dedicated email accounts for CARRP cases

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

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

C. Petitions that Do Not Convey Status

1. Petitions that do not convey immigrant or non-immigrant status are not vetted and adjudicated under CARRP. Adjudication of these petitions establishes eligibility for the visa category, not admissibility.
2. Certain steps are required by the Designated CARRP officer for all national security concern that arise: (b)(7)(e)
 - a. National security concern must be documented.
 - 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
3. Domestic Operations Operational Guidance lists the petitions that do not convey immigrant/non-immigrant status:

I-129	Nonimmigrant worker
I-539	Change or Extension of Stay (COS or EOS)
I-129F	Fiancé/e
I-130	Alien relative
I-140	Employment
I-360	Religious Worker cases only
I-600/I-800	Adoption
I-824	Application for action on petition

Why are these petitions not covered by CARRP*?

These petitions are adjudicated based on eligibility. Since they do not convey status, inadmissibility is not considered during the adjudication. (b)(7)(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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

4. Which applications and petitions does CARRP policy cover?

- All other applications
 - e.g. I-485, N-400, I-765, I-687, I-821, etc.
- Petitions
 - Form I-129 petitions requesting change of status (COS) or extension of Stay (EOS)
 - Form I-730 (alien relative of asylee or refugee)
 - **Form 1526 (petition for entrepreneur)

Remember: Certain steps are required by the Designated CARRP officer for all national security concern that arise:

- a. National security concern must be documented.
- b. Thorough review for ineligibility and fraud concern (b)(7)(e)
- c. Deconfliction

D. Officer Responsibilities

1. Field Responsibilities – Designated CARRP Officer:

Designated Officers in the FIELD are responsible for:

- Establishing articulable link
- Internal and External Vetting of KST and Non-KSTs
- Deconfliction on KSTs and Non-KSTs
- Adjudicating all NS related applications and petitions
 - Approvals on Non-KSTs require Senior level official in Field (see Ops Guidance)
 - If KSTs are otherwise approvable (after eligibility assessment/internal vetting), assistance may be requested from HQFDNS
 - Approvals on KSTs require concurrence by the USCIS Deputy Director

~~FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE~~

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

2. NSD and CARRP

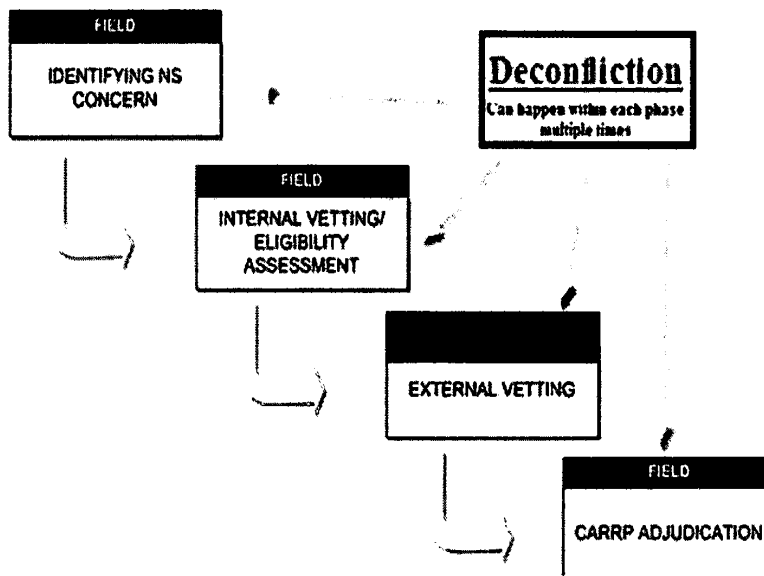
HQFDNS – NSD will:

- Conduct limited High-Side check and Tearlines
- Pursue declassification and/or use of classified information
- Conduct outreach to Intel Community
- Provide policy guidance, technical assistance, and other operational support

E. Four Stages in the CARRP Workflow

- 1) Identify NS Concern
- 2) Eligibility Assessment/Internal Vetting
- 3) External Vetting
- 4) Final Adjudication

****DECONFLICTION**



FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

1. Identifying National Security Concerns

- a. Generally results from security check but may be identified from other sources at any time during the adjudication process
- b. Confirm match
 - i. KSTs via Terrorist Screening Center (TSC) by designated officer
 - ii. Non-KSTs
- c. Determine and document articulable concern by designated officer
 - i. Background Check and Adjudicative Assessment (BCAA)
 - ii. FDNS-DS
- d. Consider effect of NS indicators relating to family members and close associates on the individual

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

2. Eligibility Assessment includes Internal Vetting

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

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

3. External Vetting

Outreach to record owner of national security information:

- a. To obtain information that may be relevant in determining eligibility
- b. To obtain information regarding the nature and extent of the national security concern
- c. For KSTs and Non-KST NS concerns, the Field conducts external vetting
- d. Senior Official in the field must confirm no ground of ineligibility exist prior to requesting assistance for HQFDNS.

4. Final Adjudication of National Security Cases (CARRP Adjudication)

If NS concern remains, evaluation of results of internal and external vetting to make eligibility determination.

- a. For all NS concerns designated officers with appropriate concurrence may seek assistance from HQFDNS. Senior Official will confirm that the application/petition is approvable
- b. For KST NS concerns, only the USCIS Deputy Director has the authority to approve.
- c. For Non-KST NS concerns, Senior-level officials have authority to approve or the 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

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

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

- d. 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.

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

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

Instructor's note: Each component has specific guidance for handling cases with material support. Domestic Operations does not require that the cases are immediately entered into FDNS-DS or a BCAA is completed. Only after a determination has been made that the individual is not eligible based on the NS ground, or will not be granted an exemption, would entry in FDNS-DS be required as well as a TECS record based on the inadmissibility finding. For determinations on material support and other terrorist-related exemption determinations, see the following memoranda:

- 1) "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 July 28, 2008 from Acting Deputy Director Michael L. Aytes;

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

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

- 2) "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," dated March 26, 2008, from Deputy Director Jonathan Scharfen; and
- 3) "Processing the Discretionary Exemption to the Inadmissibility Ground for Providing Material Support to Certain Terrorist Organizations," dated May 24, 2007 from Deputy Director Jonathan Scharfen. See respective operational guidance for specific handling steps for material support cases:
- *Implementation of Section 691 of Division J of the Consolidated Appropriations Act, 2008, and Updated Processing Requirements for Discretionary Exemption to Terrorist Activity Inadmissibility Grounds.* 7/28/08 Michael L. Aytes, HQ USCIS
 - *Withholding Adjudication and Review of Prior Denials of Certain Categories of Cases Involving Association with, or Provision of Material Support to, Certain Terrorist Organizations or Other Groups.* 3/26/08 Jonathan Scharfen, HQUSCIS
 - *Authorization to process cases involving the provision of material support to the AUC.* 3/10/08 Paul S. Rosenzweig DHS Policy
 - *Authorization to process cases involving the provision of material support to the ELN.* 12/18/07 Paul S. Rosenzweig DHS Policy
 - *Processing the Discretionary Exemption to the Inadmissibility Ground for Providing Material Support to the Revolutionary Armed Forces of Colombia (FARC).* 09/06/07 Jonathan Scharfen HQUSCIS + (Material Support)
 - Attachment: Material Support Exemption Worksheet
 - *Processing the Discretionary Exemption to the Inadmissibility Ground for Providing Material Support to Certain Terrorist Organizations* 5/24/07 Jonathan Scharfen

G. Special Considerations

Specific guidance on these applications and cases may be found in the respective operational guidance. For Domestic Operations: see pp. 30- 34 and p 44 "Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns" dated April 24, 2008, signed by Don Neufeld.

1. Includes information on handling both NS concerns and egregious public safety concerns
 - a. Application for Employment Authorization (Forms I-765)
 - b. Application for Travel Authorizations (Form I-131)

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

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

- c. Application for Replacement Permanent Resident Card (Form I-90) - updated guidance has been issued
- d. Santillan Cases – also known as EOIR cases
- e. Appeals/Motions to Reconsider or Reopen
- f. Application for Naturalization

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

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

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

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

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

ALWAYS DECONFLICT PRIOR TO USCIS ACTION!!!!

Reminders:

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

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

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

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

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

Each year USCIS conducts specific checks or a combination of checks on 6-7 million individuals seeking immigration benefits.

A. USCIS Security Checks Overview

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

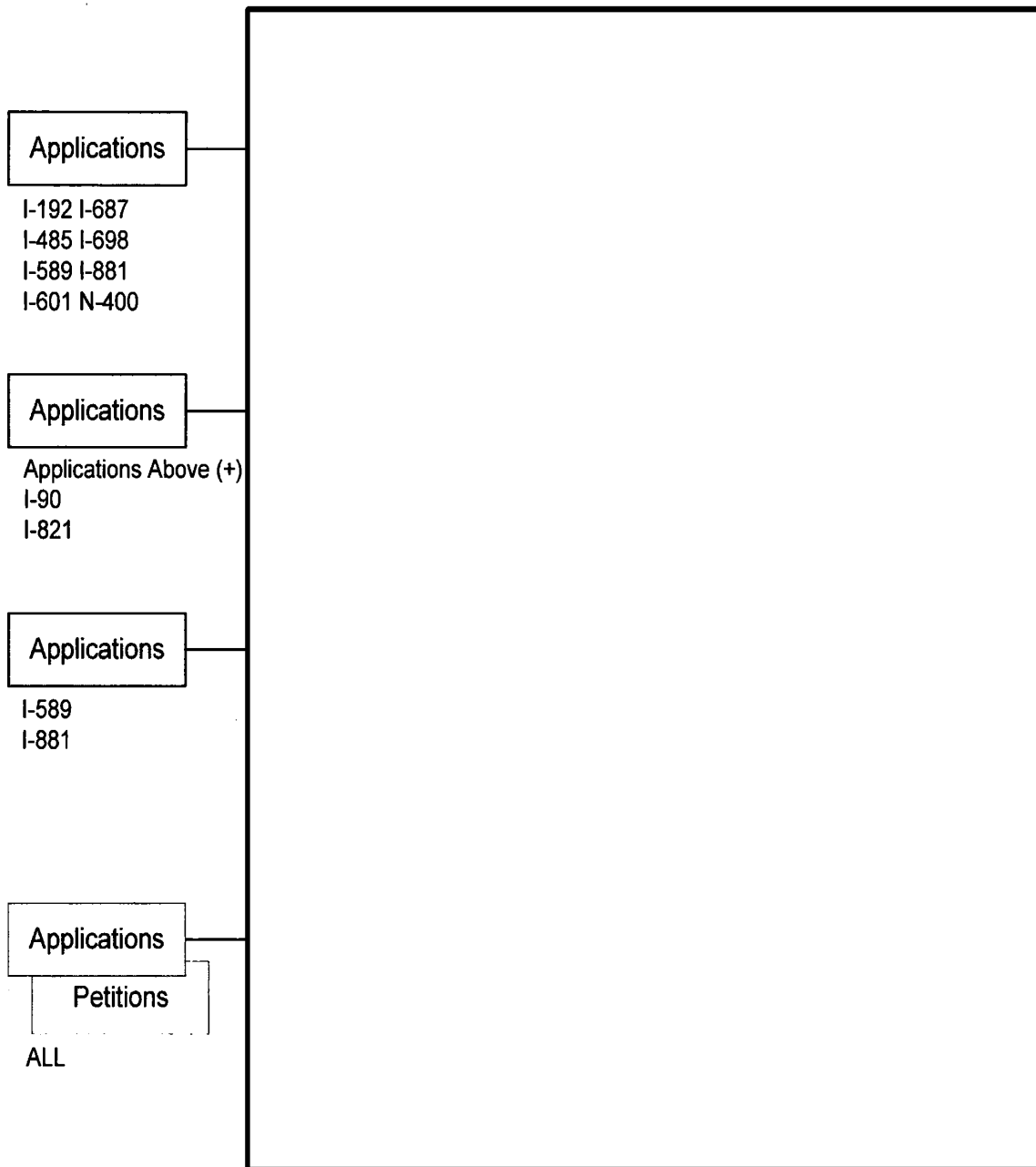
1. FBI Name Check
2. FBI Fingerprint Check
3. TECS/Interagency Border Inspection System (IBIS)
4. United States-Visitor and Immigrant Status Indicator Technology (US-VISIT)/Automated Biometrics Identification System (IDENT).

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

(b)(7)(e)

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

B. FBI Name Check

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

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

The NNCP conducts manual and electronic searches of the FBI's Central Records System (CRS) Universal Index (UNI). The CRS encompasses the centralized records of FBI Headquarters, field offices, and Legal Attaché offices. The CRS contains all FBI investigative, administrative, personnel, and general files.



(b)(7)(e)

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



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.

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

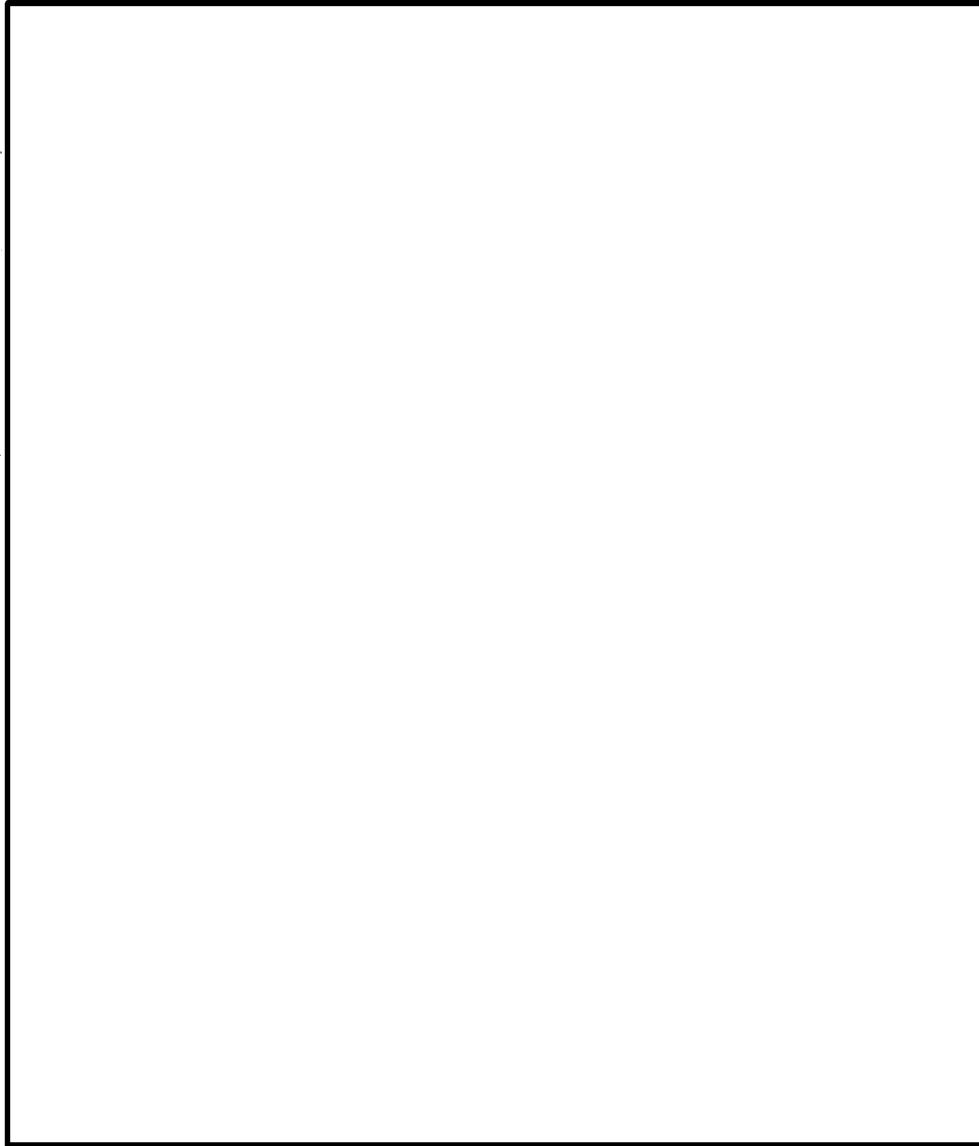
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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

1. Results of FBI Name Check

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

A. Pending Response

(b)(7)(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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

D. Unknown Response (UN)



(b)(7)(e)

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

-Also see the LHM-Letterhead Memorandum.

2. Validity of FBI Name Check



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

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

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

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

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

5. Multiple Name Checks for Same Application –

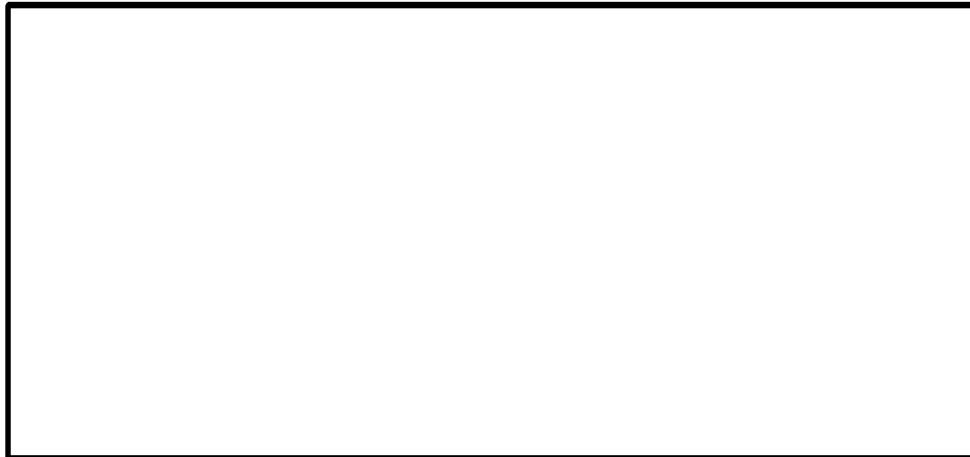
(b)(7)(e)

A large rectangular box with a black border, used to redact information from the document.

- A definitive response may be used with another application if final adjudication occurs within 15 months of the FBI process date.

6. Response with Incorrect Date of Birth

(b)(7)(e)

A large rectangular box with a black border, used to redact information from the document.

7. Response with Incorrect A#

The name search is based on the name and date of birth of the applicant. If a record can be located in the name check database using a name/DOB search, the record can be used. Name checks performed with an inaccurate or missing A-number are valid and should **not** be resubmitted for a new check.

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

The place of birth does not need to be displayed in the response to make the response valid.

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

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



(b)(7)(e)

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



10. FBI Name Check Factors



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

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

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

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

C. FBI Fingerprint Check

1. Background

(b)(7)(e)



2. Applications/Petitions Requiring FBI Fingerprint Check

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

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

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

3. Validity of FBI Fingerprint Check

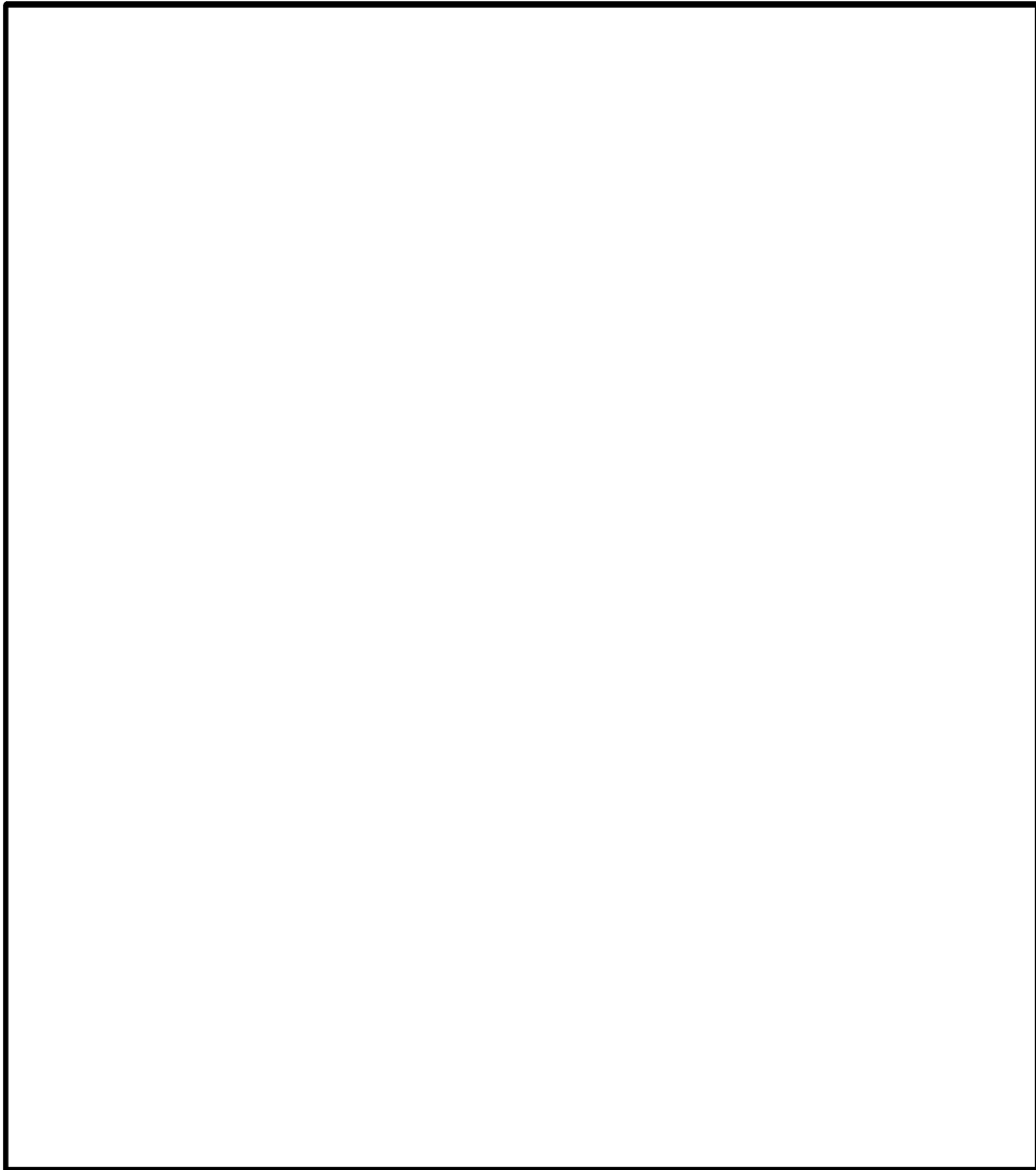
- a. Must be less than fifteen (15) months old at the time of adjudication

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

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

4. Results of FBI Fingerprint Check

(b)(7)(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). This information shall not be distributed beyond the original addressees without prior authorization of the originator.

D. TECS/Interagency Border Inspection System (IBIS)

Instructor's note: Students should be receiving IBIS training later in the course. This is meant to be an overview, explaining the history, basic requirements, and the possible results/information that can be gained from querying IBIS. See Inter-Agency Border Inspection System Standard Operating Procedures (IBIS SOP) dated March 1, 2006.

1. Background

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

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

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

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

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

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

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

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

- USCIS conducts IBIS checks on every applicant, petitioner and beneficiary and in certain cases on businesses. See page 13 of the IBIS SOP dated March 1, 2006, for a list of who to query by application and petition.
- USCIS conducts 33-35 million IBIS name checks per year & receives approximately 10,000 hits of a national security nature.
- Approximately 1,500 are Known or Suspected Terrorists (KSTs).

(b)(7)(e)

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

2. National Crime Information Center (NCIC)



3. IBIS Usage

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

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

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

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

4. Applications/Petitions Requiring TECS/IBIS

- a. Must be run on the following subjects age 14 and over:
 - i. Applicants
 - ii. Petitioners
 - iii. Beneficiaries
 - iv. Derivatives
 - v. Household Members (for I-600, I-600A, I-800, I-800A, I-290B, and EOIR-29 cases only.)
- b. Not only conducted on the applicant and beneficiary but also on the petitioner (individual, business, organization):
 - i. Employment based petitions
 - ii. Religious worker petitions
 - iii. To deny immigration benefits to ineligible petitioners in accordance with the Adam Walsh Act

5. Results from TECS/IBIS

- a. Immigration Services Officers primarily use the subject and business query in TECS.
- b. TECS provides information relating to open and closed investigations, intelligence reports, wants and warrants, etc.
- c. Results identify concerns such as: criminal, immigration violations, public safety, and national security
- d. Queries available at discretion of local office, if not required

6. Validity of TECS/IBIS Checks

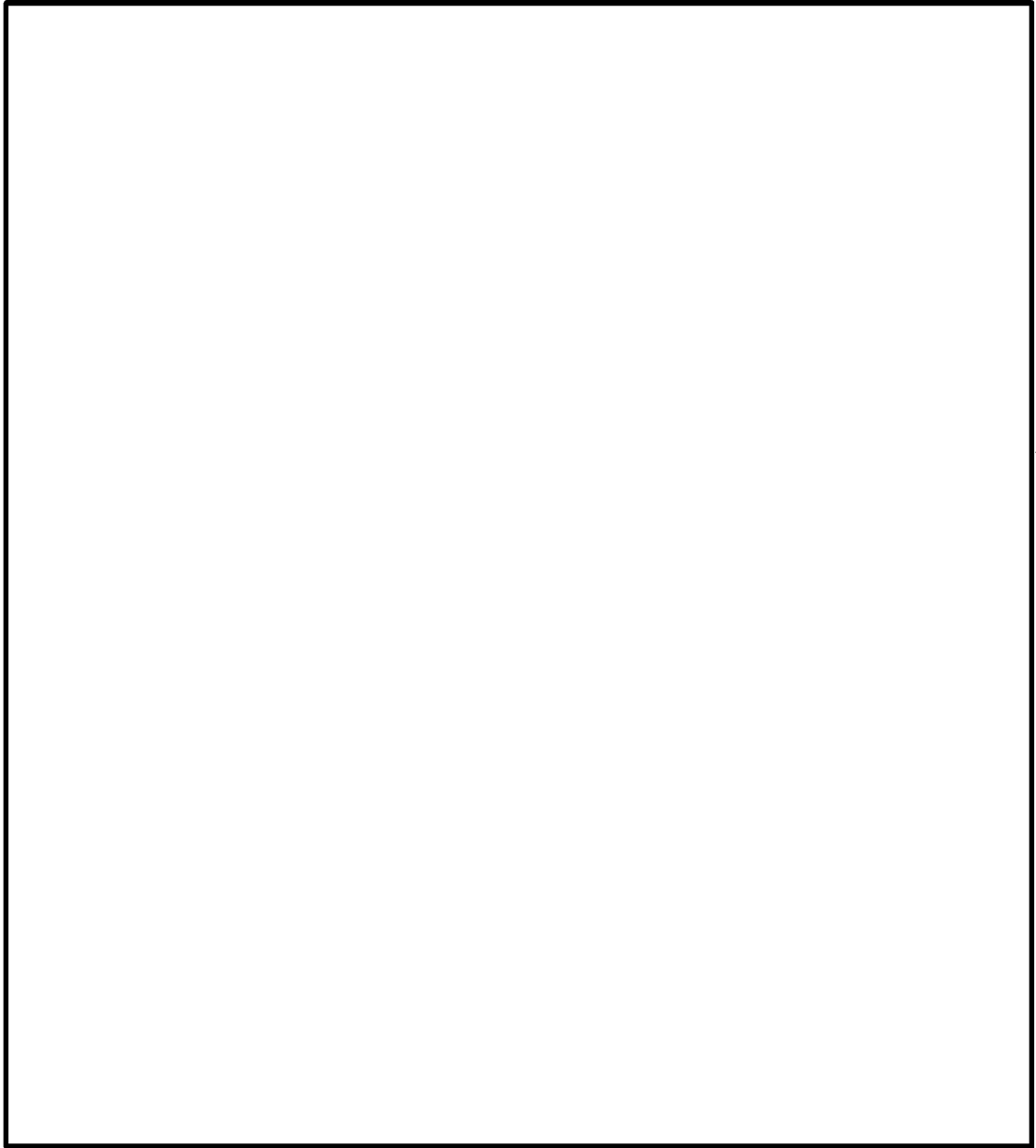
- a. Must be run on all new applications/petitions within 15 calendar days of initial receipt
- b. For applications/petitions filed at a service center or a lockbox, this process is run automatically through a process called Batch Processing
- c. The IBIS query must be valid at the time of final adjudication

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

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

- d. The IBIS query is valid for 180 CALENDAR days. At the time of adjudication if the validity has expired, a manual IBIS query must be completed

(b)(7)(e)



Queries items that do not fit in the other subject categories

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

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

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

- Used primarily by Asylum Branch
- Used by DOS, CBP, ICE
- Loads biographical and biometric information
 - Two Prints vs. Ten Prints
- US-VISIT watch list
 - Not same as Terrorist Watchlist
- The National Background and Security Check Operating Procedures (NABISCOP) (currently being reviewed by interested parties) is intended for all USCIS personnel who perform security and background checks when processing requests for immigration benefits.
- USCIS personnel include USCIS employees and contractors. USCIS personnel must have 1) a need-to-know, 2) required training and 3) the appropriate level of background and security clearances to conduct these checks.
- As of the date of future publication, the NABISCOP is intended to replace the Interagency Border Inspection System Standard Operating Procedures (IBIS SOP), dated March 1, 2006, which will then be rescinded.
- Incorporating elements from the IBIS SOP, the NABISCOP will then be considered the foundation for service-wide security background check procedures.
- NABISCOP is intended to be used in concert with other USCIS policy and guidance as well as component specific guidance and standard operating procedures as they relate to the processing of specific applications, petitions, and other immigration benefits.

F. Third Agency Rule

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

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

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

G. DHS Components

1. All DHS components are considered one agency.
2. Information from these components is oftentimes "Law Enforcement Sensitive" (e.g. TECS/IBIS hit information) and must be protected regardless.
3. Component information shall not be disclosed to another agency without the permission of the owning component.
4. Includes but not limited to Immigration and Customs Enforcement (ICE), CBP, the U.S. Secret Service.
 - "DHS Policy for Internal Information Exchange and Sharing," dated February 1, 2007: All DHS components are considered to be part of one "agency" for purposes of the Privacy Act, 5 U.S.C. § 552a(a)(1), (b)(1).
 - No DHS component should consider another DHS component to be a separate agency for information-sharing purposes.
 - Absent any legal prohibitions as set forth by the Department's Office of General Counsel, information shall be shared within DHS whenever the requesting officer or employee has an authorized purpose for accessing the information in the performance of his or her duties, possesses the requisite security clearance, if one is needed, and assures adequate safeguarding and protection of the information.
 - From this point forward, information-access and -sharing agreements with outside entities will be negotiated and entered into on behalf of the Department as a whole, not on behalf of an individual DHS component.

H. USCIS Fact Sheet on Immigration Security Checks

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

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

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



Who has the firstQUESTION?

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

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

IV. APPLICATION

A. In-Class Laboratory

- None

B. In- Class Practical Exercises

- 13 Review questions
- 15 Scenarios for Applying Referral Criteria(if time permits)

C. Review Power Point

- 12 Review question covering the entire presentation.

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

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

V. REFERENCES

A. INA §§ 101(a)(43), 101(f)(6), 212(a)(3), 212(a)(6)(C)(i), 219, 237(a)(4), 237(c), 240(b)(4)(B),

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

C. Nutshell Chapter 8 §§ 8-1.2(c), 8-2.2(d)

Chapter 9 § 9-1.1(d)(2)

Chapter 13 § 13-4.6

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

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

VI. Appendix

- A. Clarification and Delineation of Vetting and Adjudicating Responsibilities for Controlled Application Review and Resolution Program (CARRP) Cases in Domestic Field Offices, dated June 5, 2009.
- B. USCIS Operational Memorandum, "*Policy for Vetting and Adjudicating Cases with National Security Concerns*" dated April 11, 2008
- C. USCIS Memorandum, "*Revised National Security Adjudication and Reporting Requirements*," dated February 4, 2008.
- D. USCIS Operational Memorandum, "*FBI Name Check Process and Clarification for Domestic Operations*," dated December 21, 2006.
- E. USCIS Fact Sheet, "*Immigration Security Checks—How and Why the Process Works*," dated April 25, 2006.
- F. DHS Secretary's Memorandum, "Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings," dated October 4, 2004.
- G. Guidance for Identifying National Security Concerns

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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