

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

Memorandum

Original Dated April 11, 2008

TO: FIELD LEADERSHIP

FROM: Jonathan R. Scharfen, Deputy Director /S/

SUBJECT: Policy for Vetting and Adjudicating Cases with National Security Concerns

I. Purpose

This memorandum outlines USCIS policy for identifying and processing cases with national security (NS) concerns,¹ and rescinds existing policy memoranda pertaining to reporting and resolving NS concerns. It also identifies Headquarters' Office of Fraud Detection and National Security (HQFDNS) as the point of contact for technical advice to assist the field² with vetting and adjudicating cases with NS concerns. This policy, known as the Controlled Application Review and Resolution Program (CARRP), establishes the following:

- The field is responsible for vetting and documenting Non-Known or Suspected Terrorist (Non-KST)³ NS concerns, and adjudicating all NS-related applications and petitions.⁴

¹A **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 sections [212\(a\)\(3\)\(A\), \(B\), or \(F\)](#), or [237\(a\)\(4\) \(A\) or \(B\)](#) of the Immigration and Nationality Act (the Act). This determination requires that the case be handled in accordance with CARRP policy outlined in this memorandum.

² **Field** refers to Field Offices, Service Centers, the National Benefits Center, and equivalent offices within the Refugee, Asylum, and International Operations Directorate (RAIO).

³ **Known or Suspected Terrorist (KST)** is a category of individuals who have been nominated and accepted for placement in the Terrorist Screening Database (TSDB), are on the Terrorist Watch List, and have a specially-coded lookout posted in TECS/IBIS, and/or the Consular Lookout Automated Support System (CLASS), as used by the Department of State. **Non-KST** is the category of remaining cases with NS concerns, regardless of source, including but not limited to: associates of KSTs, unindicted co-conspirators, terrorist organization members, persons involved with providing material support to terrorists or terrorist organizations, and agents of foreign governments. Individuals and organizations that fall into this category may also pose a serious threat to national security.

⁴This policy applies to all applications and petitions that convey immigrant or non-immigrant status. This policy does not apply to petitions that do not convey immigrant or non-immigrant status. See Operational Guidance for instructions.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS. **Confidential - Subject to Protective Order** www.uscis.gov **CAR000001**

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

Policy for Vetting and Adjudicating Cases with National Security Concerns
Page 2

- The FDNS-Data System (FDNS-DS) is the primary system for recording vetting, deconfliction, and other resolution activities.⁵
- HQFDNS maintains responsibility for external vetting⁶ of Known or Suspected Terrorist (KST) hits; and, upon request from the field, provides advice, technical assistance (including draft decisions), and operational support on KST and Non-KST cases with NS concerns.

II. Effective Date and Implementation

Operational Guidance implementing this policy will soon be issued by the Domestic Operations Directorate⁷ (DomOps) and individual components of the Refugee, Asylum, and International Operations Directorate (RAIO). This policy will be effective upon issuance of each directorate's respective guidance.

III. Rescission of Prior Policy and Procedures

Upon issuance of the Operational Guidance, the following policy memoranda and procedures will be rescinded:

- *Processing of Applications for Ancillary Benefits Involving Aliens Who Pose National Security or Egregious Public Safety Concerns*, dated May 11, 2007;
- *Processing of Forms I-90 Filed by Aliens Who May Pose National Security or Egregious Public Safety Concerns*, dated May 11, 2007;
- *National Security Reporting Requirements*, dated February 16, 2007;
- *National Security Record Requirements*, dated May 9, 2006;
- *Permanent Resident Documentation for EOIR and I-90 Cases*, dated April 10, 2006;
- Appendix A of the Inter-Agency Border Inspection System (IBIS) [Standard Operating Procedure](#), dated March 1, 2006;

⁵ If FDNS-DS is not currently available at any specific field office, officers must document CARRP procedures by another method as identified in Operational Guidance.

⁶ **External Vetting** consists of inquiries to record owners in possession of NS information to identify: (a) facts 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. See section IV.C for further instruction.

⁷ The **Domestic Operations Directorate** comprises Service Center Operations and Field Operations.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVEPolicy for Vetting and Adjudicating Cases with National Security Concerns
Page 3

- *Revised Instructions for Processing Asylum Terrorist/Suspected Terrorist Cases*, dated January 26, 2005; and
- Section VIII of the Asylum Identity and Security Check Procedures Manual.

Officers should refer to relevant Operational Guidance⁸ when adjudicating the following, *if found to involve NS or Egregious Public Safety*⁹ concerns:

- Petitions that do *not* convey immigrant or non-immigrant status;
- Applications for employment authorization;
- Applications for travel authorization;
- Replacement Lawful Permanent Resident cards;
- *Santillan*¹⁰ cases.

IV. Policy Guidance

This policy, in conjunction with Operational Guidance, provides direction to identify and process cases containing NS concerns in the most efficient manner. The process allows sufficient flexibility to manage the variety of cases encountered by USCIS.

Officers should note that at any stage of the adjudicative process described below, deconfliction may be necessary before taking action on a KST or Non-KST NS concern. Deconfliction is a term used to describe coordination between USCIS and another government agency owner of NS 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, or timing of the decision) do not compromise or impede an ongoing investigation or other record owner interest.

A. Identifying National Security Concerns

As a result of the security checks¹¹ or at any stage during the adjudicative process, the

⁸ Including [Policy Memorandum 110](#) (*Disposition of Cases Involving Removable Aliens*) issued July 11, 2006. That memorandum is not rescinded and does not apply to asylum applications.

⁹An **Egregious Public Safety (EPS)** case is defined in Policy Memorandum 110.

¹⁰ *Santillan et al. v. Gonzales, et al.*, 388 F. Supp2d 1065 (N.D. Cal. 2005).

¹¹**Security checks** may consist of the FBI Name Check, FBI Fingerprint Check, Treasury Enforcement Communications System/Inter-Agency Border Inspection System (TECS/IBIS), or United States Visitor and Immigrant Status Indicator Technology/Automated Biometrics Identification System (US VISIT-IDENT). Specific checks or combinations of checks are required for each application or petition type, pursuant to each component's procedures.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVEPolicy for Vetting and Adjudicating Cases with National Security Concerns
Page 4

officer may identify one or more indicators¹² that may raise a NS concern. In such cases, the officer must first confirm whether the indicator(s) relates to the applicant, petitioner, beneficiary, or derivative (“the individual”).¹³ When a Non-KST NS indicator has been identified, the officer must then analyze the indicator in conjunction with the facts of the case, considering the totality of the circumstances, and determine whether an articulable link exists between the individual and an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F), or 237(A) or (B) of the Act.

1. For Non-KST NS indicators, the officer should refer to the Operational Guidance for instruction on identifying those indicators that may raise a NS concern.
2. After confirming the existence of a KST NS concern via a TECS/IBIS check, the officer must contact the Terrorist Screening Center (TSC), as instructed in the content of the TECS/IBIS record, and must determine whether the KST NS concern relates to the individual. Officers are not authorized to request from the record owner any NS information related to a KST NS concern other than identification of the subject.

The officer must also consider and evaluate, in all cases, indicators related to family members or close associates of the individual to determine whether those indicators relate to the individual as well.

B. Internal Vetting and Assessing Eligibility in Cases with National Security Concerns

For both Non-KST and KST concerns, once the concern has been identified, the officer must conduct a thorough review of the record associated with the application or petition to determine if the individual is eligible for the benefit sought. The officer must also conduct internal vetting¹⁴ to obtain any relevant information to support adjudication and, in some cases, to further examine the nature of the NS concern.¹⁵

For Non-KST NS concerns, the field is authorized to perform internal and external vetting. See step IV.C below for an explanation of external vetting.

For KST NS concerns, the field is only authorized to perform internal vetting. Record owners in possession of NS information are not to be contacted. HQFDNS has sole responsibility for external vetting of KST NS concerns.

¹² Guidelines for types of indicators that may be encountered during adjudication will be provided as an attachment to the Operational Guidance to assist officers in identifying NS concerns.

¹³ For purposes of this memorandum, the term “individual” may include a petitioner.

¹⁴ **Internal vetting** may consist of DHS, open source, or other systems checks; file review; interviews; and other research as specified in Operational Guidance.

¹⁵ If an [exemption is granted under section 212\(d\)\(3\)\(B\)\(i\) of the Act](#) for a terrorist-related inadmissibility ground, and if no other NS concern is identified, no further vetting is necessary and the application may continue through the routine adjudication process.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVEPolicy for Vetting and Adjudicating Cases with National Security Concerns
Page 5

The purpose of the eligibility assessment is to ensure that valuable time and resources are not unnecessarily expended externally vetting a case with a record owner when the individual is otherwise ineligible for the benefit sought. When this is the case, the application or petition may be denied on any legally sufficient grounds.¹⁶

When a NS concern exists, the NS information may be of a restricted or classified nature. These NS or law enforcement operations-based restrictions are often directly linked to protecting sensitive sources, methods, operations, or other elements critical to national security. Access to this information is therefore limited to those with a direct need to know and, when applicable, appropriate security clearance. As a policy matter, USCIS requires that a thorough eligibility assessment and completion of internal vetting precede any outreach for access to NS information.

C. External Vetting of National Security Concerns1. Non-KST NS Concerns

In a case with a Non-KST NS concern, the officer must initiate the external vetting process before the case may proceed to final adjudication if:

- the application or petition appears to be otherwise approvable, and internal vetting is complete;
- there is an identified record owner in possession of NS information; and
- the NS concern remains.

At this stage, the officer confirms with the record owner the earlier USCIS identification of the NS concern (*see* step IV.A above) and obtains additional information regarding the nature of the NS concern and its relevance to the individual. This is accomplished by obtaining from the record owner facts and fact patterns to be used in confirming whether an articulable link exists between the individual and an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F) or 237(A) or (B) of the Act.

Additionally, the officer seeks to obtain additional information that may be relevant in determining eligibility and, when appropriate, removability. This process requires close coordination with law enforcement agencies, the Intelligence Community,¹⁷ or other record owners. If the external vetting process results in a finding that the NS concern no longer exists, and if the individual is otherwise eligible for the benefit sought, the application or petition is approvable.

¹⁶ All references in this memorandum to “denying” a case also encompass the possibility of referring an asylum case to an Immigration Judge.

¹⁷ Officers are not authorized to contact Intelligence Community members; such outreach is conducted by HQFDNS.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVEPolicy for Vetting and Adjudicating Cases with National Security Concerns
Page 6

When USCIS obtains information from another government agency during the external vetting process, DHS policy guidance¹⁸ requires that authorization from the record owner be obtained prior to any disclosure of the information. Therefore, in order to use the information during adjudication, prior written authorization must be obtained from the record owner. If the information indicates that the individual is ineligible for the benefit sought, and if permission from the record owner has been secured for the use of unclassified information,¹⁹ the application or petition may be denied based on that unclassified information.

2. KST NS Concerns

For KST NS concerns, field officers are not authorized to conduct external vetting with record owners in possession of NS information. As stated above, only internal vetting of KST NS concerns is permitted at this stage. HQFDNS has sole responsibility for external vetting of KST NS concerns, which must be conducted in cases with a confirmed KST hit that have been determined to be otherwise approvable.

D. Adjudicating National Security Cases

Upon completion of required vetting, if the NS concern remains, the officer must evaluate the result of the vetting and determine any relevance to adjudication, obtain any additional relevant information (e.g., via a request for evidence, an interview, and/or an administrative site visit), and determine eligibility for the benefit sought. Adjudication of a case with a NS concern focuses on thoroughly identifying and documenting the facts behind an eligibility determination, and, when appropriate, removal, rescission, termination, or revocation under the Act.

If the individual is ineligible for the benefit sought, the application or petition may be denied.

If the vetting process results in a finding that the NS concern no longer exists, and if the individual is otherwise eligible for the benefit sought, the application or petition may be approved.

Non-KST NS Concerns

Officers are not authorized to approve applications with confirmed Non-KST NS concerns without supervisory approval and concurrence from a senior-level official (as

¹⁸ See [DHS Management Directive 11042.1](#), *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, dated 1-6-2005; and DHS Memorandum, *Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings ("Ridge Memo")*, dated 10-4-2004.

¹⁹ Requests for declassification of information and use of classified information during adjudication may only be made by HQFDNS. Officers should refer to Operational Guidance for further instruction.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

Policy for Vetting and Adjudicating Cases with National Security Concerns
Page 7

defined in Operational Guidance). That official also has discretion to request additional external vetting assistance from HQFDNS in accordance with Operational Guidance.

2. KST NS Concerns

Officers are not authorized to approve applications with confirmed KST NS concerns. If the senior-level official concurs, external vetting assistance must be requested from HQFDNS in accordance with Operational Guidance.

V. Conclusion

Officers should make every effort to complete NS cases within a reasonable amount of time, by taking into consideration the nature of the concern and the facts contained in each individual case. HQFDNS is available to provide technical expertise in answering questions that may arise in these cases. Any questions or issues that cannot be resolved in the field regarding identification, vetting, or adjudication of cases with NS concerns are to be promptly addressed through the established chain of command.

Distribution List: Regional Directors
 District Directors
 Field Office Directors
 Service Center Directors
 Asylum Office Directors

FOR OFFICIAL USE ONLY / LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy governing the use of FOUO information. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This document and the information contained herein are not to be distributed outside of DHS.

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

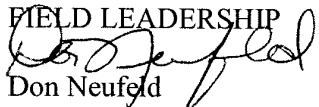
U.S. Department of Homeland Security
20 Massachusetts Ave NW
Washington, D.C. 20529



U.S. Citizenship
and Immigration
Services

HQ 70/28.1

Interoffice Memorandum

TO: FIELD LEADERSHIP
FROM: 
Don Neufeld
Acting Associate Director, Domestic Operations

DATE: **APR 24 2008**

RE: Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns

Introduction

A central mission of United States Citizenship and Immigration Services (USCIS) is to protect the integrity of the U.S. immigration system and preserve the safety of our homeland. National security (NS) matters are a primary consideration in USCIS adjudications and measures must be adopted to ensure a consistent approach in resolving these concerns. In order to efficiently process cases with NS issues and mitigate potential risks to national security, USCIS is delegating decision-making authority to the field. This authority includes the responsibility for the vetting and adjudication of applications and petitions involving national security concerns.

Purpose

This memorandum and attached operational guidance provides instruction to USCIS Field Offices for vetting and adjudicating cases with national security concerns. Issuance of this memorandum implements the recently distributed policy memorandum entitled, "*Policy for Vetting and Adjudicating Cases with National Security Concerns.*" This

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

new policy establishes the Controlled Application Review and Resolution Program (CARRP), which consists of a four-step process of evaluating national security concerns.

Effective immediately, all Field Offices are directed to comply with the attached operational guidance and instructions when adjudicating applications or petitions with national security concerns.

Training

A train the trainer session has been scheduled from May 5-9 in Washington, DC for identified field officers. These new trainers, along with FDNS personnel, will then be deployed to provide training to additional staff from May 12-23.

The additional field officers who will be identified to receive this training will attend a one week training session during the week of May 12 or May 19. Training sites during the week of May 12 will be at the National Benefits Center, Texas Service Center, California Service Center and a location to be determined in the New York City area. Training sites during the week of May 19 will be at the 3 aforementioned centers.

Coordination of this training is being handled by Headquarters, Regional Office and Service Center representatives.

Contact

USCIS personnel with questions regarding this memorandum should raise them through the appropriate channels to the Office of Field Operations and Service Center Operations.

Distribution List: Regional Directors
 District Directors
 Field Office Directors
 Service Center Directors

Attachments: CARRP Policy Memorandum
 Operational Guidance
 KST Flowchart
 Non-KST Flowchart

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

U.S. Department of Homeland Security
Washington, DC 20528



U.S. Citizenship
and Immigration
Services

Interoffice Memorandum

To: All Refugee Affairs Division Personnel

From: Barbara L. Strack *B. Strack*
Chief, Refugee Affairs Division

Date: May 14, 2008

Re: Operational Guidance for Vetting and Adjudicating Refugee Cases with National Security Concerns

On April 11, 2008, USCIS Deputy Director Scharfen issued the memorandum "Policy for Vetting and Adjudicating Cases with National Security Concerns." This policy, known as the Controlled Application Review and Resolution Program (CARRP), provides USCIS adjudicators instructions for identifying, vetting, and adjudicating cases with national security concerns. The policy outlines a four-step process for adjudicators to follow when analyzing and vetting national security information and assessing eligibility for cases when national security information is identified. This memorandum defines headquarters and field responsibilities and establishes the Fraud Detection and National Security-Data System (FDNS-DS) as the primary system for recording activities.

With the issuance of this memorandum, Refugee Affairs Division (RAD) is establishing procedures for all refugee status adjudications involving an applicant for whom national security information is identified. The attached operational guidance outlines the responsibilities at RAD headquarters and field level in identifying, vetting, and adjudicating refugee cases containing national security concerns. This guidance assigns to Headquarters RAD (HQRAD) Integrity Unit the responsibility for external vetting efforts (for non-Known or Suspected Terrorist (non-KST) cases), deconfliction activities, and coordination/communication with Headquarters FDNS (HQFDNS).

The guidance instructs the field to document identified national security information and adjudicator analysis of this information in the Refugee Application Assessment. It further describes the requirement for completion of the Background Check and Adjudicative Assessment (BCAA) and the case entry into FDNS-DS for 1) All KST cases; 2) cases where a national security concern has been confirmed and the application is

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

This document and any attachments are FOR OFFICIAL USE ONLY. They contain information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). These documents are to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information, and are not to be released to the public or other personnel who do not have a valid "need-to-know" basis without prior approval from the originator. If you have received these documents by mistake, please contact the originator for specific handling and destruction procedures.

Operational Guidance for Vetting and Adjudicating Refugee Cases with National Security Concerns
Page 2

recommended for approval; and 3) cases determined to present a tangible/imminent threat/risk to the US, even cases resulting in denial.

This operational guidance requires all refugee cases containing national security concerns to undergo supervisory review. Additional review and concurrence by HQRAD is required for the approval of any case containing an unresolved national security concern.

Questions

Questions related to this memorandum may be directed to Mary Margaret Stone, RAD Policy and Analysis Section.

- Attachments:
- 1) USCIS memorandum of April 11, 2008, "Policy for Vetting and Adjudicating Cases with National Security Concerns"
 - 2) Refugee Adjudication Standard Operating Procedures: Cases Involving National Security Concerns

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

This document and any attachments are FOR OFFICIAL USE ONLY. They contain information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). These documents are to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information, and are not to be released to the public or other personnel who do not have a valid "need-to-know" basis without prior approval from the originator. If you have received these documents by mistake, please contact the originator for specific handling and destruction procedures.



USCIS Domestic Operations Directorate (DOMOPS) CARRP Workflows



U.S. Citizenship
and Immigration
Services

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.



U.S. Citizenship and Immigration Services

Controlled Application Review and Resolution Program (CARRP) Summary

FIELD	<p>Identifying a NS Concern: As a result of the security checks or at any stage during the adjudicative process, the officer may identify one or more indicators that may raise a NS concern. In such cases, the officer must first confirm whether the indicator(s) relates to the applicant, petitioner, beneficiary, or derivative ("the individual"). When a Non-KST NS indicator has been identified, the officer must analyze the indicator and determine whether an articulable link exists between the individual and an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F), or 237 (A) or (B) of the Immigration and Naturalization Act ("the Act"). A KST NS concern must be confirmed via a TECS/IBIS check. If confirmed, the officer must contact the Terrorist Screening Center in order to determine whether the KST NS concern relates to the individual. (CARRP Policy Memorandum, p. 4).</p>
IDENTIFYING A NATIONAL SECURITY (NS) CONCERN	

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08

FIELD	<p>Assessing Eligibility in Cases with a NS Concern: If it is determined that a NS concern exists, the officer must conduct a thorough review of the record associated with the application or petition to determine if the individual is eligible for the benefit sought. The officer must also conduct internal vetting to obtain any relevant information to support adjudication and, in some cases, to further examine the nature of the NS concern. (CARRP Policy Memorandum, p. 4).</p>
INTERNAL VETTING/ ELIGIBILITY ASSESSMENT	

FIELD-NON-KST OR HQFDNS-KST	<p>External Vetting Non-KST Cases: If an application or petition appears to be otherwise approvable, and internal vetting is complete; there is an identified record owner in possession of NS information; and the NS concern remains, then the officer must initiate the external vetting process (Non-KST cases only) before the case may proceed to final adjudication. (CARRP Policy Memorandum, p. 5). KST Cases: Field officers are not authorized to conduct external vetting with record owners in possession of NS information. If the application/petition is otherwise approvable for KST cases, HQFDNS must conduct external vetting of KST concerns. (CARRP Policy Memorandum, p. 6).</p>
EXTERNAL VETTING	

FIELD	<p>CARRP Adjudication: Upon completion of required vetting, if the NS concern remains, the officer must evaluate the result of the vetting and determine any relevance to adjudication, obtain any additional relevant information, and determine eligibility for the benefit sought. Adjudication of a case with a NS concern focuses on thoroughly identifying and documenting the facts behind an eligibility determination, and, when appropriate, removal, rescission, termination, or revocation under the Act. (CARRP Policy Memorandum, p. 6).</p>
CARRP ADJUDICATION	

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

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



U.S. Citizenship and Immigration Services

Background Check and Adjudicative Assessment (BCAA)

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

U.S. Citizenship and Immigration Services

Background Check and Adjudicative Assessment (BCAA)

IMPORTANT: No classified information may be added to this worksheet.

Date:		Officer:		Program Office:	
NS Concern:		Urgency:		Due Date (if applicable):	
A. Subject:					
A#(s):		Current Immigration Status:			
Name: Last		First		Middle	
Alias(es):					
Date of Birth:		Country of Birth:			
Country(ies) of Citizenship:					
Organization(s):					
Associated A#(s):					
B. National Security Summary:					
Basis for NS referral: <input type="checkbox"/> LHM <input type="checkbox"/> TECS/IBIS <input type="checkbox"/> Non-TECS/IBIS					
If Non-TECS/IBIS, source:					
CLASSIFIED Information: <input type="checkbox"/> Yes <input type="checkbox"/> No Date:					
C. Systems Checks Results:					
TECS/IBIS:		Date:		FBI Name:	
FBI Fingerprint:		Date:		US-VA:	
Other(s):					
Decision: <input type="checkbox"/> Yes <input type="checkbox"/> No Date:					

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08

The Background Check and Adjudicative Assessment (BCAA) is used to document NS concerns and track actions taken on applications or petitions where such concerns exist. [Specific guidance on the use of this worksheet is available in each component's operational guidance.] The BCAA is also used as a record to assist data entry into the Fraud Detection and National Security Data System (FDNS-DS). Component guidance will outline when a case must be entered into FDNS-DS.

USCIS will complete the BCAA and coordinate with FDNS for entry into FDNS-DS for the following cases:

- all KST cases, regardless of the decision on the underlying application/petition;
- cases where a NS concern has been confirmed and the application/petition is recommended for approval (except for cases receiving a 212(d)(3)(B)(i) terrorist activity exemption and for which no other national security concerns exist); and
- to the extent required by operational guidance, cases where a national security concern has been confirmed and the application/petition is denied.

Source: BCAA Guidance and Instructions

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

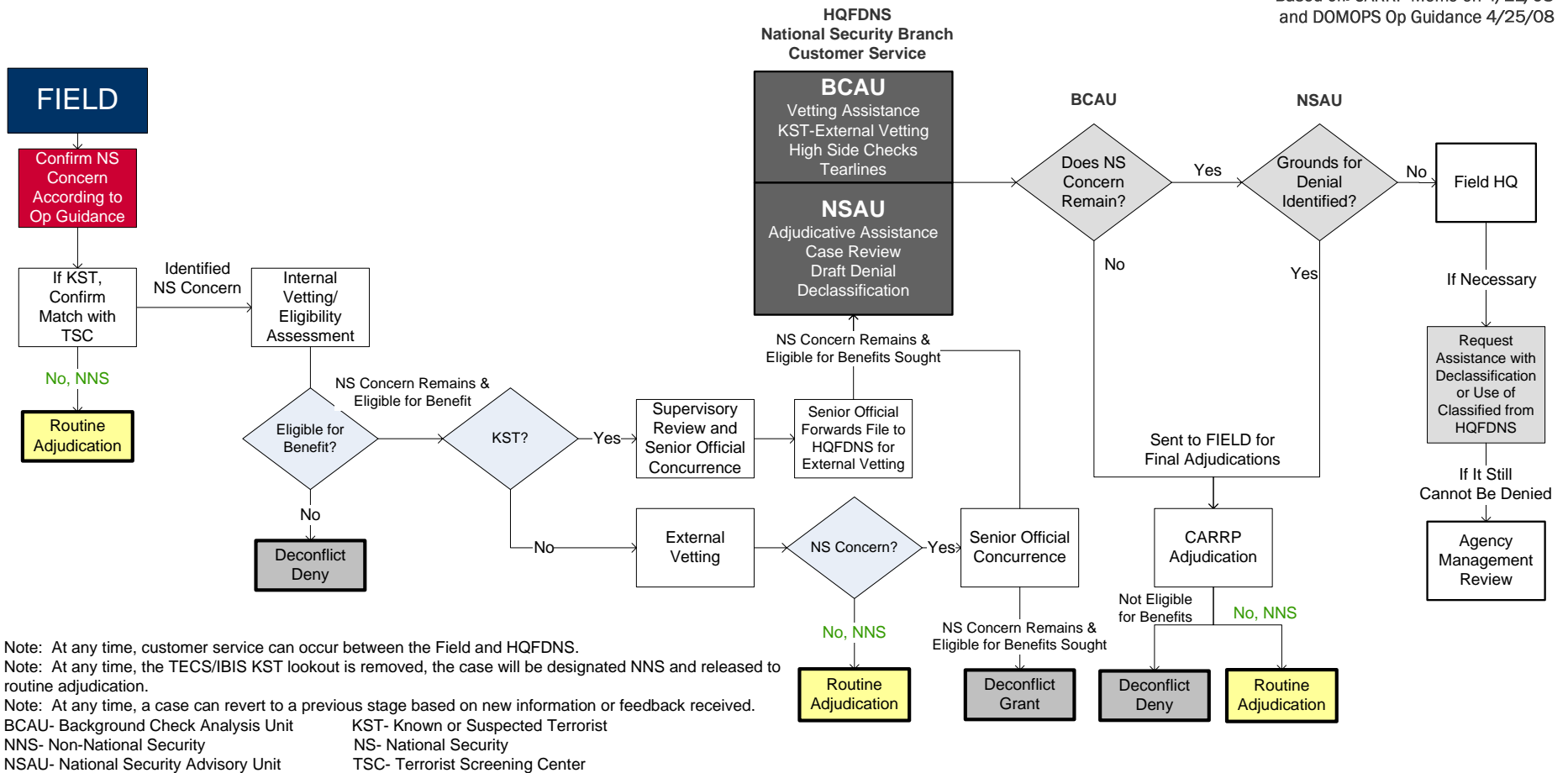
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

CARRP Workflow Overview

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



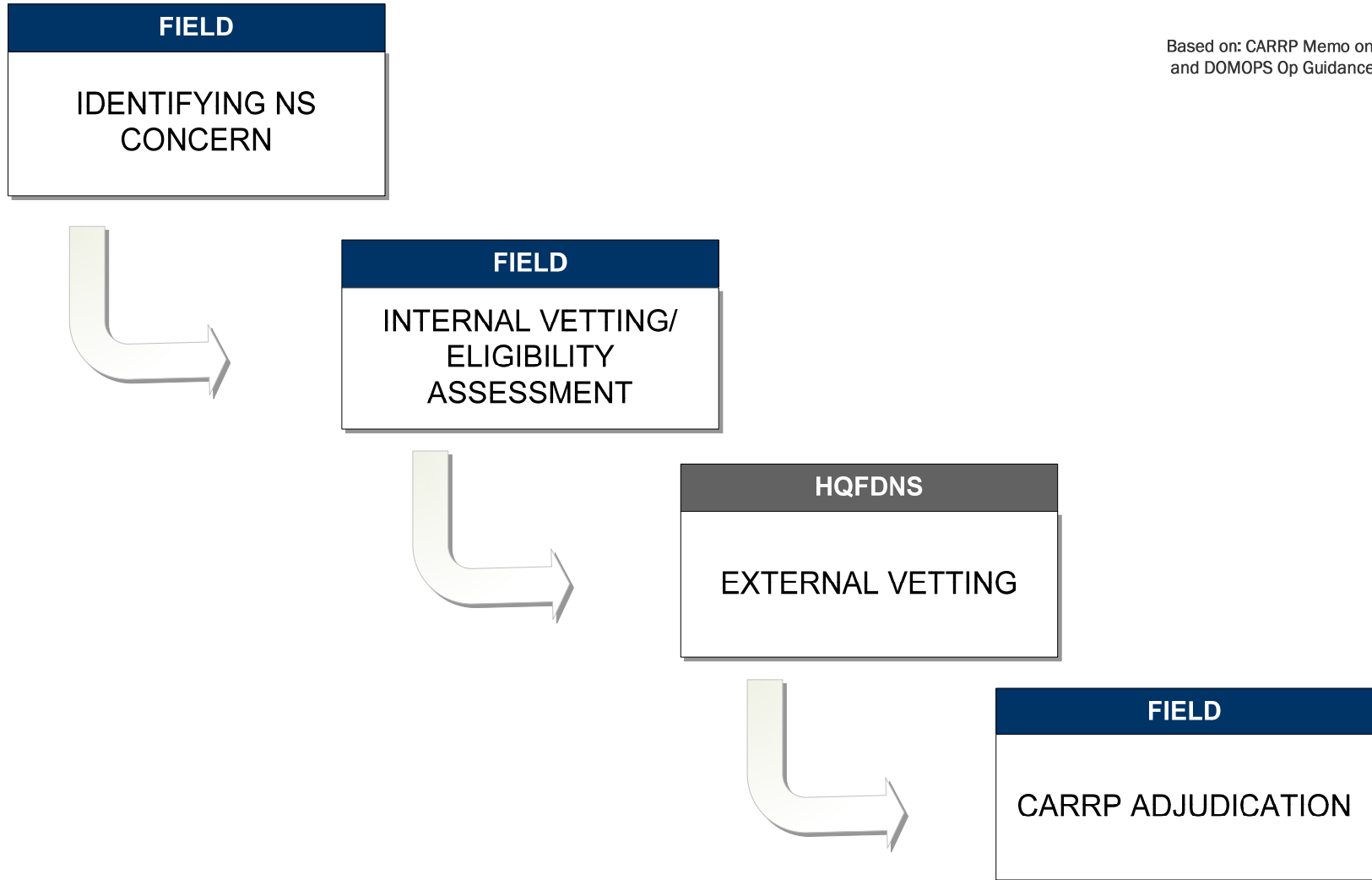
FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.



U.S. Citizenship
and Immigration
Services

High Level CARRP KST Workflow



Based on: CARRP Memo on 4/11/08
and DOMOPS Op Guidance 4/25/08

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

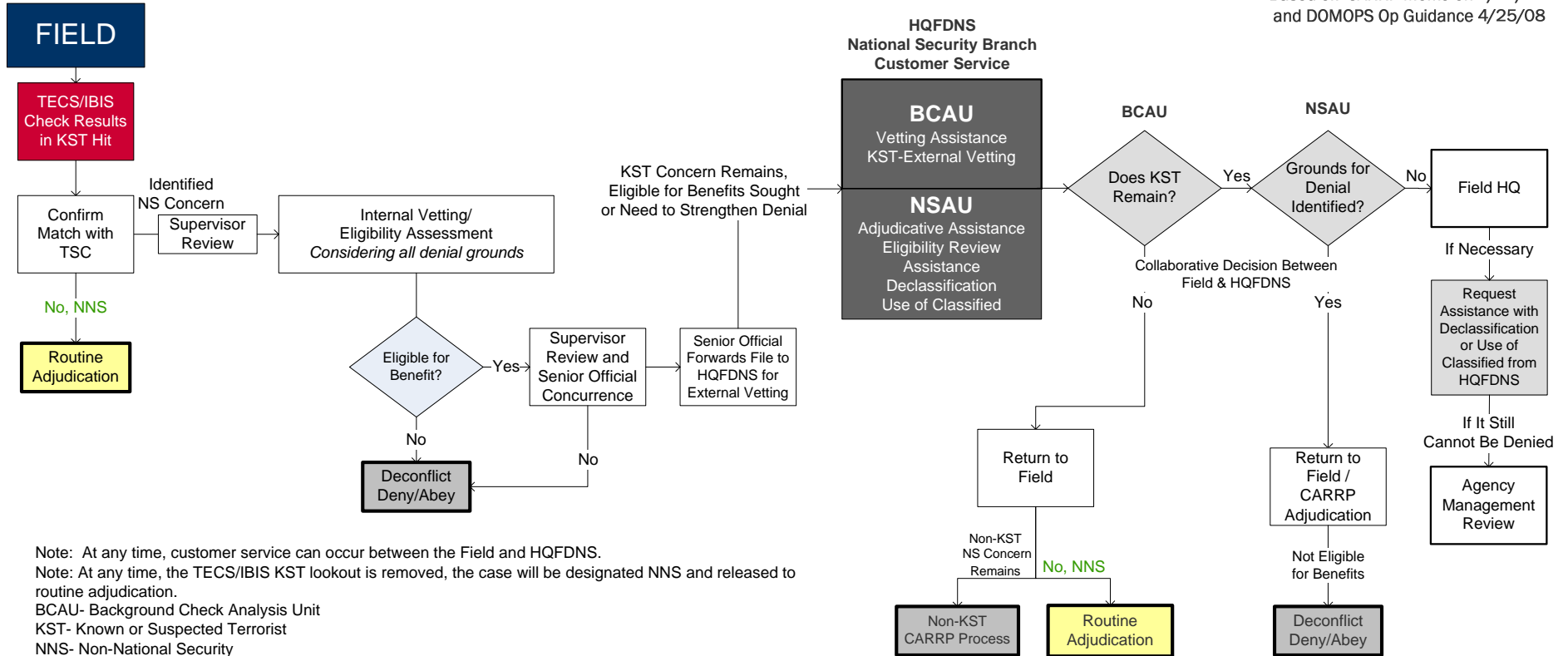
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Mid Level CARRP KST Workflow

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



Note: At any time, customer service can occur between the Field and HQFDNS.
 Note: At any time, the TECS/IBIS KST lookout is removed, the case will be designated NNS and released to routine adjudication.
 BCAU- Background Check Analysis Unit
 KST- Known or Suspected Terrorist
 NNS- Non-National Security
 NS- National Security
 NSAU- National Security Advisory Unit
 TSC- Terrorist Screening Center

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

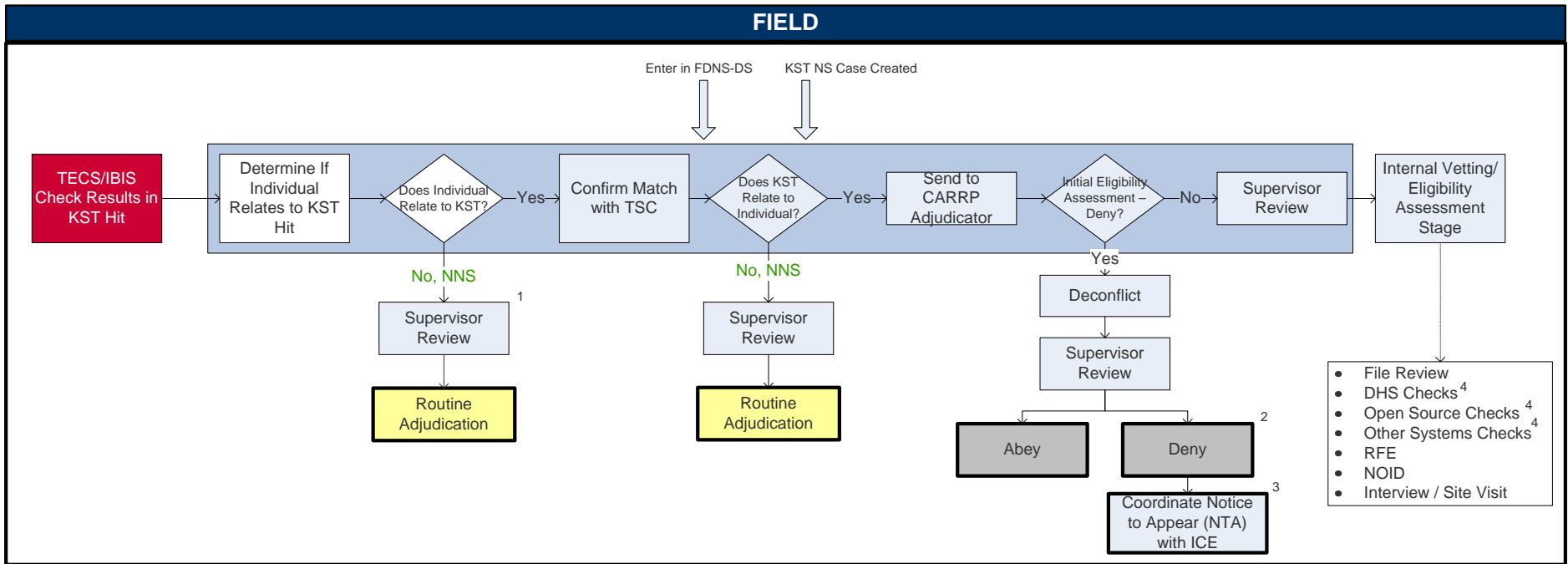
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP KST Workflow: Identifying NS Concern

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



Note: At any time, a NS Concern can be designated NNS and released to routine adjudication. Also at any time, a supervisor review can return a NS Concern or NS Case to an earlier stage in the CARRP process.

1. An IBIS Resolution Memo is produced at this point.
 2. All references to denying a case also encompass the possibility of referring an asylum case to an Immigration Judge. (CARRP Memo, p. 5)
 3. Coordinate NTA with ICE if individual is amenable to removal and present in the US.
 4. Refer to DOMOPS Ops Guidance for a full review of all security checks which can be conducted.
- Field- The Field refers to Field Offices, Service Centers, and the National Benefits Center.

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

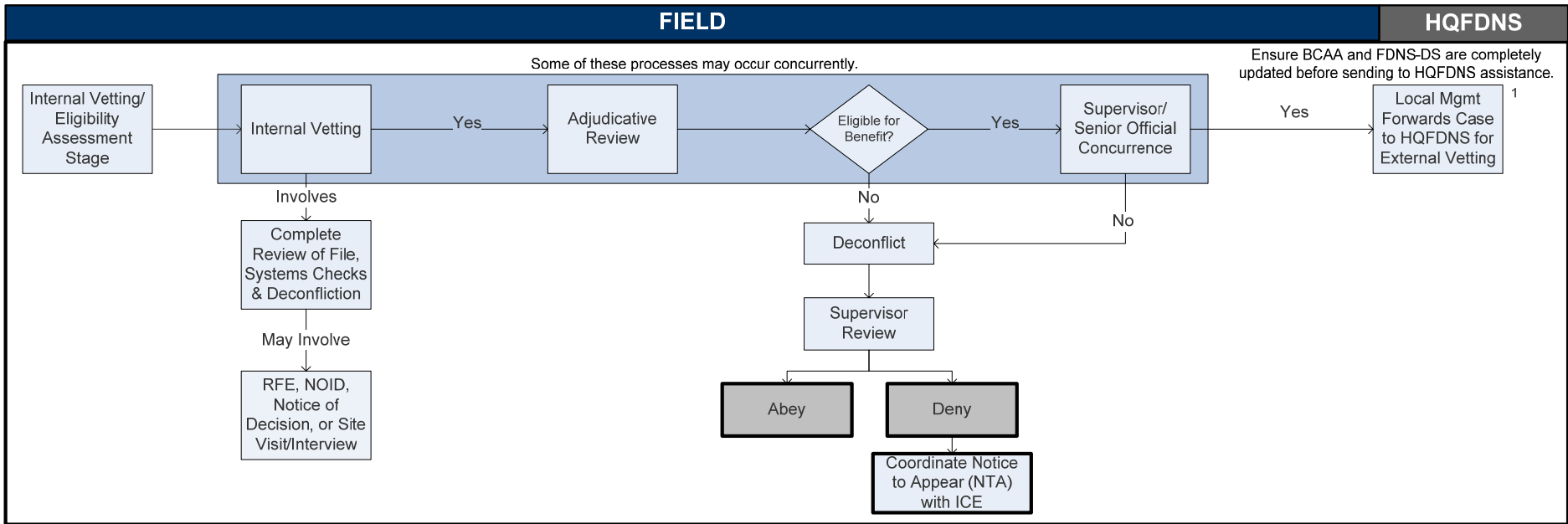
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP KST Workflow: Internal Vetting/Eligibility Assessment

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



1. Forward file after confirming subject remains on the Terrorist Watch List, documenting all adjudicative actions in FDNS-DS, and attaching completed BCAA to FDNS-DS record. As digitization occurs, files may not be physically moved up to HQFDNS, but will be digitally transferred. Refer to DOMOPS Ops Guidance for information concerning when vetting assistance may be requested from HQFDNS.

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

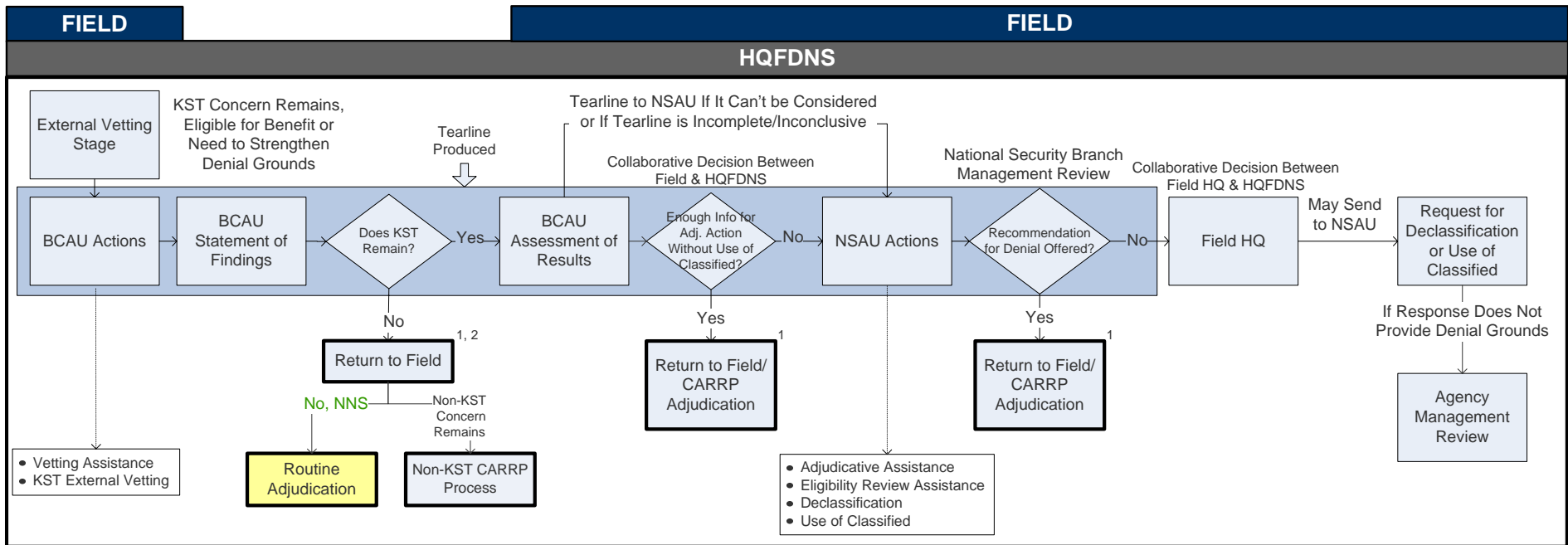
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP KST Workflow: External Vetting

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



1. HQFDNS will notify the Field of the results and what denial grounds have been identified via FDNS-DS, email, or STE/STU-III.
 2. Only returned to the Field if the LE hit has been removed.
 Note: Per DOMOPS Ops Guidance, the designated CARRP officer must notify HQFDNS whenever new factors arise that may affect the application/petition if case is at HQFDNS.

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

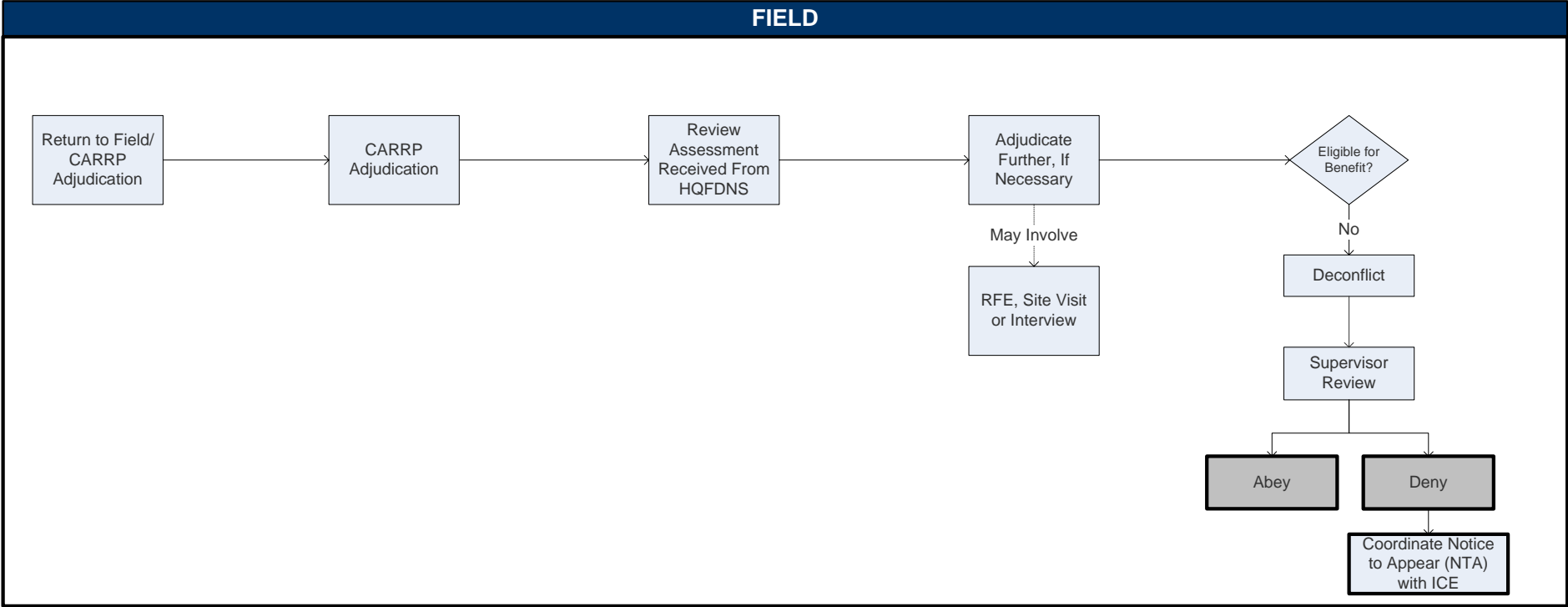
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP KST Workflow: CARRP Adjudication

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



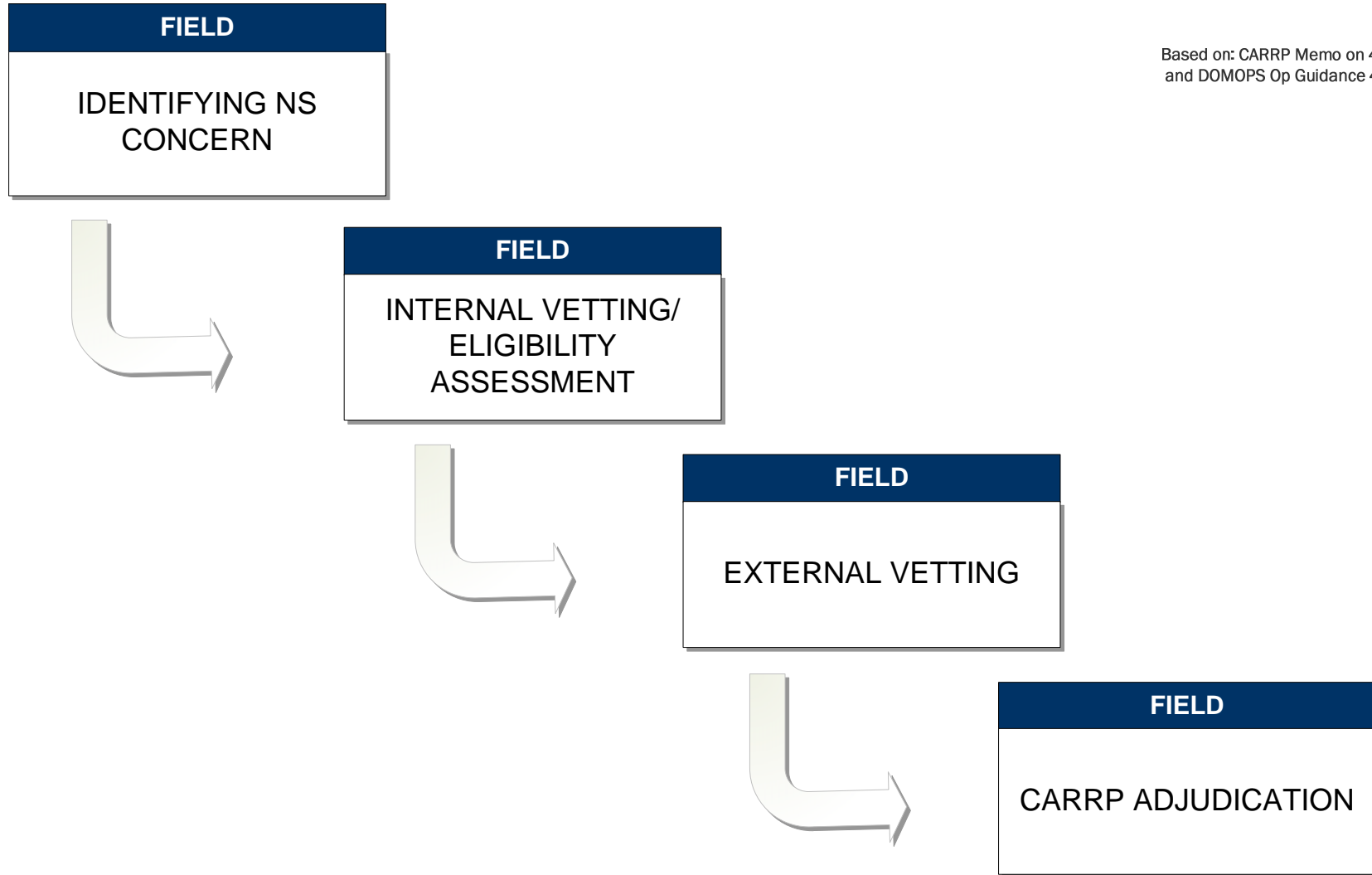
FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.



U.S. Citizenship
and Immigration
Services

High Level CARRP Non-KST Workflow



FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

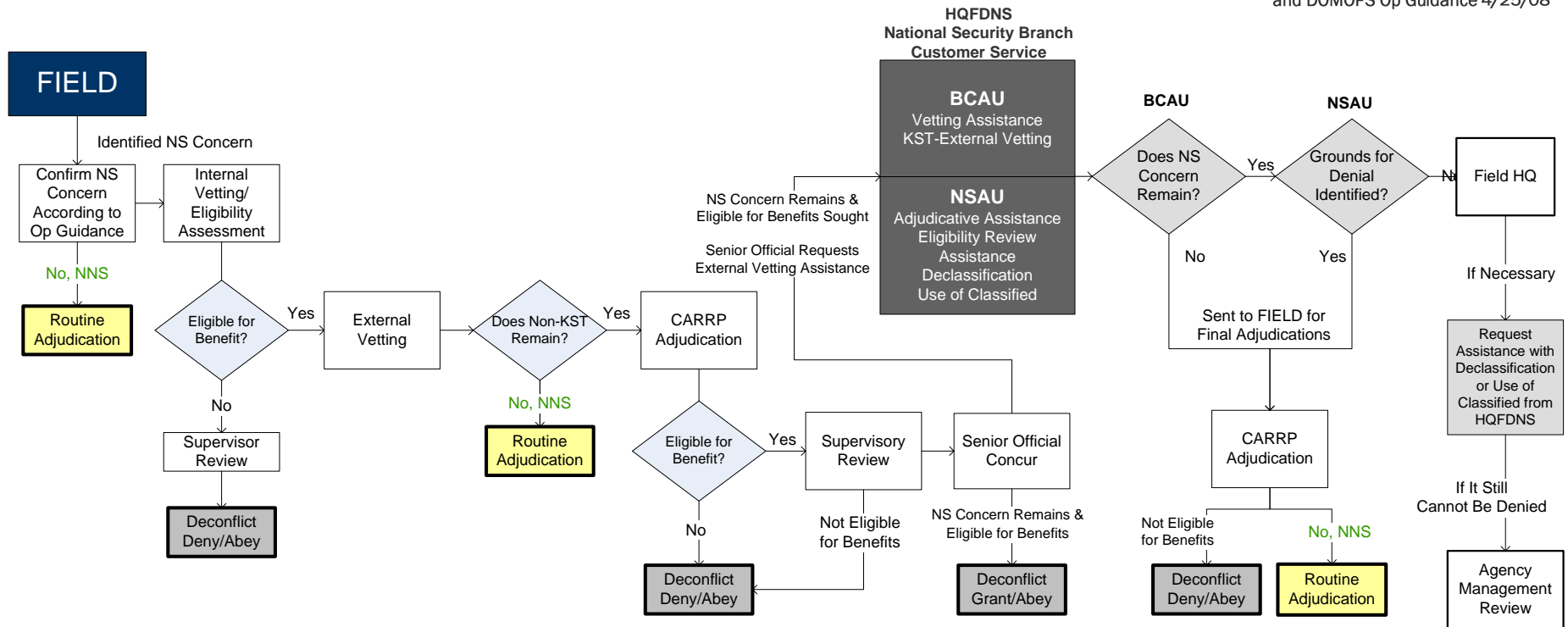
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Mid Level CARRP Non-KST Workflow

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



Note: At any time, customer service can occur between the Field and HQFDNS.
 BCAU- Background Check Analysis Unit
 KST- Known or Suspected Terrorist
 NNS- Non-National Security
 NS- National Security
 NSAU- National Security Advisory Unit

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

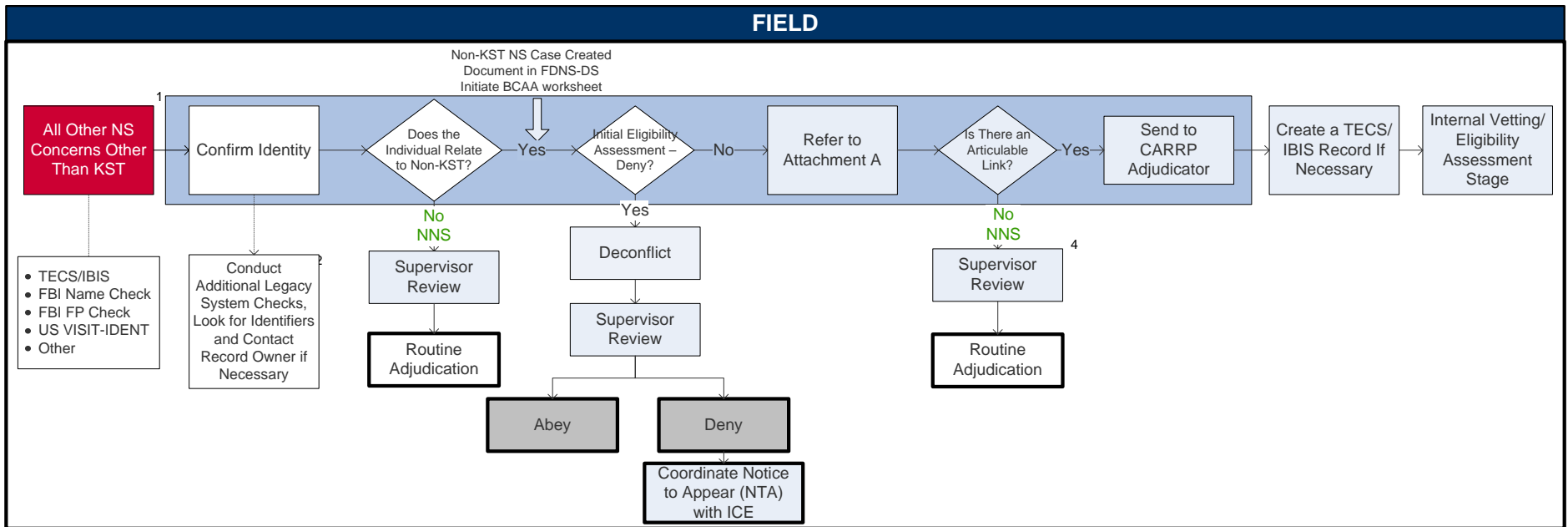
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP Non-KST Workflow: Identifying NS Concern

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



1. A Non-KST may arise as a result of a security check or at any stage of the adjudicative process. (DOMOPS Ops Guidance, p. 9)

2. Identifiers- Refer to p. 10 of DOMOPS Ops Guidance.

3. An IBIS Resolution Memo is produced at this point.

4. Update FDNS-DS will information.

Note: At any time, a KST lookout may be entered on an individual. If this occurs, the NS Case should follow the KST CARRP process. At any time, a NS Concern can be designated NNS and released to routine adjudication. Also at any time, a supervisor review can return a NS Concern or NS Case to an earlier stage in the CARRP process.

Attachment A: "Guidance for Identifying National Security Concerns" from DOMOPS Ops Guidance

Field: The Field refers to Field Offices, Service Centers, and the National Benefits Center (p. 4)

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

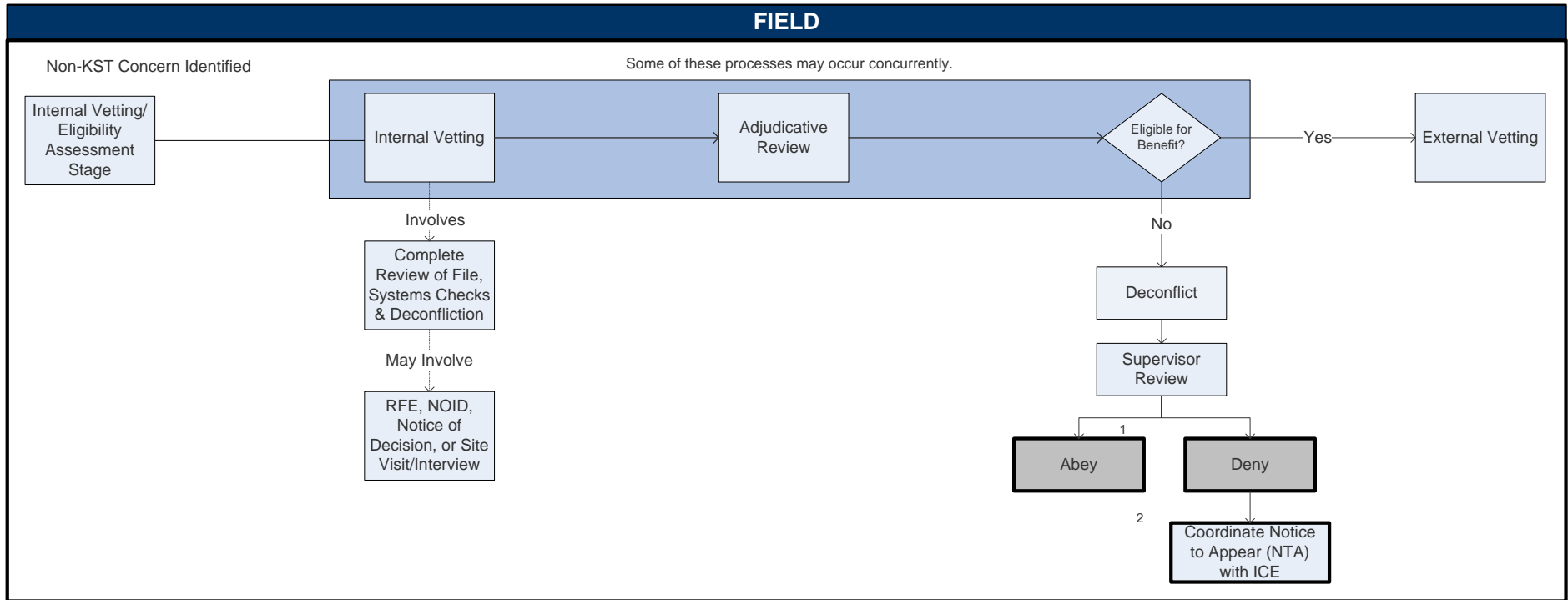
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP Non-KST Workflow: Internal Vetting/Eligibility Assessment

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



1. All references to denying a case also encompass the possibility of referring an asylum case to an Immigration Judge. (CARRP Memo, p. 5)
 2. Coordinate NTA with ICE if individual is amenable to removal and present in the US.

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

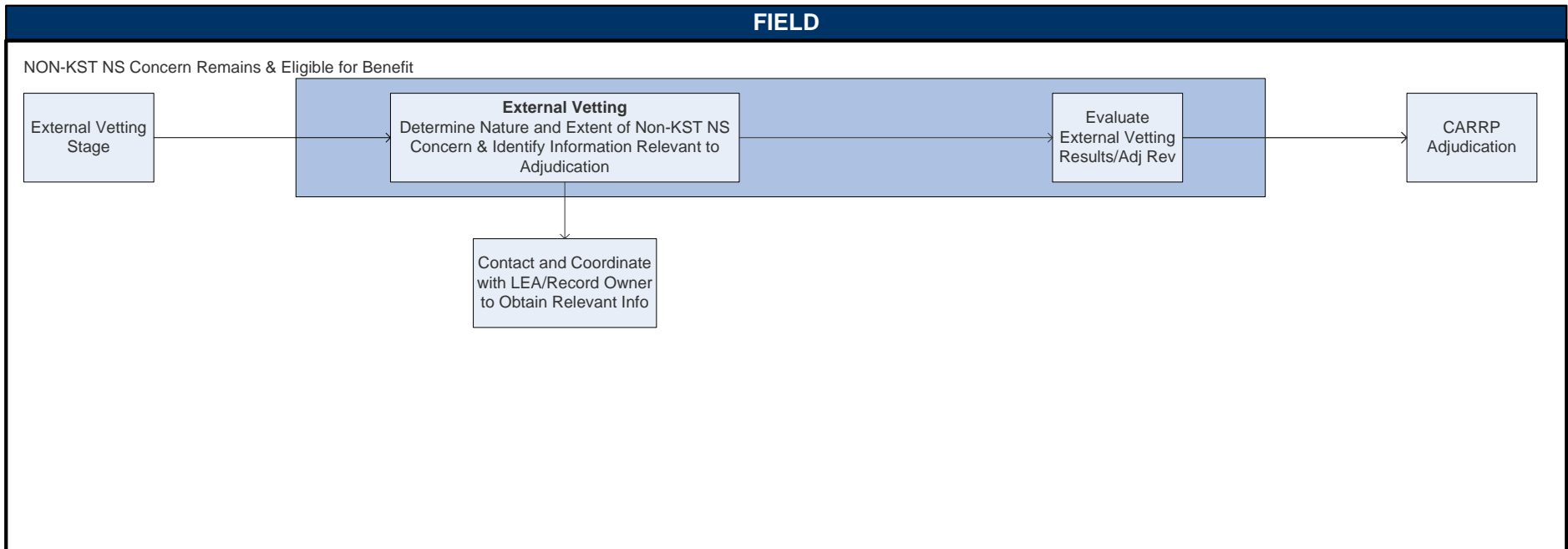
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship
and Immigration
Services

Low Level CARRP Non-KST Workflow: External Vetting

Based on: CARRP Memo on 4/11/08
and DOMOPS Op Guidance 4/25/08



LEA- Law Enforcement Agency

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

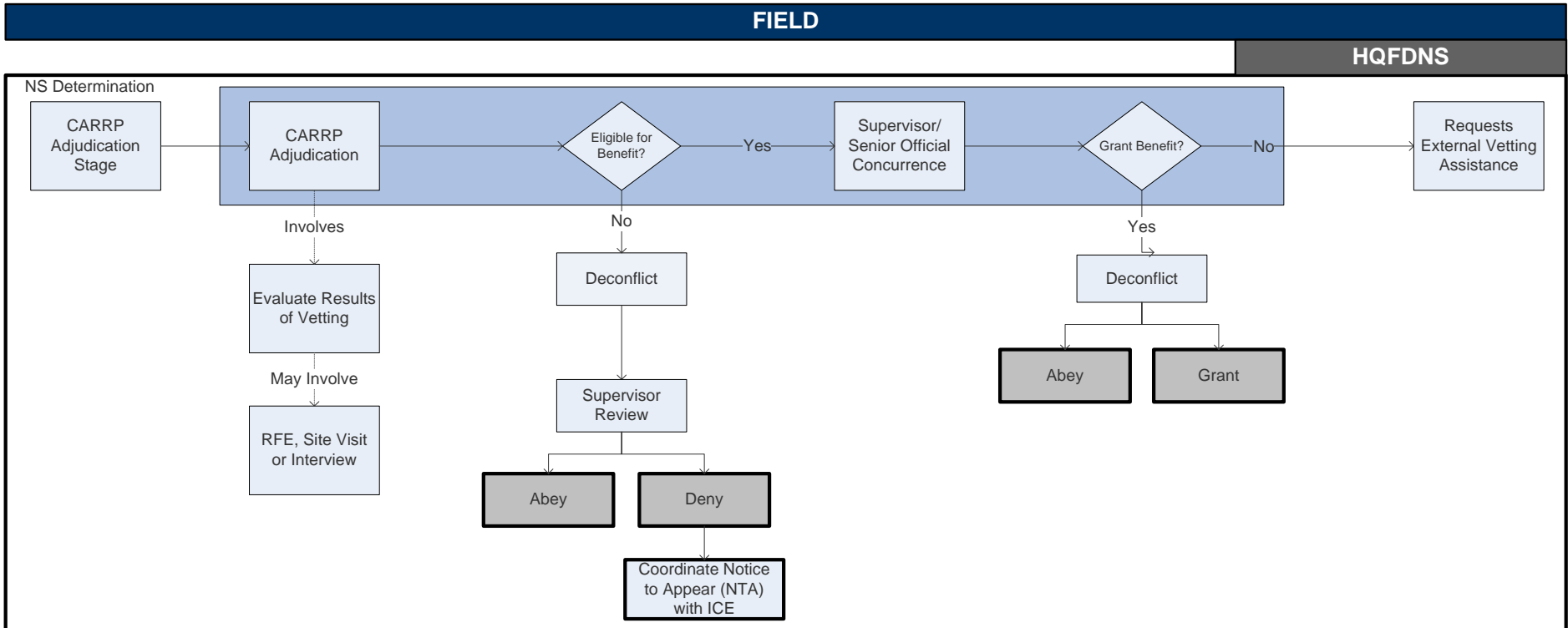
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP Non-KST Workflow: CARRP Adjudication Part I

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

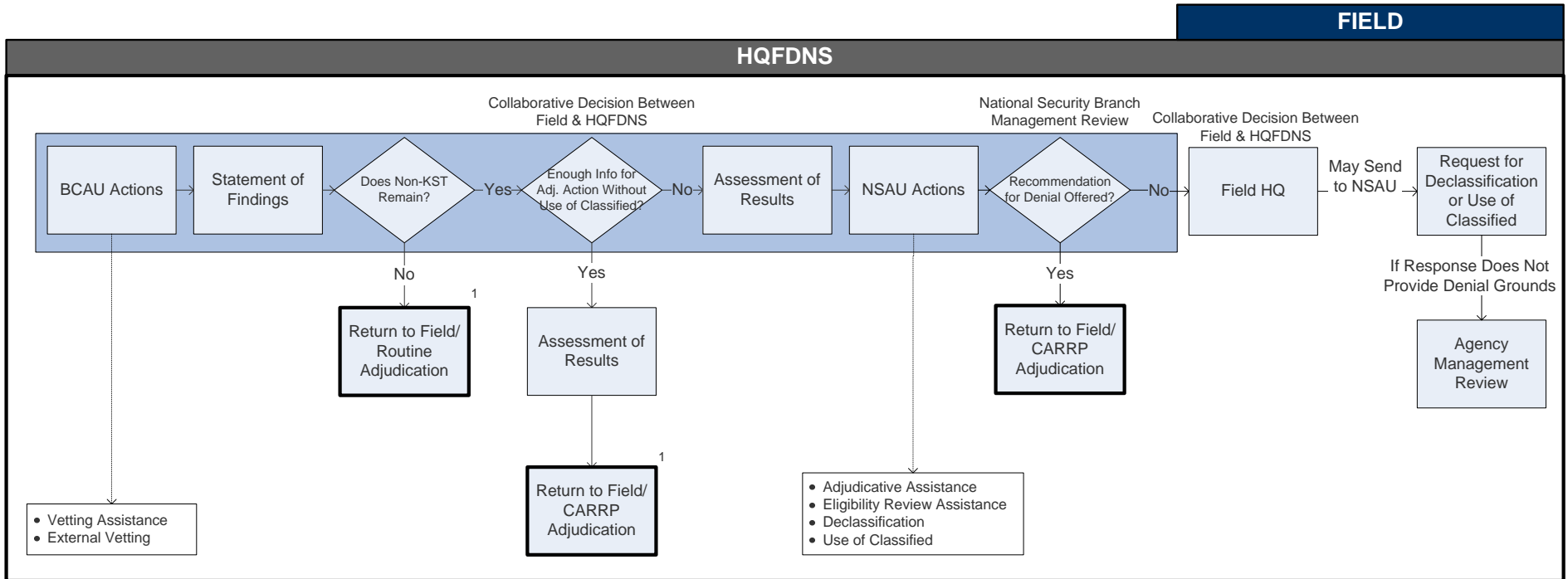
This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond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



U.S. Citizenship and Immigration Services

Low Level CARRP Non-KST Workflow: CARRP Adjudication Part II

Based on: CARRP Memo on 4/11/08 and DOMOPS Op Guidance 4/25/08



1. HQFDNS will notify the Field of results via FDNS-DS, email, or STE/STU-III.

BCAU- Background Check Analysis Unit

NSAU- National Security Advisory Unit

Field HQ- HQ Office of Field Operations (OFO) or HQ Service Operations (SCOPS) (p. 29 DOMOPS Ops 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.

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

Attachment A – Guidance for Identifying National Security Concerns

I. Introduction

USCIS seeks to ensure that immigration benefits are not granted to individuals and organizations that pose a threat to national security. It is important, therefore, that officers be able to identify certain indicators of a National Security (NS) concern. A 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 sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Immigration and Nationality Act (the Act). This includes, but is not limited to, terrorist activity; espionage; sabotage; and the illegal transfer of goods, technology, or sensitive information.

The officer should consider the *activities, individuals, and organizations* described in sections 212(a)(3)(A), (B), and (F), and 237(a)(4)(A) and (B) of the Act as examples of indicators of a NS concern and for determining whether a NS concern exists. When evaluating whether a NS indicator or NS concern exists, however, the facts of the case do not need to satisfy the legal standard used in determining admissibility or removability. This guidance provides examples of indicators of a NS concern that are intended as signals to alert the officer to consider the totality of circumstances in determining whether a NS concern exists. While this document is not exhaustive, it is intended to serve as a reference tool for all officers when evaluating cases that may have NS concerns.

This guidance does not apply to one type of NS concern: Known or Suspected Terrorist (KST) NS hits,¹ which automatically indicate the presence of a NS concern. Rather, officers must refer to this guidance when assessing whether a *Non-KST* NS concern exists in any given case. The Non-KST category refers to all other NS concerns, regardless of source, including but not limited to: associates of KSTs, unindicted co-conspirators, terrorist organization members, persons involved in providing material support to terrorists or terrorist organizations, and agents of foreign governments. Individuals and organizations that fall into this category may also pose a serious threat to national security.

¹A **Known or Suspected Terrorist (KST)** is a category of individuals who have been nominated and accepted for placement in the Terrorist Screening Database (TSDB), are on the Terrorist Watch List, and have a specially-coded lookout posted when queried in TECS/IBIS, and/or the Consular Lookout Automated Support System (CLASS), as used by the Department of State.

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

1

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

CAR000084

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

II. Process for Identifying Cases that May Include a NS Concern

At any stage of the screening or adjudicative processes, an officer may identify an indicator of a NS concern with respect to an individual or organization. Such information may be identified through the following:

- Security check results, e.g., information obtained from FBI Name Checks, FBI Fingerprint Checks, The Enforcement Communications System/Interagency Border Inspection System (TECS/IBIS), Consular Lookout Automated Support System (CLASS), Department of State Security Advisory Opinions (SAOs), United States Visitor and Immigrant Status Indicator Technology/Automated Biometric Identification System (US-VISIT/IDENT), and other system checks;
- Testimony elicited during an interview;
- Review of the petition or application, supporting documents, the A-file, or related files;
- Leads from other US Government agencies or foreign governments; and
- Other sources, including open source research.

Once an indicator is identified, the officer must evaluate whether a NS concern exists. The officer must consider the totality of circumstances to determine whether an articulable link exists between the individual or organization and prior, current, or planned involvement in, or association with, an activity, individual, or organization described in sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Act.

III. Indicators of a NS Concern

An indicator of a NS concern may be identified at any stage of the screening or adjudicative processes through the review of USCIS security checks, file information, site visit results, and any other relevant sources. The guidance below provides examples of indicators of a NS concern that appear in the Act and in non-statutory sources.

A. Statutory Indicators

1. Sections 212(a)(3)(A), (B), and (F), and 237(a)(4)(A) and (B) of the Act contain comprehensive definitions of activities (including inchoate acts of threat, attempt, or conspiracy), associations, and organizations that may imply NS concerns:
 - “Terrorist Activity” is defined at section 212(a)(3)(B)(iii) of the Act.
 - Conduct that constitutes “engaging” in terrorist activity is defined at section 212(a)(3)(B)(iv) of the Act.
 - “Terrorist Organizations” are defined at section 212(a)(3)(B)(vi) of the Act. See the Department of State website (www.state.gov/s/ct/list/) for lists of Tier I and Tier II

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

2

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

CAR000085

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

terrorist organizations. See the Department of Treasury listing of Specially Designated Global Terrorist Entities pursuant to Executive Order 13224 (www.state.gov/s/ct/list/) for some organizations likely to meet the Tier III undesignated terrorist organization definition.

2. Other sections of the Act whose reference in a record may imply NS concerns, and therefore may require further research to determine whether NS concerns exist, include:
 - 208(b)(2)(A) Exceptions to Asylum Eligibility;
 - 212(a)(2)(D) Inadmissible Aliens – Money Laundering;
 - 221(i) Issuance of visas – Revocation of visas or other documents;
 - 235(c) Removal of aliens inadmissible on security and related grounds;
 - 236A Mandatory detention of suspected terrorists; habeas corpus; judicial review; and
 - 237(a)(2)(D) Deportable Aliens – Miscellaneous crimes.

B. Non-Statutory Indicators

1. Employment, Training, or Government Affiliations

Certain types of employment, training, government affiliation, and/or behavior may (or may not) be indicators of a NS concern, depending on the circumstances of the case, and require additional scrutiny to determine whether a NS concern exists. For 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. Officers may also need to consider proficiency in particular technical skills gained through formal education, training, employment, or military service, including foreign language or linguistic expertise, as well as knowledge of radio, cryptography, weapons, nuclear physics, chemistry, biology, pharmaceuticals, and computer systems.

2. Other Suspicious Activities

Certain other types of suspicious activities 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. These include but are not limited to:

- Unusual travel patterns and travel through or residence in areas of known terrorist activity;
- Criminal activities such as fraudulent document manufacture; trafficking or smuggling of persons, drugs, or funds; or money laundering;
- Large scale transfer or receipt of funds; and

FOR OFFICIAL USE ONLY (FOUO) – LAW ENFORCEMENT SENSITIVE

3

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

CAR000086

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

- Membership or participation in organizations that are described in, or that engage in, activities outlined in sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Act.

3. Family Member or Close Associate

In some instances, the officer may be aware that the petitioner, beneficiary, applicant, dependent, or derivative is a family member or close associate of a subject with a NS concern. Such information may impact the individual's eligibility for the benefit sought and/or may indicate a NS concern with respect to 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.

C. Indicators of a NS Concern as Contained in Security Check Results

1. FBI Name Check

The following terms may be contained in FBI name check responses (Letterhead Memoranda (LHMs)). They relate to law enforcement investigations,² and are examples of indicators of a NS concern:

- Foreign Counterintelligence
- Acts of Terrorism
- International Terrorism
- Domestic Terrorism
- Hostage-Taking - Terrorism
- Money Laundering or suspicious financial transactions with some link to a NS activity
- Violations of Arms Control Treaty Measures
- Sabotage
- Bombings and Explosives Violations
- Threats or Attempts to Use, Possess, Produce, or Transport Weapons of Mass Destruction (WMD)
- Use, Possession, Production, or Transport of WMD

² Please note that reference to a “closed” law enforcement investigation does not necessarily mean that there is no NS concern or that the NS concern was resolved during the course of the investigation. Law Enforcement Agencies (LEAs) close investigations for a number of reasons, some substantive and others administrative. Officers need to gather additional information to determine whether a NS concern remains despite closure of an investigation.

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

4

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

CAR000087

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

Exception: In some instances, a LHM may indicate that upon completion and closure of the investigation, the case agent made a definitive finding of no nexus to national security in relation to the USCIS subject. No NS concern exists if the LHM indicates a definitive finding of no nexus to national security to the USCIS subject, and no other indicator of a NS concern exists.

2. FBI Fingerprint or NCIC Criminal History Check (NN16):³

The following are examples of indicators of a NS concern present in responses to the FBI Fingerprint Check or the NCIC Criminal History Check:

- Classified by the Attorney General as a known terrorist;
- 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; or
- Arrested/detained by the U.S. military overseas (e.g., detainees in Iraq or Guantanamo).

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.

3. US-VISIT/IDENT

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

IV. TECS/IBIS

The following TECS/IBIS and NCIC Status Codes and Code Descriptions may (or may not) be indicators of a NS concern, depending on the circumstances of the case. Further inquiry by the officer is needed. These codes should not be considered a complete list of codes that the officer may encounter. The officer must verify any unfamiliar codes encountered.

³ See CIS policy memorandum, *Accessing National Crime Information Center Interstate Identification Index (NCIC III) Data*, dated June 3, 2005 indicating that “it is acceptable and in fact necessary to conduct an NCIC III query when fraud is articulated, or when background check processes, interviews, and/or informants indicate national security concerns or that an applicant may have a criminal record or may be involved in criminal activity.”

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

5

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

CAR000088

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

TECS/IBIS TABLE CODE CODE DESCRIPTION

LE

NCIC OFFENSE CODE CODE DESCRIPTION

LE

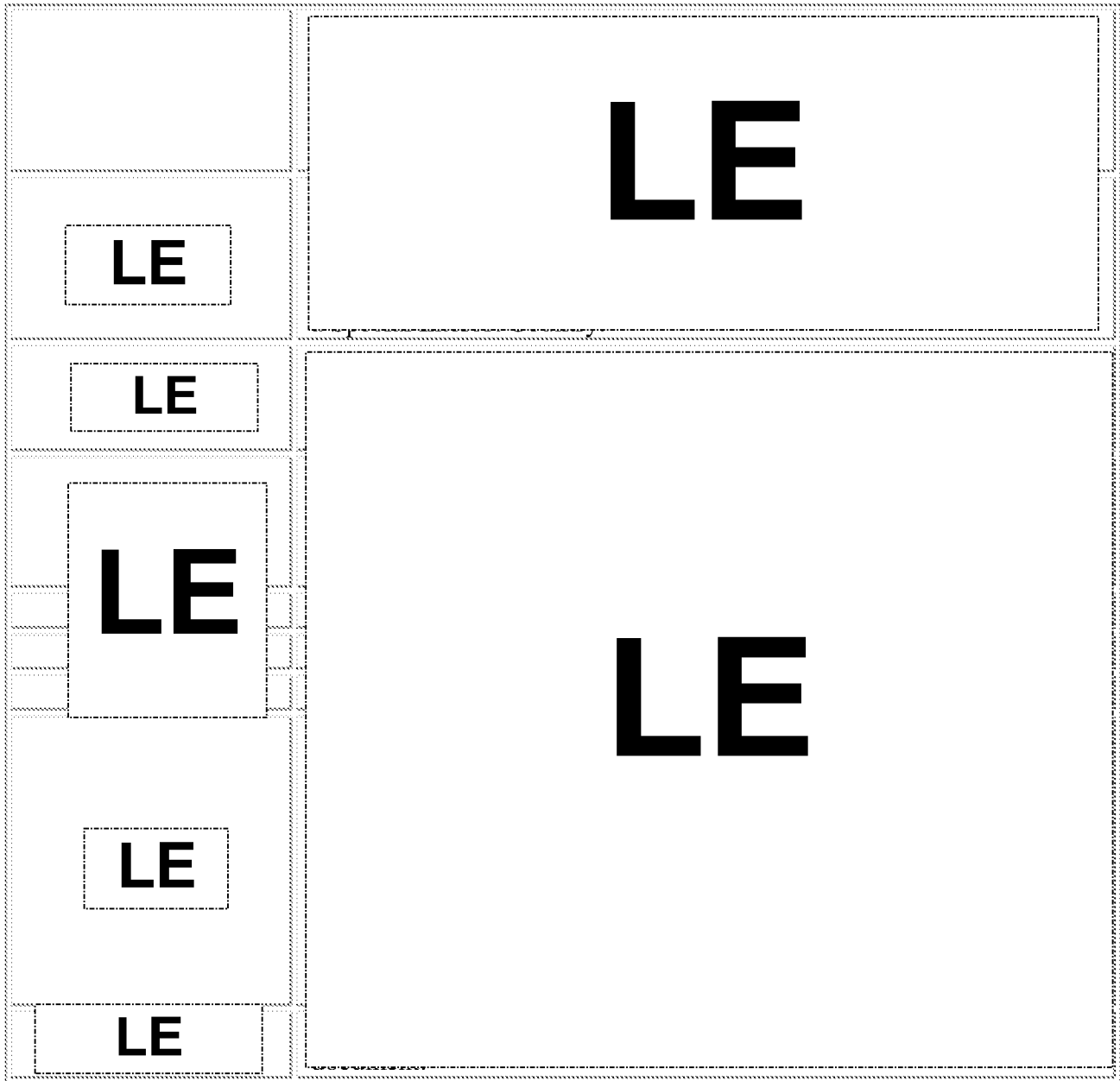
The following table contains terms and acronyms related to TECS/IBIS which may (or may not) be indicators of a NS concern, depending on the circumstances of the case. Further inquiry by the officer is needed.

CTR	Counter-Terrorism Response; this indicates that the subject has been identified, referred by or to a CTR team as a possible terrorist interest.
LE	LE
LE	LE
LE	LE
LE	LE
LE	LE
LE	LE

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE



FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

CAR000090

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

LE

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

8

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS 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.

CAR000091

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

LE

TIDE

Terrorist Identities Datamart Environment. This refers to a counter-terrorism database that coordinates the use of sensitive interagency intelligence for watch listing terrorists. This database was formerly known as TIPOFF and managed by the Department of State.

LE

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of Domestic Operations Directorate
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

HQ 70/23 & 70/28.1

FEB - 9 2009

Memorandum

TO: Field Leadership

FROM: Donald Neufeld 
Acting Associate Director, Domestic Operations

SUBJECT: National Security Adjudication and Reporting Requirements-Update

Background

U.S. Citizenship and Immigration Services (USCIS) conducts background checks on all applicants, petitioners and beneficiaries seeking immigration benefits.

On February 4, 2008, USCIS issued a memorandum advising USCIS officers that if the following types of applications were otherwise approvable, and the name check request was still pending with the FBI for more than 180 days, the application shall be approved.

- Form I-485, Application for Adjustment of Status ,
- Form I-601, Application for Waiver of Ground of Inadmissibility,
- Form I-687, Application for Status as a Temporary Resident Under Section 245A of the Immigration and Nationality Act, or
- Form I-698, Application to Adjust Status from Temporary to Permanent Resident (Under Section 245A of Public Law 99-603).

USCIS issued this guidance in response to a DHS Office of Inspector General (OIG-06-06) recommendation that the agency conform its background and security check policies with those of U.S. Immigration and Customs Enforcement (ICE).

Over the past year, the FBI has worked diligently to ensure that definitive FBI name check results are returned to USCIS in less than 180 days. In fact, the FBI is currently returning name check results on average in 90 days. Few, if any, name checks remain pending at the FBI for 180 days. In light of FBI's improved processing and response times, USCIS is revising its policy of automatic approval of certain cases after 180 days. Effective immediately, adjudicators will be

www.uscis.gov

Confidential - Subject to Protective Order

CAR000093

National Security Adjudication and Reporting Requirements-Update
Page 2

required to contact Headquarters to obtain authorization to approve the pending I-485, I-601, I-687, or I-698 prior to receiving the FBI name check results.

Implementation

This memorandum supersedes the February 4th, 2008, memorandum and is effective immediately. USCIS is also retracting the earlier released, January 22, 2009, memorandum that includes an identical subject line. Questions regarding this memorandum should be directed through appropriate supervisory and operational channels. Local offices should work through their chain of command.

Revised Guidance

A definitive FBI fingerprint check and the IBIS check must be obtained and resolved before an Application for Adjustment of Status (I-485), Application for Waiver of Ground of Inadmissibility (I-601), Application for Status as a Temporary Resident Under Section 245A of the Immigration and Nationality Act (I-687), or Application to Adjust Status from Temporary to Permanent Resident (Under Section 245A of Public Law 99-603)(I-698) is approved.

USCIS will continue to initiate FBI name checks when those applications are received. Where the application is otherwise approvable and the FBI name check has been pending for more than 150 days, the adjudicator shall notify a designated point of contact at Headquarters. The Headquarters point of contact will reach out to the FBI to determine the reason for the FBI name check processing delay. HQDOMO will then provide the adjudicating officer with case specific guidance, including where appropriate authorization to approve the pending I-485, I-601, I-687, or I-698 prior to receiving the FBI name check results.

As described in the February 4, 2008, memorandum, if derogatory or adverse information is received from the FBI after the application is approved, USCIS will determine if rescission or removal proceedings are appropriate and warranted.

There is no change in the requirement that FBI fingerprint check, IBIS check, and FBI name check results must be obtained and resolved prior to approval of an Application for Naturalization (N-400).

Distribution List:
Regional Directors
Service Center Directors
District Directors (except foreign)
Field Office Directors (except foreign)
National Benefits Center Director

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of Field Operations
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

JUN - 5 2009

HQ 70/43

Memorandum

TO: Field Leadership
FROM:  Donald Neufeld
Acting Associate Director, Domestic Operations

SUBJECT: Clarification and Delineation of Vetting and Adjudication Responsibilities for Controlled Application Review and Resolution Program (CARRP) Cases in Domestic Field Offices

I. Purpose

The purpose of this memorandum is to provide guidance to define the vetting and adjudication responsibilities for Controlled Application Review and Resolution Program (CARRP) cases in the domestic Field Offices. It outlines the distinctions between the duties and responsibilities of Fraud Detection and National Security – Immigration Officer (FDNS-IO) and CARRP-trained Immigration Services Officer (CARRP-ISO). It also explains the roles of Supervisory Immigration Services Officer (SISO) and FDNS-Supervisory Immigration Officer (FDNS-SIO) at each field office.

II. Background

On April 11, 2008, USCIS released the memorandum, *Policy for Vetting and Adjudicating Cases with National Security Concerns* (CARRP memo). This memo instituted the CARRP process, a disciplined approach for identifying, recording, and adjudicating applications and petitions where a National Security (NS) concern is identified. CARRP involves four unique, but overlapping, processing steps. These include:

1. Identifying a NS Concern
2. Assessing Eligibility in Cases with a NS Concern, consisting of:
 - i. Eligibility Assessment
 - ii. Internal Vetting
3. External Vetting
4. CARRP Adjudication

Moreover, CARRP decentralized the process of vetting and adjudicating cases with NS concerns. Prior to CARRP, all such cases were handled at the Headquarters Office of Fraud Detection and National Security (HQFDNS). With the release of CARRP, responsibility for vetting and

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

2

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

adjudicating most cases with NS concerns was placed with Field Offices, allowing USCIS to leverage field resources and experienced officers for handling these difficult cases.

After the release of the CARRP memo, Domestic Operations (DomOps), Refugee Affairs Division, International Operations, and the Asylum Division issued separate, but coordinated, Operational Guidance for the implementation of CARRP within their programs. The following guidance is provided to help define the vetting and adjudication responsibilities for CARRP cases in the Domestic Operations Field Offices.

III. Policy Guidance

The current *Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns (Operational Guidance)*, issued by Domestic Operations, provides general guidelines for the processing of cases with National Security (NS) concerns under CARRP, stating the various steps of the process will be completed by a “designated officer”

While the *Operational Guidance* states that a “designated officer” may be “an Immigration Analyst, Immigration Officer, Adjudications Officer, Asylum Officer or Refugee Officer,” the Office of Field Operations (OFO) is issuing this memorandum in order to establish the assignment of specific CARRP duties and responsibilities to the FDNS-IOs and the CARRP-ISOs who perform CARRP adjudications within each Field and District Office or on temporary duty at a Field or District Office. Per the *Operational Guidance*, a Field Office Director (FOD) will designate a specific Immigration Services Officer(s) to be trained in both CARRP procedures and the use of the Fraud Detection and National Security Data System (FDNS-DS).

In addition, the memorandum entitled, *Actions to be Taken to Standardize CARRP File Identification and the Movement of CARRP Cases Between the Components of USCIS*, dated March 26, 2009, authorizes the FOD to also designate one or more SISOs in each Field Office to perform some or all of the duties described herein for a SISO if he or she chooses. The SISO will play a central role in managing the CARRP process by coordinating the movement of CARRP files, assigning CARRP cases to a CARRP-ISO for adjudication, and providing supervisory concurrence for final adjudication of CARRP cases. Additionally, the FOD will outline local procedures regarding supervision, coordination and actions of the FDNS-IO and CARRP-ISO when there is no FDNS-Supervisory Immigration Officer (FDNS-SIO) located in the Field Office.

Clarification of Duties and Responsibilities within the CARRP Process:

As mentioned earlier, The *Operational Guidance* breaks down the CARRP process into four steps.

1. Identifying a NS Concern – Step 1 of CARRP Process:

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

3

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

As noted in section III of the *Operational Guidance*, indicators of a NS concern may be identified at any time during the adjudicative processing of an application or petition. When such an indicator is noted for a case within a Field Office, the FDNS-IO is responsible for completing the identification of the NS concern. To do this, the FDNS-IO does the following:

LE

More detailed guidelines on completing the identification of a NS concern are available in the *Operational Guidance*, section III.

In many instances, CARRP cases received in a Field Office will have gone through Step One of the *Operational Guidance*, “Identifying a NS Concern” at either a Service Center or the National Benefits Center (NBC). In such cases, the SISO overseeing the CARRP process in each Field Office will coordinate with the FDNS-SIO, if available, or follow local procedures to have the case assigned to the appropriate FDNS-IO for Step Two of the *Operational Guidance*, “Assessing Eligibility in Cases with a NS Concern.” The SISO will also assign a CARRP-ISO to adjudicate the application or petition in each CARRP case.

2. Assessing Eligibility in Cases with a NS Concern – Step 2 of CARRP Process:

Step 2 of the *Operational Guidance* includes both an *eligibility assessment* and *internal vetting* of the CARRP case. The purpose of Step 2 is two-fold: First, it is at this point in the CARRP process where both the FDNS-IO and the CARRP-ISO are required to thoroughly review the case file. The FDNS-IO completes required systems checks and internal vetting, and the CARRP-ISO completes an eligibility assessment of the CARRP case to determine whether any statutory or regulatory ineligibility exist. Second, specific questions and issues are compiled by both the FDNS-IO and the CARRP-ISO for discussion with the Record Owner of the NS hit so that the critical decisions, such as when an interview should be scheduled, can be made regarding adjudicating the application or petition.

The FOD in each Field Office will decide on the workflow of the CARRP case for this step of the CARRP process. More detail about the features of the elements of step two are described below:

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

4

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

a. The Eligibility Assessment

The CARRP-ISO assigned to adjudicate the CARRP case will conduct a complete review of the case file in order to assess the individual's eligibility for the benefit sought and identify any questions and/or issues for discussion with the Record Owner during deconfliction. **Any denial** at this stage in the CARRP process shall be issued **only** after proper deconfliction, completion of required systems checks and supervisory concurrence. No denial shall be issued at this stage in the CARRP process based solely on discretionary grounds. See Section IV, "Assessing Eligibility in Cases with a NS Concern – Step 2 of CARRP Process" of the *Operational Guidance*. **The CARRP-ISO is responsible for documenting their actions related to the adjudication process in FDNS-DS at all stages of the adjudications process.**

b. Internal Vetting

The FDNS-IO is responsible for conducting the internal vetting of a CARRP case. This includes a complete review of the file to obtain any relevant information to support the adjudication, to perform the required systems checks, ensuring all systems checks are current, and, in some cases, to further examine the nature of the NS concern. A complete list of both the required and suggested systems checks which are a part of the internal vetting process can be found in Section IV, "Assessing Eligibility in Cases with a NS Concern – Step 2 of CARRP Process" of the *Operational Guidance*. **The FDNS-IO is responsible for documenting his or her actions in FDNS-DS throughout the CARRP process.**

As in the Eligibility Assessment part of this step, **any denial** at this stage in the CARRP process shall be issued **only** after proper deconfliction, completion of required systems checks and supervisory concurrence. No denial shall be issued at this stage in the CARRP process based solely on discretionary grounds. See Section IV, "Assessing Eligibility in Cases with a NS Concern – Step 2 of CARRP Process" of the *Operational Guidance*.

Performance of the eligibility assessment, internal vetting and deconfliction processes must be closely coordinated between the CARRP-ISO and the FDNS-IO. The FOD or SISO must ensure that there is efficient communication between CARRP-ISOs and FDNS-IOs so that mistakes are not made.

c. Deconfliction

As the Field Office's primary point of contact and liaison with Law Enforcement Agencies (LEA), the FDNS-IO is responsible for deconfliction with the Record Owner

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

5

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

for all CARRP cases. FDNS-IOs are reminded that deconfliction may be necessary at any stage of the CARRP process and that deconfliction may need to be completed more than once before the final adjudication of a CARRP case. Again, this emphasizes the need for the FDNS-IO to maintain efficient communication with the appropriate CARRP-ISO and the SISO.

When contacting an LEA, it is also important for FDNS-IOs to remember that they must be careful to observe all security and special handling precautions in accordance with DHS and originating Record Owner requirements. Maintaining good security protocols promotes close and productive relationships with USCIS' law enforcement partners.

As per the *Operational Guidance*, the FDNS-IO may ask the Record Owner whether their agency has additional information (other than NS related information) that would affect the eligibility for the benefit sought. The FDNS-IO may also seek to resolve any other relevant concerns (i.e., criminal, public safety, fraud) identified through the security check process or review of the file. The FDNS-IO should explain the benefit sought to the Record Owner and bring up any questions or issues requested by the CARRP-ISO during the eligibility assessment in order to gain as much information as possible for the adjudication of the case. When possible, the FDNS-IO should include the CARRP-ISO when contacting the Record Owner for deconfliction.

Complete instructions for deconfliction are in Section IV, part C, "Deconfliction" of the *Operational Guidance*.

d. Documenting Eligibility Assessment and Internal Vetting

The results of the eligibility assessment, internal vetting and deconfliction must be fully documented in FDNS-DS. A copy of the Background Check and Adjudicative Assessment (BCAA) Report should then be printed from FDNS-DS and placed in the A-File.

Both the FDNS-IO and the CARRP-ISO are responsible for entering their activities, documentation, etc. into the FDNS-DS system throughout the CARRP process. USCIS policy requires that each action taken while working on a CARRP case is immediately entered into FDNS-DS and that each process phase be immediately updated as it is completed in order to ensure accurate reporting for each NS case. Field Offices may have varying local procedures to ensure FDNS-DS is fully up-to-date at the end of each and every stage of the CARRP process. Such procedures are permissible provided that all information pertaining to each CARRP case is entered into FDNS-DS at the appropriate time as dictated by FDNS-DS User Guidelines. (See the FDNS web site on the USCIS intranet).

e. Individual Deemed Eligible for the Benefit

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

6

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

Per the *Operational Guidance*, when a NS concern remains and the individual is deemed eligible for the benefit at the Eligibility Assessment/Internal Vetting stage, no benefit may be granted until external vetting is complete, unless an exception applies. See Section VIII, “Case Specific Exceptions and Miscellaneous Guidance”, which includes ancillary benefits, I-90s, Santillan cases, motions, appeals, exemptions and dealing with classified information.

3. External Vetting – Step 3 of CARRP Process:

a. KST NS Concerns

Pursuant to current CARRP guidance, FDNS-IOs in the Field are not authorized to conduct external vetting with a Record Owner in possession of NS information where NS concerns indicate the subject is a KST. FDNS-IOs are authorized to conduct internal vetting of KST cases, as designated earlier in this memo, while CARRP-ISOs are authorized to conduct an initial eligibility assessment of KST cases. HQFDNS has sole responsibility for external vetting of KST NS concerns and conducts external vetting only as a last resort when the NS Concern remains and ineligibility grounds have not been identified.

If, following internal vetting and an initial eligibility assessment, the applicant or petitioner is found to be otherwise eligible, either the FDNS-IO or the CARRP-ISO must proceed as follows:

- The CARRP-ISO must complete the initial eligibility assessment and update FDNS-DS accordingly;
- The FDNS-IO must complete all internal vetting and deconfliction and update FDNS-DS accordingly; and
- Per local procedure established by the FOD, either the SISO in charge of CARRP or the FDNS-SIO, must verify that the internal vetting and deconfliction was completed, documented in the physical file by including a copy of the BCAA report (printed from FDNS-DS), and all actions are properly updated within FDNS-DS. Supervisory concurrence must be indicated in FDNS-DS.

Per the *Operational Guidance* “local management” (either the FOD or the District Director (DD) which is to be determined in each Field Office) must review the case to confirm that no grounds of ineligibility have been identified. Local management (FOD and/or DD as per local policy) concurrence must be indicated in FDNS-DS.

Per local office procedures, the FOD or designated supervisor (“Designated supervisor” may be an SISO or FDNS-SIO, depending on local staffing), in charge of CARRP will designate which officer, the FDNS-IO or the CARRP-ISO, must complete a Request for Assistance (RFA) to HQFDNS as noted in Section II.B of the *Operational Guidance*.

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

7

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

Also per local office procedures, the FOD or SISO will designate which personnel will charge the file to COW FD0004 in NFTS and forward the physical file to HQFDNS, attention Milagros Castillo, Staff Assistant. FDNS-IOs and CARRP-ISOs are reminded that they may request both vetting and adjudicative assistance from HQFDNS, and should do so in cases involving KSTs or cases in litigation.

b. Non-KST NS Concerns

The FDNS-IO in each Field Office is responsible for conducting external vetting of Non-KST cases. Complete instructions for Section V, “External Vetting – Step 3 of CARRP Process” are available in the *Operational Guidance*.

The FDNS-IO must seek any additional information that may be relevant to a determination of eligibility. This may include information concerning indicators of fraud, foreign travel and information about employment or family relationships that would otherwise not rise to the threshold necessary for criminal prosecution. It is vital for the FDNS-IO to clearly document any facts or fact patterns found during the external vetting process for use by the CARRP-ISO in the final adjudication of the case.

As stated earlier, the FDNS-IO is the primary point of contact and liaison for external vetting of Non-KST CARRP cases with any LEA, Record Owner and relevant agency. Complete instructions for Section V, “External Vetting – Step 3 of CARRP Process” are available in the *Operational Guidance*.

Throughout the CARRP process, FDNS-IOs must conduct deconfliction as necessary. This is done to ensure that planned adjudicative activities (e.g., interview, request for evidence, site visit, decision to grant or deny a benefit, or timing of the decision) do not compromise or impede an ongoing investigation or other Record Owner interest. This requires close coordination with the CARRP-ISO regarding any interview that may be necessary or required to complete the adjudicative process.

It is vital for the FDNS-IO to fully document all activities and their results connected with external vetting in FDNS-DS. This documentation must be completed before the case moves forward in the CARRP process.

The FDNS-IO must also ensure deconfliction is complete and documented properly in FDNS-DS before any CARRP case goes forward for adjudication.

4. CARRP Adjudication – Step 4 of CARRP Process:

CARRP-ISOs are responsible for the adjudication of CARRP cases assigned to them by the SISO in charge of CARRP, or the FOD, in each Field Office. The CARRP-ISO must check

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

8

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

FDNS-DS to ensure deconfliction is complete before adjudicating any CARRP case. If the deconfliction does not appear in the FDNS-DS record, the CARRP-ISO shall inform the SISO responsible for CARRP cases. The SISO must then contact the FDNS-SIO, if one is located in the Field Office, to direct the FDNS-IO to either complete the required deconfliction and document this action in FDNS-DS or, if deconfliction has been completed, direct the FDNS-IO to complete the documentation of the deconfliction in FDNS-DS. If a Field Office does not have an FDNS-SIO, the SISO must follow local procedures to contact an FDNS-IO to complete and/or document the required deconfliction in FDNS-DS.

a. Adjudicating Applications with KST NS Concerns

Upon completion of all external vetting, HQFDNS will return cases to the submitting officer when:

1. HQFDNS has determined that the information obtained during external vetting is sufficient to support a denial of the pending application or petition; or
2. HQ senior leadership and the USCIS Deputy Director recommend approval of the application or petition. Following this recommendation, the HQ program office with jurisdiction over the case, in coordination with HQFDNS and Office of Chief Counsel, will issue written direction to the field on how to proceed with adjudication.

b. Adjudicating Applications or Petitions with Non-KST NS Concerns

The CARRP-ISO must obtain supervisory approval and concurrence from the FOD in order to approve any application or petition that grants a benefit to an individual with remaining Non-KST NS concerns. Once the FOD concurs that the individual is otherwise eligible for the benefit, the FOD may use his or her discretion to have the CARRP-ISO grant the benefit or the FOD may designate either the FDNS-IO or the CARRP-ISO to request further assistance from HQFDNS/ASU (Adjudication Support Unit). (See Section VI, "Requesting Vetting Assistance from HQFDNS" in the *Operational Guidance*.) If, after consultation with the respective HQ component, the FOD decides to grant the benefit, the FOD, or FOD's designee, must document all adjudicative actions in FDNS-DS, and print out the BCAA report for inclusion in the case file.

REMEMBER: Both FDNS-IOs and CARRP-ISOs have distinct duties to perform in the processing of CARRP cases; however, close cooperation and coordination of effort between Officers is necessary in order to bring each case to completion.

Field Office personnel are reminded to follow the guidelines for confidentiality, Privacy Act requirements (e.g., DHS Handbook for Safeguarding Sensitive Personally Identifiable Information) and handling sensitive but unclassified (For Official Use Only – FOUO)

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

9

Clarification and delineation of vetting and adjudication responsibilities for CARRP cases in Domestic Field Offices.

information while working on all CARRP cases. Specific guidelines may be found in Sections C & D, pages 7 & 8 of the *Operational Guidance*.

In addition, Field Office personnel are reminded to adhere to all security-related policies related to protecting FOUO and classified information. Specific guidelines regarding the provisions of Executive Order are found in the *Operational Guidance*. Information regarding the specific regulations governing the protection of FOUO and Executive Order 12958, as amended, Classified National Security Information, is available at the intranet site of the USCIS Office of Security and Investigations.

IV. Contact Information

Questions regarding this memorandum may be directed through official channels to HQ, Office of Field Operations.

Distribution List:

Regional Directors
District Directors
Service Center Directors
Field Office Directors
National Benefits Center Director

FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director (MS 2000)
Washington, DC 20529-2000



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

July 26, 2011

PM-602-0042

Policy Memorandum

SUBJECT: Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists

Purpose

This memorandum provides revisions to the Controlled Application Review and Resolution Program (CARRP), the U.S. Citizenship and Immigration Services (USCIS) policy on processing cases containing national security (NS) concerns. This memorandum amends previous guidance established in the policy memoranda listed below and authorizes designated officers¹ in the field² to perform external vetting in cases involving Known or Suspected Terrorists (KSTs). Further, this memorandum rescinds guidance requiring the field to seek adjudicative assistance from Headquarters FDNS (HQFDNS) for both KST and Non-KST cases.

Scope

Unless specifically exempted herein, this policy memorandum applies to and is binding on all USCIS employees.

Authority

This memorandum revises:

The April 11, 2008, policy memorandum issued by Deputy Director Jonathan R. Scharfen titled "Policy for Vetting and Adjudicating Cases with National Security Concerns" (CARRP Memo).

Background

The April 11, 2008 memorandum established CARRP, a disciplined, agency-wide approach for identifying, processing and adjudicating applications and petitions involving NS concerns.

Under CARRP, responsibility for vetting and documenting Non-KST NS concerns and adjudicating all NS-related applications and petitions was delegated to the field. HQFDNS retained responsibility for the external vetting of KST cases.

¹ The term "designated" refers to those officers that are currently assigned and are responsible for various steps in the CARRP process (i.e., identifying, vetting/eligibility assessment, external vetting, CARRP Adjudication). This policy memorandum and the attached supplemental guidance do not intend to change the delineated roles and responsibilities (instituted by various USCIS Directorates) of USCIS officers currently processing CARRP cases.

² The field refers to Field Offices, Service Centers, the National Benefits Center, and equivalent offices within the Refugee, Asylum, and International Operations Directorate (RAIO), and the officers designated to perform different tasks related to the CARRP process.

PM-602-0042: Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists
Page 2

Over the past three years, the field has acquired valuable experience and expertise in vetting and adjudicating NS cases. In addition, the field has worked diligently to establish collaborative working relationships with their counterparts in the law enforcement community, including local Joint Terrorism Task Forces (JTTFs). This has resulted in an access to information and resources not previously available to the field. As such, authorizing the field to externally vet KSTs directly with the law enforcement and intelligence community (LEIC) will increase efficiency and effectiveness by reducing the often redundant movement of information between the field, HQFDNS, and the LEIC without compromising the integrity of the process.

Policy

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.

In addition, if, after completing the vetting and deconfliction process in KST cases, there continue to be national security concerns, and there is insufficient evidence or other grounds to deny the application, offices are to seek further guidance from their respective HQ Directorate, in consultation with local and HQ counsel when appropriate. HQFDNS will no longer provide adjudicative assistance. HQFDNS will, however, remain available to provide vetting assistance, including the identification of the record owner and the resolution of issues involving record owners.

Implementation

As a result of this delegation of authority, the nature of assistance requested from HQFDNS is limited to those outlined below. Following the initial eligibility assessment and internal vetting, if no ineligibility grounds are identified, the field will conduct external vetting³. Upon obtaining local management approval, the field may e-mail a Request for Assistance (RFA) to HQFDNS (FDNS-NSB@dhs.gov) under the following circumstances:

- To identify the NS record owner of the KST nominating entity;
 - HQFDNS will identify a POC. The field must then contact the POC for external vetting and deconfliction.
 - If HQFDNS is unable to identify a POC⁴, HQFDNS will conduct external vetting and deconfliction.
- To seek assistance in contacting or resolving issues with the record holder; and
- To conduct queries of classified systems⁵.

Except as noted in this memo, all current CARRP guidance provided by various Directorates remains in effect.

³ External vetting must be conducted if no ineligibility grounds have been identified or if Field Management determines further processing is necessary to strengthen or support a decision. KST external vetting is to be conducted by officers who are currently conducting external vetting of Non-KST cases.

⁴ These KSTs are generally nominated by certain members of Intelligence Community for which a POC is not available.

⁵ Classified High Side checks must not be requested routinely. Rather, the field must articulate a need for such checks. For example, where the nominating agency is either a foreign entity or a member of Intelligence Community (other than the FBI) and additional information cannot be obtained through the local JTTF.

PM-602-0042: Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists
Page 3

Use

This PM is intended solely for the guidance of USCIS personnel in the performance of their official duties. It is not intended to, does not, and may not, be relied upon to create any right or benefit, substantive or procedural, enforceable at law or by any individual or other party in removal proceedings, in litigation with the United States, or in any other form or manner.

Contact Information

Questions or suggestions regarding this PM should be addressed through appropriate channels to HQFDNS.

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of Fraud Detection and National
Security
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

Supplemental Guidance:

Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists

A. KST Hits

HQFDNS has issued a policy memo directing that external vetting for Known or Suspected Terrorists (KSTs) should now be done by local Field Offices and Service Centers. These questions and answers serve as supplemental guidance to clarify the requirements of the new CARRP policy, and answer questions raised during the drafting phase of the policy.

CARRP procedures and requirements outlined in existing policy and operational guidance (provided by various HQ directorates) remain the same, other than those specified in the attached policy memorandum. Also, this revised policy does not replace existing protocols, work flow process and procedures, or delineated roles and responsibilities of USCIS officers currently processing CARRP cases.

1. Who will conduct external vetting of KST cases?

External vetting of KST cases will now be conducted by those officers currently assigned to conduct external vetting for non-KST cases (i.e., FDNS IOs, Background Check Unit officers, and etc.).

2. How will field offices conduct external vetting if they do not have a designated USCIS representative with local JTTF?

To conduct external vetting, the field must have the contact name and phone number for the law enforcement agency (LEA) and/or record owner who may or may not be assigned to a local Joint Terrorism Task Force (JTTF). While having a designated USCIS representative with local JTTF is highly advantageous, it is not a necessary requirement for the field to be able to conduct external vetting.

Field offices that do not have an established relationship with their local JTTF or other Law Enforcement Intelligence Community (LEIC) partners may continue to request

assistance in identifying the record owner by submitting a Request for Assistance (RFA) to HQFDNS via the FDNS-NSB@dhs.gov mailbox.

3. What is the difference between KST and Non-KST external vetting?

There is no difference. The purpose of external vetting, as defined in current operational guidance provided by various Directorates, is to make inquiries of record owners in possession of national security (NS) information. Specifically, the designated officer will determine the nature and quality of the NS concern, the status of any investigation related to the NS concern, and if the NS concern impacts the subject's eligibility for the benefit requested or if the alien may be subject to a ground of removal under the Immigration and Nationality Act (INA). 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.

External vetting must be conducted if no ineligibility grounds have been identified (after eligibility assessment and internal vetting have been completed) or if Field Management determines further processing is necessary to strengthen or support a decision.

4. What is the purpose of Classified High Side Checks?

The purpose of classified checks is to obtain additional information that may identify additional ineligibility grounds or support additional lines of questioning. However, classified High Side checks must not be requested routinely. Rather, the field must articulate a need for such checks. For example, the field may request high side checks when the nominating agency is either a foreign entity or a member of Intelligence Community (other than the FBI) and additional information cannot be obtained through the local JTTF.

NOTE: In reviewing the classified systems check results to identify possible grounds of ineligibility, develop lines of questioning when interviewing the individual, or identify information which if declassified, could be used to support a denial, the field must never cite the information provided by another agency in a decision without first obtaining written permission from the originating agency. Additionally, the field should never develop a line of questioning or provide a written decision which could implicate classified information that has not been declassified unless it can be clearly demonstrated that the information can be obtained from a publicly available source. If the information has been declassified, the field must still obtain written permission from the originating agency to use the information. The field may request assistance from HQFDNS in declassifying information if the owner of the information requests HQ involvement.

5. Can the field approve KST cases?

No. Officers in the field are not authorized to approve KST cases. Current policies and procedures for the approval of cases involving KSTs have not been changed.

6. What should the field do with KST cases that have been determined to be otherwise approvable?

Upon completion of internal and external vetting, if the national security concern remains, or the KST individual remains eligible for the benefit, the KST case must be elevated to the respective HQ directorate point of contact (POC) for further evaluation, in consultation with local and HQ counsel.

HQ will return a case to the submitting officer when senior leadership and the USCIS Deputy Director have reviewed the application or petition and made an appropriate recommendation, or released the case to the field for adjudication.

7. How should the KST cases be elevated to respective HQ directorate?

Officers should follow current local and directorate guidance for forwarding cases to their respective HQ directorate POCs.

8. What will happen to the existing Request for Assistance (RFA) process?

HQFDNS is not changing the existing RFA process. However, the nature of assistance provided will be different.

Upon obtaining local management approval, the field may e-mail an RFA to HQFDNS (FDNS-NSB@dhs.gov) under the following circumstances:

- To identify the NS record owner of the KST nominating entity;
 - HQFDNS will identify a POC. The field must then contact the POC for external vetting and deconfliction.
 - If HQFDNS is unable to identify a POC¹, HQFDNS will conduct external vetting and deconfliction.
- To seek assistance in contacting or resolving issues with the record holder; and
- To conduct queries of classified systems.

¹ These KSTs are generally nominated by certain members of Intelligence Community for which a POC is not available.

9. *Can the field contact the record owner who is a member of the Intelligence Committee?*

Contact with the Intelligence Committee is not reserved for HQFDNS if the Intelligence Community member has released his/her name for the field to contact. If the name is not released or is not available, HQFDNS will conduct external vetting before returning the case back to the field.