EXHIBIT 45
FILED UNDER SEAL

National Background, Identity, and Security Check Operating Procedures

Table of Contents

1

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

2

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

4

National Background, Identity, and Security Check Operating Procedures

National Background, Identity, and Security Check Operating Procedures

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

I.   Introduction

The U.S. Citizenship and Immigration Services Fraud Detection and National Security Directorate (FDNS) developed this handbook (HB), National Background Identity and Security Checks Operating Procedures (NaBISCOP), as a standard working tool to document routine administrative and procedural operational activities.

The Mandatory Review Date (MRD) of this HB is two years from the official issue date. After two years, this document will be reissued without change, revised, or withdrawn from the U.S. Citizenship and Immigration Services Knowledge Management Directory. However, revisions may be made by the sponsoring office at any time.

This HB is marked "FOR OFFICIAL USE ONLY – LAW ENFORCEMENT SENSITIVE." It contains Sensitive But Unclassified information that requires protection against unauthorized disclosure. As such, it is to be controlled, stored, handled, transmitted, distributed and disposed of in accordance with DHS Management Directive (MD) 11042.1, "Safeguarding Sensitive But Unclassified (For Official Use Only) Information." It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). Where they occur in this document, names and other identifiers are provided purely for illustrative purposes. They do not relate to actual applicants or petitioners.

USCIS personnel must have (1) a need-to-know, (2) the required training, and (3) the appropriate level of background and security clearances to conduct these checks. See Section IV, Part A for more details. Questions or comments regarding any part of this document should be directed to USCIS FDNS NSD at FDNS-NaBISCOP@uscis.dhs.gov.

A. Scope and Use

The NaBISCOP HB is intended for use by all USCIS personnel[1] who perform security and background checks when processing requests for immigration benefits and by, as well as supervisors and managers who oversee these personnel and processes. The HB is presented as intended to be a "user friendly" electronic resource that provides ready access to materials through internal links. Additionally, it provides references to other related policy and or guidance.

The NaBISCOP provides overarching baseline requirements for USCIS background and security checks and incorporates all applicable USCIS policies and procedures related to USCIS background and security checks. As those policies and procedures change, the NaBISCOP will be updated to reflect the changes.

USCIS employees and offices may be subject to directorate specific background check requirements in addition to but not superseding NaBISCOP requirements. However, such

---

[1] USCIS personnel include USCIS employees and contractors.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

<u>**National Background, Identity, and Security Check Operating Procedures**</u>

requirements should not be viewed as a basis to revise, supplement, disregard or deviate from the NaBISCOP baseline requirements, unless directorate or component specific exceptions are specifically acknowledged in the NaBISCOP -for example, if an important component-specific exception has been recognized for a specific background check, the NaBISCOP will make note of this exception with language such as "Refer to component specific guidance for additional details."

The NaBISCOP 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. In addition, the NaBISCOP and any related instructions are in no way intended to and do not prohibit enforcement of the immigration laws of the United States.

Further, the NaBISCOP has been written to encompass baseline USCIS requirements and has purposely used broad language, as appropriate in specific sections, to allow for best practices based on differing caseloads and system capabilities in various USCIS locations. The NaBISCOP itself does not provide sufficient guidance for building systems with optimal background check capabilities. Therefore, existing systems should not be modified, and new systems should not be designed or built, based solely upon an independent interpretation of any part of the NaBISCOP. Rather, proposed technical developments related to background checks should be considered in consultation with the FDNS Screening Coordination Office, the FDNS Systems Integration Branch, the USCIS Background Check Working Group, and/or the various BCWG directorate/office representatives, as applicable.

B. Authority
Authority to issue and appropriately revise or update the NaBISCOP lies with the Associate Director, Fraud Detection and National Security Directorate (FDNS).

C. Background
The background check process is a critical element in USCIS's mission to ensure the integrity of the U.S. Immigration system. The process identifies individuals who may pose a risk to our national security or public safety. The process also identifies other derogatory information that may affect eligibility for the immigration benefit sought.

As part of its function to oversee background check policy and procedures for USCIS, FDNS worked closely with other directorate and program office experts to develop the NaBISCOP, a unified procedures manual covering background and security checks.

National Background, Identity, and Security Check Operating Procedures

The NaBISCOP is issued with concurrence by the Field Operations Directorate; the Service Center Operations Directorate; the Refugee, Asylum, and International Operations Directorate; the Office of Policy and Strategy; and the Office of Chief Counsel.

D. Implementation

The NaBISCOP replaces the Interagency Border Inspection System Standard Operating Procedure (IBIS SOP) dated March 1, 2006, which is now rescinded. Incorporating elements from the IBIS SOP, the NaBISCOP is now the foundation for service-wide security and background check procedures. It is intended to be used in concert with other USCIS policies and guidance, as well as component-specific guidance and standard operating procedures, as they relate to the processing of specific immigration benefit applications and petitions. Training materials for NaBISCOP must adhere to the policies and procedures outlined in this document and must be updated to include any subsequent policy or procedural changes.

Updates or modifications to the NaBISCOP can be found on the FDNS website Table of Revisions.

E. Contact Information

Questions regarding the NaBISCOP or background check procedures should be addressed through the respective chain of command. Questions that cannot be answered locally may be sent through the Officer's HQ component via email to the FDNS-NaBISCOP mailbox: ███████
███████ @uscis.dhs.gov

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431514

<u>**National Background, Identity, and Security Check Operating Procedures**</u>

II. <u>Employee Safety</u>

Employee safety should always be the first priority. The background check process may alert USCIS that the individual applying for a benefit is wanted for a criminal offense or is a potential threat to USCIS personnel and customers. If an individual who is wanted for a criminal offense(s) or is otherwise a potential threat, is physically present in USCIS space, the USCIS officer should, in consultation with a supervisor, determine if immediate action is required, such as detention by appropriate law enforcement personnel.

If it is determined that the individual should be detained, the Federal Protective Service (FPS) should be the first point of contact, if available to the office. For offices without FPS presence, local law enforcement should be contacted. If the individual is not present in USCIS space, authorized USCIS personnel should coordinate with FPS or local authorities, as appropriate.

Officers should follow established local or component guidance related to officer safety when performing site visits. A Significant Incident Report (SIR) must be completed and forwarded within one hour to the USCIS Command Center for any arrest or detention of an individual within USCIS space (warrant, detention, removal, etc.). Refer to SIR guidance found at Office of Security and Integrity's (OSI) website:
http://███████████████████████████████████

NOTE: USCIS personnel may not detain a subject for any violation of State or Federal law. In addition, care must be taken that a subject does not have the perception of being detained by USCIS personnel.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431515

National Background, Identity, and Security Check Operating Procedures

III.   Protecting Sensitive Information from Unauthorized Disclosure

As part of the background and security check processes, USCIS personnel handle and share sensitive information on a need-to-know basis. Federal law and agency policy protect against unauthorized disclosure of information collected and maintained in USCIS systems of records both in the electronic and paper form. Much of the information contained in USCIS systems and files is Sensitive But Unclassified (SBU) information and must not be shared or disclosed except pursuant to those rules and regulations.

This section reminds USCIS personnel when and how to protect from unauthorized disclosure Sensitive but Unclassified (SBU) and classified information.

For specific guidance on handling SBU and classified information, USCIS personnel should refer to the Office of Security and Integrity's (OSI) pamphlet entitled, Safeguarding Classified and Sensitive Unclassified Information. This document may be found on OSI's webpage under their Administrative Security section on USCIS Connect.

Additional questions about the safeguarding of SBU and classified information should be addressed to your field security manager or the OSI. The contact information of field security managers may be found on the USCIS intranet at:

http://██
██████████████████████

A. For Official Use Only (FOUO)

FOUO is the designator used within DHS to identify SBU information within the DHS community that is not otherwise specifically described and governed by statute or regulation and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest.

For additional guidance on FOUO, refer to DHS Management Directive (MD) 11042.1, "Sensitive But Unclassified Information,"

Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," "Official Use Only (OUO)," and "Law Enforcement Sensitive (LES)."

A security clearance is not required for access to FOUO information. Access to FOUO information is based on "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need-to-know, the holder of the information will request dissemination instructions from their next-level supervisor or the information's originator. Do not apply FOUO designation to any information in order to conceal government negligence, ineptitude, or other disreputable circumstances embarrassing to a government agency, and do not dispose of FOUO information in regular wastebaskets and recycle bins.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

B. DHS: One Agency for Information Sharing Purposes

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

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

C. Third Agency Rule

Records of other agencies either loaned to USCIS or a part of USCIS files must be protected from unauthorized disclosure. The contents of an agency's records in possession of USCIS shall not be disclosed to another agency without the prior consent of the originating agency. See the DHS memorandum entitled "Safeguarding Sensitive But Unclassified (For Official Use Only) Information" for more guidance.

This principle is generally known as the "third agency rule." When processing a FOIA request involving the release of third agency material, the agency concerned shall be consulted regarding release of the document or information originating with them and the requester should be advised accordingly. When the request involves third agency material which is classified, the requester must be referred to the originating agency for a determination as to release in accordance with applicable law. The third agency rule also applies to the U.S. attorneys' offices representing USCIS in court.

D. Safeguarding Classified Information

Information received as a result of security checks such as the FBI Name Check or when conducting external vetting for cases with national security (NS) concerns may be classified as Confidential, Secret, or Top Secret. Often classified information is referred to as National Security Information (NSI).

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP⸺in whole or in part⸺unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431517

National Background, Identity, and Security Check Operating Procedures

USCIS employees must always work to protect such information from improper disclosure. National guidance is provided by the USCIS Office of Security and Integrity (OSI).

Consult OSI guidance and training material at OSI's Administrative Security Division, or the local OSI field security manager (FSM) for the best way to safeguard classified information. The OSI pamphlet entitled Safeguarding Classified and Sensitive Unclassified Information provides specific guidance for handling classified information.

Note: Unauthorized disclosure of classified documents does not mean that the documents have been declassified. A National Security Information (NSI) Violation is committed whenever an individual handling classified information fails to safeguard it in strict accordance with governing directives. You must abide by the classification markings on the document and handle it according to the appropriate protections even if the document has been posted on internet websites.

Safeguarding Classified National Security Information	
Dos	**DON'Ts**
▪ Wear ID badges at all times	▪ Do not transport classified information without courier card.
▪ Properly package NS information before mailing	▪ Do not mail TOP SECRET documents.
▪ Use cover sheets ▮▮▮▮▮▮▮▮) on classified information	▪ Do not mail SECRET or CONFIDENTIAL information using FedEx, DHL, UPS, etc, absent an urgent requirement for overnight delivery and prior approval from Chief, OSI.
▪ Ensure classified information material is properly marked and safeguarded	▪ Do not discuss classified information with unauthorized personnel.
▪ Properly mark all electronic media with the appropriate classification label	▪ Do not assume a person has a National Security Information (NSI) security clearance based on their position or badge cover.
▪ Secure classified information in a GSA-approved security container only	▪ Do not take classified material to your home or other unauthorized area.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

▪ Confirm the clearance of the person requesting access to classified information with OSI and verify their need-to-know.
  • Send an e-mail to OSI Personnel Security Customer Service using the following look-up name in Outlook, "█████████", or using the e-mail address, ████████████
 	
  • Include the following information:
  • Your name, title, and phone number
  • The employee's name and last four digits of the Social Security number.
  • In addition, if needed, you must specifically request verification of the employee's level of IT access or background investigation.
  • You will receive an e-mail reply generally in less than one day identifying the level of security clearance and the date that the clearance was granted.
	• Do not discuss classified information on a telephone unless using STE or STU-III equipment.

• Only discuss classified information in a secure area.	• Do not fax classified information on a non-secure fax machine.
• Conduct End-of-Day Security Checks and record SF 701/702 forms.	• Do not reproduce classified information on a copy machine that has not been accredited by OSI.
• Use DHS 11000-11, Classified Document Record of Transmittal when transmitting Top Secret, Secret and Confidential material.	• Do not store funds, weapons, medical items or items of intrinsic value in the same container used for storage of classified information.
• Destroy NS documents in a GSA-approved shredder only.	• Do not store combinations of safes containing classified information anywhere but inside a GSA-approved security container.
• Ensure SBU and FOUO information is properly protected and safeguarded.	• Do not dispose of classified information in regular waste baskets and recycle bins.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

• Report all incidents involving the mishandling or potential compromise of classified, SBU, or FOUO information to supervisor. • For information on reporting incidents, visit the OSI website at htt█████████████████████████ ████████████████	

DHS policy precludes the use of classified information as the basis for denial of a benefit, without formal authorization by the Secretary of DHS and permission of the owning agency. Refer to the October 4, 2004, memorandum entitled "Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings".

E.   Personally Identifiable Information (PII)

DHS defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual. This definition applies regardless of whether the individual is a U.S. citizen, a legal permanent resident, a visitor to the U.S., a DHS employee, or a contractor."

Refer to the June 13, 2007, DHS memorandum entitled "Review of Safeguarding Policies and Procedures for Personnel-Related Data," and the USCIS Office of Privacy webpage on the USCIS intranet for additional information.

There are two categories of PII risk sensitivity:

- Low Risk PII is information that appears on an average business card (i.e., names, business phone numbers, and office titles) and is least likely to cause harm to an individual.
- Sensitive PII (SPII) is information that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

The July 8, 2008, memorandum entitled "USCIS Policy Regarding Personally Identifiable Information" from USCIS Chief Privacy Officer Donald Hawkins and the DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provide detailed guidance on securing PII and reporting possible improper disclosure. Proper procedures include:

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP---in whole or in part---unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431520

National Background, Identity, and Security Check Operating Procedures

- Share or discuss sensitive personal information only with those personnel who have a need to know it for purposes of their work. Share only the necessary information, and ensure each recipient has a need to know all the information you share.
- Do not leave work folders containing SPII unattended; this information should be maintained either in secured file cabinets or on computers that have been secured.
- Lock up hardcopy documents, flash drives, laptops, and other equipment that contain SPII when you're not using them.
- If e-mailing a document with SPII:
  - Encrypt and password-protect the document if transmitting outside the DHS firewall (i.e., to a non-DHS e-mail address). Do not include the password for the document in the same e-mail. USCIS currently uses WinZip 10 for encryption. Or,
  - Redact (remove) all SPII from the document. The only safe way to redact information is to re-key or copy-and-paste the non-PII data into a new document, since computer hackers can restore data that has merely been deleted.
  - Exception: If you are e-mailing a document and the SPII is a full social security number (SSN), you must encrypt the document in all instances. However, it is permissible to disseminate the last four digits of the SSN within the DHS firewall, unencrypted.
- Never send or receive e-mails with PII to your or someone else's personal commercial e-mail account.
- Do not remove records about individuals from a USCIS office unless you first obtain clearance from a supervisor by providing both sufficient justification for removing the material as well as evidence that you can appropriately secure it at your destination and while in transit.
- Dispose of SPII appropriately: use burn bags or approved shredders set to graffiti or cross cut standards for hard copy records, and erase electronic records.
- Keep the use of social security numbers to a minimum. The SSN was never intended to be an all-purpose personal identifier, and we must use these numbers sparingly and judiciously to thwart identity thieves. See the June 4, 2007, Privacy Policy Guidance Memorandum for details on the only times you are authorized to use SSNs at USCIS.

F.   Privacy Act

The Privacy Act of 1974 states, as a general matter, that no federal agency can share information about an individual in the absence of an exception or published "routine use."

The Privacy Act protects information on United States citizens (USC) and lawful permanent residents (LPR). The Privacy Act itself does not apply to aliens who are not LPRs. However, by memorandum issued by the DHS Privacy Office dated February 1, 2007, as a matter of policy,

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

the protections of the Privacy Act are to be afforded to non-citizens and non-LPRs to the maximum extent practicable.

Protected information includes information contained in a USCIS system of records where a name or unique identifying number of an individual (e.g., A#) can be used to retrieve information. For example, DHS maintains information in A-files and electronically in the Central Index System (CIS2), the FBI Fingerprint Check, and in TECS.[2] Because these types of records can be retrieved by name and A#, the Privacy Act covers information contained in A-files, CIS, and TECS. USCIS maintains other systems of records in which information pertaining to individuals may be stored.

Information cannot be disclosed to any person or other agency unless the individual USC or LPR provides written permission to share the information, with some exceptions. If one of those exceptions applies, information may be shared with a person or other agency without the permission of the individual USC or LPR.

The USCIS chief privacy officer has issued guidance on the transmittal and handling of Personally Identifiable Information (PII) by USCIS employees. The memorandum entitled, "USCIS Policy Regarding Personally Identifiable Information," can be accessed on the Office of Privacy webpage.

If an alien or a USC specifically asks if there is information about him or her in TECS, the individual may submit a Freedom of Information Act (FOIA) request to Customs and Border Protection (CBP) at the following address:

> U.S. Customs and Border Protection
> 1300 Pennsylvania Ave., NW,
> Attn: Mint Annex Building, FOIA Division
> Washington, D.C. 20229

G. Confidentiality
In addition to the rules and regulations mentioned above for sharing information found in USCIS files and systems, special care must also be taken in the following circumstances:

1. Asylum and Refugee
Under Title 8 Code of Federal Regulations (C.F.R.) § 208.6, information regarding an individual's status as an asylum seeker or asylee, information contained in or pertaining to his or

---

[2] Formerly, security checks by USCIS were referred to as the Interagency Border Inspection System (IBIS) checks. However, IBIS is no longer a separate database and all information formerly in IBIS is now accessed through TECS, formerly the acronym for the Treasury Enforcement Communications System. References to IBIS or TECS/IBIS are now obsolete, and any such references in older documents should be interpreted as now referring to TECS.

National Background, Identity, and Security Check Operating Procedures

her application, and records pertaining to any credible fear or reasonable fear determination must not be disclosed without the written consent of the applicant or a waiver from the Secretary of DHS, unless disclosure is otherwise specifically permitted by regulation. The confidentiality provisions of Title 8 C.F.R. § 208.6 have been extended to refugee applicants and information contained in or pertaining to refugee applications. Thus, as a matter of policy, a refugee's information must be protected in the same manner as an asylee's information

Public disclosure of such information may subject the claimant to retaliatory measures by government authorities or non-state actors in the event that the claimant is repatriated, or endanger the security of the claimant's family member(s) who may still be residing in the country of origin. Moreover, public disclosure might, albeit in rare circumstances, give rise to a plausible protection claim where one would not otherwise exist by bringing an otherwise ineligible claimant to the attention of the government authority or non-state actor against which the claimant has made allegations of mistreatment.

There are exceptions for sharing asylum and refugee related information in certain limited and enumerated circumstances, including disclosure for United States Government investigation concerning criminal or civil matters. See Title 8 C.F.R. § 208.6 for the list of exceptions, and see the April 18, 2007, DHS memorandum entitled "Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies," the fact sheet on confidentiality in asylum cases, and local guidance for more information.

2.   **Violence against Women Act/T and U Nonimmigrant Visas**
Section 384 of the 1996 Illegal Immigration Reform and Immigrant Responsibility Act, as amended, Title 8 U.S.C. § 1367, limits the use and disclosure of information relating to aliens seeking protection under the Violence Against Women Act (VAWA), as amended, or as T (victims of trafficking) or U (victims of qualifying criminal activity) non-immigrants.

Generally, USCIS personnel may not disclose any information that relates to an alien who is the beneficiary of an application for relief under the VAWA, where such claim is either pending or approved, including T and U visa applicants. Title 8 U.S.C § 1367(a)(2) prohibits not only the disclosure of information relating to the subject's protected claim, but any information relating to the subject. USCIS can share the information with other DHS employees, but not outside of DHS. In limited situations, certain exceptions to the disclosure prohibition may apply. For example, certain information may be disclosed to Federal, state and local public and private agencies providing benefits, to be used solely in making determinations of eligibility for benefits pursuant to section 1641(c) of 8 USC. In addition, if there is a legitimate law enforcement reason to release the information, the Secretary of Homeland Security may authorize such a release to law enforcement officials. Other limited exceptions to the general prohibition on disclosure are listed at 8 USC 1367(b).

National Background, Identity, and Security Check Operating Procedures

USCIS personnel seeking authorization to disclose information pursuant to an exception listed at 8 USC 1367(b) should contact the Office of Chief Counsel.

3.   Legalization/Seasonal Agricultural Worker (SAW)

Sections 210 and 245A of the Act limit the use and disclosure of information provided by "amnesty" applicants under the 1986 Immigration Reform and Control Act. USCIS may not use or disclose information in a legalization application or its accompanying evidence except to adjudicate the application itself, or for certain law enforcement functions and fraud proceedings.

The legalization regulations at 8 C.F.R. § 245a.3(n)(4)(i) and (ii) and 8 C.F.R. § 245a.4(b)(23)(iv) permit information contained in granted legalization files (i.e. for visa classifications W16 and W26) to be used at a later date when adjudicating an immigrant visa petition or other status petition under section 204 of the Act as well as for a naturalization application.

Consult with USCIS counsel when contemplating any use or disclosure of this information because inappropriate use or disclosure of the information carries civil and criminal penalties.

Furthermore, when processing other applications and petitions, aliases found in previously filed legalization and SAW applications (likely found under the red legalization sheet) should not be queried in security checks unless it falls under 8 C.F.R. §245a.3(n)(4)(i) and (ii) and 8 C.F.R. §245a.4(b)(23)(iv) as indicated above.

4.   Temporary Protected Status (TPS)

USCIS/DHS may not publicly disclose information relating to the Temporary Protected Status (TPS) of an alien. See section 244(c)(6) of the Act. Implementing regulations prohibit DHS from disclosing any information submitted by an alien in support of a TPS application to a third party requester without a court order or the written consent of the alien. 8 C.F.R. §244.16 defines third party requesters as any requester other than the alien, his or her authorized representative, an officer of the Department of Justice, or any federal or State law enforcement agency. The regulation further states that any information provided under this part may be used for the purposed of enforcement of the Act or any criminal proceeding.

19
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

IV.   Background Check Process

Background checks are conducted on all individuals and organizations who seek an immigration benefit. As part of the background check, USCIS requires that specific security checks or a combination of checks are completed for each application or petition type.

"Relationship of Security Checks to the Background Check Process"
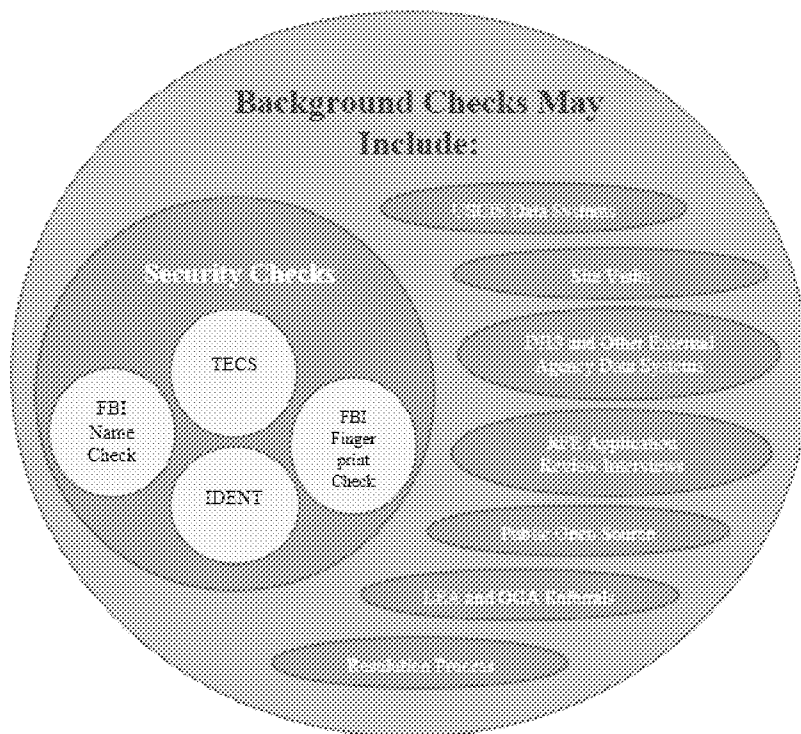
Specific checks or a combination of checks are required for each application or petition type, pursuant to each USCIS component's procedures, and may consist of the following:

- TECS;
- FBI Name Check;
- FBI Fingerprint Check;
- IDENT (Legacy US-VISIT IDENT);
- Security Advisory Opinion (SAO);
- Consular Lookout And Support System (CLASS)

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

Although CLASS and SAO name checks are initiated by DOS through its contracted Resettlement Support Centers (RSCs), the adjudication of refugee applications/petitions includes the review and analysis of CLASS and SAO results, as appropriate, by USCIS officers prior to the applicant's final adjudication, or at any time derogatory information may arise in the process. These checks are a mandatory part of refugee processing.

In addition to the above-mentioned security checks, USCIS may identify derogatory information regarding an individual or organization through other sources including but not limited to the following:

- Information received from the public. This includes applications and petitions, supporting documentation, responses to Requests for Evidence, site visits, interviews, tip letters, or information from media, internet, magazines, newspapers, or radio.
- DHS and other federal agency data systems.
- Referrals from Law Enforcement Agencies (LEAs) and Other Government Agencies (OGAs). Examples include local and state police departments, Federal Bureau of Investigation (FBI), Department of Justice (DOJ), Department of Agriculture (USDA), Department of Labor (DOL), Department of State (DOS), Department of Treasury (Office of Foreign Assets Control - OFAC), and Department of Commerce (Bureau of Industry and Security), etc.
- Other U.S. Government fingerprint holdings.

The background check refers to the analysis of the results of the security checks or any other identified concern relating to national security or public safety AND the actions required to resolve the concern.

A.   Who Requests and Reviews Background Checks
USCIS personnel must have a need-to-know to request and review security checks and resolve the results of those checks.

- The term, "USCIS personnel," includes USCIS officers, other USCIS employees, and contractors.
- The term, "USCIS officer," refers to the following, including senior and supervisory officers: immigration analyst, intelligence research specialist, immigration information officer, immigration officer, adjudication officer, field office director, immigration services officer, overseas adjudications officer, asylum officer, refugee officer, economist, or compliance officer.

National Background, Identity, and Security Check Operating Procedures

USCIS personnel may initiate security checks[3] and determine whether a result of a security check relates to the subject or does not relate (DNR). However, USCIS officers perform the review and resolution of security checks and the completion of the background checks.

In addition to the "need-to-know" requirement, USCIS personnel must meet training and clearance requirements for the security checks and processes listed in Appendix C. For classified information received from any other source, USCIS personnel must also have the appropriate clearance level and security briefing to handle such information.

Required Training and Clearance Requirements by Security Check or Process		
Security Check or Process	Requirements	
	Training	Clearance
TECS Security Check	Successful completion of mandatory TECS and FBI National Crime Information Center (NCIC) training and certification, and refresher training as required by local policy.	Proper National Agency Check with Inquiries (NACI) background checks.
FBI Name Check	USCIS personnel must have received a security briefing from OSI to handle classified Letterhead Memorandum	USCIS personnel must have a security clearance at the same level or higher than the classification (if any) of the Letterhead Memorandum.

In addition to the above guidance, each office or center has local policy which delineates the roles and responsibilities for those who may perform security and background checks. Refer to local policy for these additional roles and responsibilities.

B.   Overview of Background Check Process

The figure below illustrates a high-level view of the background check process once potentially derogatory information has been identified as a result of the security checks or from other sources.

---

[3] For refugee cases overseas, security checks are initiated by the Department of State (DOS).

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431527

National Background, Identity, and Security Check Operating Procedures
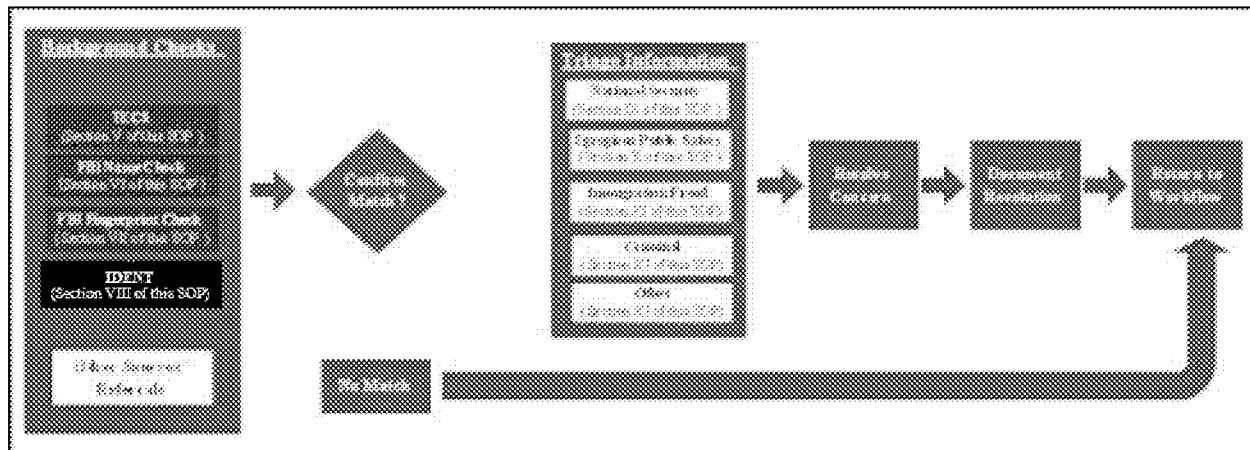
1. Confirm Match: determine if the results or other source information relates to the individual or organization seeking the immigration benefit. If results do not relate, document the determination and return to workflow.
2. Triage Information: determine if the concern involves national security, Egregious Public Safety (EPS), criminal, articulated immigration fraud, or other concerns identified by local management, and if it requires referral for special processing.
3. Resolve Concern: resolution actions may require USCIS officers to conduct additional database searches, reach out to other DHS components or a third agency for additional information, request a site visit, conduct an interview or re-interview, etc.
4. Document the Resolution.
5. Adjudication.

1.   Confirm Match

USCIS personnel must:

- Determine if the subject of the derogatory information relates to the individual applying for the immigration benefit. For more information, go to Section V.G.2.(a), Results of TECS Queries, for details on confirming NS hits in the handbook.
- Compare the information from the security check or other source to the biographic, biometric information, and physical descriptors about the individual.

USCIS personnel may use any of the personal identifiers (As listed in the figure below, a combination of identifiers, or any other available identifiers to assist in the determination.)

DEF-00431528

National Background, Identity, and Security Check Operating Procedures

Personal Identifiers

Biometric Data	Biographical Data		Physical Descriptors	
- Fingerprints	- A #	- Passport #	- Photo	- Eye Color
- Fingerprint Identification Numbering System (FINS#)	- Name	- Parents' Names	- Height	- Scar
- FBI Number	- DOB	- Address History	- Weight	- Tattoos
	- COB	- I-94s	- Hair Color	
	- SSN	- NATZ Certificate #		
	- COC	- IRS-assigned ITINs		

Note: the data elements shown are examples and do not represent the exhaustive number of personal identifier related data elements

A wealth of biographic and biometric information may be obtained from any of the databases used for background and security checks, as well as other systems and/or documents in the file. The above figure indicates some, but not all, types of personal identifiers.

Biographic and Biometric Information Sources		
USCIS Systems	**DHS Systems**	**Third Agency Systems**
• Central Index System (CIS2) • Person-Centered Query System (PCQS) (e.g. FBI Name Check results) • CLAIMS 4 • Mainframe Computer Linked Application Information Management System (CLAIMS) (e.g. CLAIMS3, CPMS QUERY for Fingerprint Tracking System and FBI Name Check results) • Marriage Fraud Amendment System (MFAS)[4]	• Student & Exchange Visitor Information • System (SEVIS) • TECS (e.g. link lists, inspection records, travel history) • ENFORCE Alien Removal Module (EARM)[5] • Enforcement Integrated Database (EID) Arrest Guide for Law Enforcement (EAGLE) • Analytical Framework for Intelligence (AFI) • Arrival and Departure Information System (ADIS) • IDENT (Legacy US-VISIT IDENT)	• DOS's Consular Consolidated Database (CCD) • DOS's Consular Lookout and Support System (CLASS) • DOS's Worldwide Refugee Admissions Processing System (WRAPS) • Department of Defense's Automated Biometrics Identification System (ABIS)

---

[4] Marriage Fraud Amendment System (MFAS) Historical data can be accessed through Person-Centered Query System (PCQS).

[5] ENFORCE Alien Removal Module (EARM) Historical data can be accessed through (PCQS). EARM is now replaced with Enforcement Integrated Database (EID) Arrest Guide for Law Enforcement (EAGLE).

DEF-00431529

National Background, Identity, and Security Check Operating Procedures

Biographic and Biometric Information Sources		
USCIS Systems	DHS Systems	Third Agency Systems
• Re-engineered Naturalization Application Casework System (RNACS) • Image Storage Retrieval System (ISRS) • Fraud Detection and National Security Data System (FDNS-DS) • Case and Activity Management for International Operations (CAMINO) • Parole Case Tracking System (PCTS) • Customer Profile Management System (CPMS) (e.g., CPMS Query for Fingerprint Results) • GLOBAL		

While USCIS officers primarily rely on best judgment and experience in determining whether the information relates to the individual, USCIS personnel should consult with a supervisor if there is any uncertainty as to whether the information relates to the individual applying for the benefit. If there continues to be uncertainty about the match, supervisors may work through their chain of command and with HQ, if necessary.

2.   Triage Information

a)   Conclusive Match

Once it is determined that the information relates to the individual, USCIS personnel must determine if the results fall into the following categories which require special processing:

- National Security: refer to section IX of the NaBISCOP.
- Egregious Public Safety or other criminal cases: refer to section X of this document.
- Articulated Immigration Fraud: refer to section XI of this document.

25

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

Criminal hits, which involve a violation of U.S., state, or local criminal law, but do not rise to the level of activity described in Egregious Public Safety, impact each application or petition differently and should be considered during the adjudications process to determine if such activity is an impediment to the requested status or benefit.

b)   Inconclusive Match

When USCIS officers are unable to confirm the match after exhausting available electronic systems and other resources, personnel must consult their chain of command to determine follow-up action. In some instances, follow-up action may include an interview, a site visit, or a Request for Evidence (RFE) to confirm the match. USCIS officers must then document the hit, include a statement in the Resolution Memorandum or other memoranda, as required, explaining the inconclusive nature of the match determination, actions taken to resolve the hit, and refer the case to the appropriate unit or field office to confirm the match.

If USCIS personnel are still unable to confirm the match, refer the case through the chain of command.

3.   Resolve Concern
Resolution may require a variety of activities which include but are not limited to: systems research (internal, external, open source), contact with other DHS components or third agencies, interview, site visits, referral to ICE (RTI) by FDNS or the Background Check Unit (BCU), deconfliction, and adjudication (if the subject is statutorily ineligible for the benefit).

Deconfliction is the coordination between USCIS and another governmental agency or record owner to ensure that planned adjudicative activities (e.g., interview, request for evidence, site visit, decision to grant or deny a benefit, issuance of Notice to Appear (NTA) and the timing of such) do not compromise or impede an ongoing investigation or other record owner interest.

4.   Document the Resolution
Each hit requires documentation of any resolution. Review the specific information for each background and security check for more information on documenting the resolution.

5.   Adjudication
Once the concern has been resolved, the case should proceed to adjudication.

C.   Overseas Processing
USCIS currently conducts name checks against TECS on most applicants, petitioners, beneficiaries, and dependents over the age of 14. These checks are conducted for individuals who are in the United States. DOS[**LE**]. As a result, in the case of individuals residing outside the United States, security checks may be performed [**LE**] by USCIS[**LE**].

DEF-00431531

National Background, Identity, and Security Check Operating Procedures

LE

After consultation with DOS [LE]

[LE] USCIS concluded that the background checks conducted on visa and refugee applicants abroad are commensurate with those performed by USCIS during the petition or application process in the United States. To streamline the process and eliminate duplicative efforts, USCIS modified previous TECS name check procedures on applications and petitions when the filing clearly establishes that the beneficiary and dependents are outside the United States and will apply for their visas or for refugee processing abroad.

While this reduced the number of security checks performed by USCIS, it did not compromise national security, as the affected individuals continue to undergo CLASS and other security checks by DOS as well as additional security checks initiated by USCIS during the visa and/or refugee resettlement application process and by CBP during the admission process.

D.   Refugee Processing

Refugee applicants undergo a series of security checks. All refugee applicants, regardless of age, undergo CLASS name checks, which are initiated at the time of pre-screening by the Resettlement Support Centers (RSCs) – organizations contracted by DOS. Responses are received prior to interview, with evidence of the response in the case file. If there is a new name, alias, alternate date of birth, or other high value identifier identified at the interview, USCIS requests another CLASS name check on the new information, and the case is placed on HOLD until that response is received. All case members must have cleared/resolved CLASS name checks on all names and dates of birth in order for a case to be approved.

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP──in whole or in part──unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431532

National Background, Identity, and Security Check Operating Procedures

> # LE

Enhanced FDNS Review (EFR) checks are conducted on select refugee applicants for the groups designated by USCIS as requiring this check. Refugee resettlement applicant EFR checks are processed by HQFDNS's Immigration Vetting Division and HQFDNS's Social Media Division, and responses must be received from both units before an application can be approved. Responsibility for reviewing matches identified by HQFDNS rests with International and Refugee Affairs Division (IRAD) staff. If a new name or other High Value Data Element associated with the applicant is developed at any point during the adjudication, IRAD may request EFR be run again on the applicant.

All refugee applicants ages 14-79 are fingerprinted prior to admission to the United States. In most processing locations, portable machines are used to electronically take 10-prints (rolls/slaps) and a digital photo. In those locations where portable technology is not possible, fingerprints are taken overseas on FBI FD-258 cards and submitted to OBIM IDENT prior to arrival at the POE. The fingerprints are run against:

- FBI/Criminal Justice Information Services (CJIS) records Next Generation Identification (NGI) system (formerly known as IAFIS) for criminal history and previous immigration data;
- OBIM IDENT, and the prints are enrolled in OBIM IDENT for future comparison; and
- The DOD Automated Biometric Identification System (ABIS) database

USCIS IRAD receives reports of individual fingerprint hits and reviews the records to determine whether the data impacts the refugee eligibility determination.[6] All case members within the designated age range must have cleared/resolved fingerprint results in order for a case to be approved.

> ### LE
>
> # LE

---

[6] CBP's National Targeting Center-Passenger additionally reviews any matches to DOD-ABIS to determine whether the information has a bearing on an applicant's admissibility to the United States prior to adjudication of the I-590.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP—in whole or in part—unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431533

National Background, Identity, and Security Check Operating Procedures

LE

E.   Service Center Processing

TECS Batch Runs: If an application/petition is filed stateside and then forwarded to the overseas post for processing, initial TECS batch runs are performed at the time of data entry on the petitioner, beneficiary and dependents in accordance with established policies and procedures, regardless of where they are physically located. Additionally, once the initial TECS batch run has been performed and a hit has been resolved, it is not necessary to update or refresh the validity of a TECS check for the petitioner, beneficiary or dependent at the time of a final decision if they are not physically present in the United States.

TECS Backend Checks: TECS backend checks, including alias name/variation checks either through an SQ11 query or TECS alias batch run, Just In Time (JIT) or Work Distribution runs and individual SQ11 queries at the time of adjudication, should not be performed by USCIS if the address indicated in the petition/application for the beneficiary is outside the United States, and there are no other objective indicators that would lead the adjudicator to believe that the beneficiary is physically present in the United States. In addition, there should be an indication that the beneficiary intends to apply for the visa abroad.

TECS security checks shall continue in accordance with established procedures when the petition/application indicates that the beneficiary and/or any of the dependents are physically present in the United States, or the adjudicator has sufficient reason to believe that the beneficiary and/or any of the dependents are physically in the United States.

National Background, Identity, and Security Check Operating Procedures

V.   Security Check: TECS

A.   TECS

1.   About TECS

Security checks have been expanded to include TECS on individuals seeking immigration benefits and travel documents. USCIS personnel use TECS to:

- Assist federal, state, and local law enforcement and intelligence agencies in identifying individuals who pose a risk to national security and/or public safety.
- Prevent ineligible aliens from obtaining immigration benefits.
- Identify petitioners ineligible to file family-based immigrant visa petitions in accordance with the Adam Walsh Act.

2.   About NCIC

The National Crime Information Center (NCIC) is a database maintained by the Federal Bureau of Investigation (FBI). NCIC includes the Interstate Identification Index (NCIC III) that allows authorized users to access criminal history information. ███████████████████████████
███
███
███
███
███
███████████████████████████

In addition, USCIS has access to other types of records, referred to as "   **LE**   hese records can be accessed through the SQ11 search of TECS. NCIC   **LE**

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431535

National Background, Identity, and Security Check Operating Procedures

B.   Who Requires TECS Queries

A TECS query must be run on the primary name and DOB for all new applications/petitions within 15 calendar days of initial receipt of the form at the location where it should be if properly filed and sent from the lockbox OR within 15 calendar days of initial receipt if not receipted at the lockbox[7]. Any derogatory information resulting from the initial query should be reviewed and, when necessary, referred to the appropriate officer or unit within a reasonable time. (Public safety concerns may require biometrics before appropriate referral) Resolution should be completed before adjudication and does not need to be completed at each TECS query.

Applications and petitions filed at the wrong location are not data entered, but instead must be sent to the proper location. If multiple receipt files are located in a single A-file, the same Record of Inquiry - TECS (ROIT – see Appendix I) can be used to encompass all required names from the applications/petitions and supporting documentation in that single A-file.

As USCIS moves toward a paperless adjudication process, TECS checks are more frequently run on a system-to-system basis (i.e., from ELIS, TECS by ELIS (TbE), or an automated TECS check in CAMINO) rather than through direct access to Modernized TECS. System-to-system checks typically employ either the ATLAS or PCQS service. Both ATLAS and PCQS employ

LE
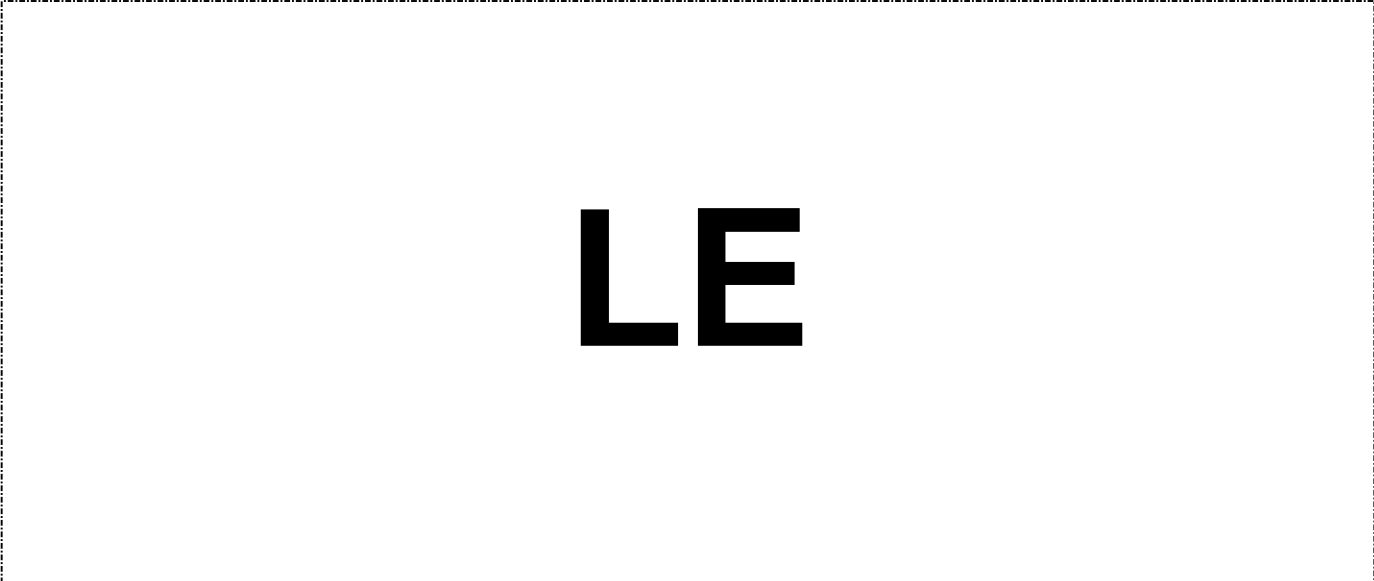
In addition, USCIS personnel who execute Modernized TECS and NCIC queries simultaneously (by checking the "NCIC" box under the Last Name field) must be mindful [**LE**] [**LE**] Detailed guidance on query procedures is in the process of being updated. In the interim, USCIS personnel should continue to follow the best

---

[7] CLASS and SAO name checks are conducted on I-590 and I-730 refugee applicants overseas. Department of State **LE**

31

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

practices currently outlined in Section V, Part D or local policy, if it requires checks that are only recommended in the NaBISCOP.

Note: Applications and petitions filed and adjudicated in USCIS international offices for applicants, beneficiaries, dependents, and derivatives that are not physically present in the U.S. are exempt from the requirement to undergo TECS checks within 15 calendar days of receipt; however TECS checks must be conducted on the primary name, dates of birth and alias prior to the final adjudication and, if applicable, travel document issuance.[8]

USCIS files that have been digitized are available in the Enterprise Document Management System (EDMS). These files are identified in the File Control Office (FCO) data field of Central Index System (CIS) by the "DIG" indicator and displayed as a comment in the history section and the status is marked as Digitized in RAILS.

If the A-file has been digitized and a new application or petition has been filed, the TECS process is as follows:

- Review the digitized A-file for all names/aliases and DOBs;
- Conduct a review of the new application/petition for any new names/aliases and DOBs;
- Query names/aliases and DOB variations; and
- Complete an ROIT for all queries conducted and place it in a T-file created for the new application/petition.

See the April 10, 2008, memorandum entitled "Adjudication and/or Processing of Cases When the File Control Office (FCO) Indicates (DIG) or (RDF)".

Note: Review of the digitized filing is not required for adjudication of Temporary Protective Status re-registration; however, if part of the digitized A-file is reviewed for adjudicative purposes, the part(s) of the digitized A-file that is reviewed for adjudicative purposes must be reviewed for TECS alias purposes. It is not otherwise necessary to review for TECS alias purposes the parts of the digitized A-file that were not reviewed for adjudicative purposes.

The table below lists, by form type, which subjects USCIS personnel must query in TECS. For appeals and motions, USCIS personnel must query those subjects required on the underlying petition/application type.

---

[8] [illegible vertical text]

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431537

National Background, Identity, and Security Check Operating Procedures

TECS Requirements by Form Type and Individual							
Form	Individual Requiring TECS Check (designated with "x")						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
BONDS				x			
EOIR-29	x		x	x	x	x	Query those subjects required on the underlying petition/application type. HH members 18 years of age and older.
I-90	x						Derogatory information from security checks to be resolved after adjudication.
I-94	x						
I-95	x						
I-102	x						
I-129			x	x			Business entities which are employment-based petitioners do not need to be queried, including sole proprietorship operated under a business name. But sole proprietorships operated under the owner's personal name must be queried and <u>may</u> require an RFE <u>or</u> additional system checks (e.g. CLEAR/Accurint) to obtain the biographical data needed for a TECS check.
I-129F			x	x			
I-129R Religious Worker			x	x			Petitioner query to include any names and addresses found in the file, belonging to the petitioning organization.
I-129S			x	x			

DEF-00431538

National Background, Identity, and Security Check Operating Procedures

TECS Requirements by Form Type and Individual							
Form	Individual Requiring TECS Check (designated with "x")						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-130			x	x[9]	x[10]		
I-131	x						Both petitioners and beneficiaries of HRIFA applications must be queried.
I-131A	x						Officers should consult the September 29, 2016 Standard Operation Procedure for issuing Carrier Documentation. USCIS International Operations ceased issuing "Boarding Letters" with the implementation of Form I-131A.
I-140			x	x	x		Business entities which are employment-based petitioners do not need to be queried, including sole proprietorship operated under a business name. But sole proprietorships operated under the owner's personal name must be queried and may require an RFE or additional system checks (e.g. CLEAR/Accurint) to obtain the biographical data needed for a TECS check.
I-191	x						
I-192	x						
I-212	x						

---

[9] In the case of individuals residing outside the United States, depending upon the application or petition type, security checks may be performed multiple times prior to their arrival into the United States by USCIS during the adjudication and travel document issuance process; by Department of State during the visa application or boarding foil issuance process; and by Customs and Border Protection inspectors at ports of entry as part of the admission process.

[10] TECS check to be completed on the derivative spouse in the event of death of the petition beneficiary, where petition reinstatement has been requested. This does not apply to USCIS International Operations, which only adjudicates I-130 Petitions filed on behalf of immediate relatives (spouse, child, parent), who may not claim derivatives.

34

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Form	Individual Requiring TECS Check (designated with "x")						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-290B	x		x	x	x	x	Query those subjects required on the underlying petition/application type.
I-360			x	x			Except for religious worker petitions, business entities to include sole proprietorships which are employment-based petitioners do not need to be queried. Individual persons are not considered business entities and must be queried in SQ11.
I-360 Religious Worker			x	x			Petitioner query to include any names and addresses found in the file, belonging to the petitioning organization.
I-485	x -		x *				- A TECS JIT check must be run on the applicant's primary name and DOB on the date of final adjudication of the form. Note: Administratively closed cases are *not* final adjudications and do not require a TECS JIT check. *TECS should be run on the petitioner of the family-based immigrant petition at the time of adjudication in support of the Adam Walsh Act.
I-485 Suppl. J	x *						*TECS should be run upon Supplement J submission (front end run from CLAIMS3) and again at the time of final I-485 adjudication.
I-526			x	x			
I-539	x				x		
I-589	x				x		

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431540

National Background, Identity, and Security Check Operating Procedures

Form	Individual Requiring TECS Check (designated with "x")						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-590							DOS LE **LE** LE IRAD conducts TECS checks of U.S. based anchor and qualified family members during RAVU processing of P-3, family reunification cases. CBP conducts **LE**
I-600			x	x		x	HH members 18 years of age and older; Beneficiaries between 14-16 years old.
I-600A	x					x	HH members 18 years of age and older.
I-601	x						Query those subjects required on the underlying petition/application type. See Section IV, Part C for more information on applications filed overseas.
I-601A	x						DOS will conduct CLASS and SAO checks when applicant is overseas. See Section IV, Part C for more information on applications filed overseas.
I-602	x						
I-612	x						
I-687	x						
I-690	x						
I-694	x						
I-698	x						
I-700	x						
I-730			x	x			See Section IV, Part C for more information on applications filed overseas.
I-751			x	x	x		Query spouse/step-parent through whom conditional residence was gained.
I-765	x						

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

TECS Requirements by Form Type and Individual							
Form	Individual Requiring TECS Check (designated with "x")						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-800			x	x		x	HH members 18 years of age and older; Beneficiaries between 14-16 years old.
I-800A	x					x	HH members 18 years of age and older.
I-817	x					x	Also query the legalized alien.
I-821	x						
I-821D		x					
I-824	x		x	x	x		Follow TECS querying procedures required by the underlying petition/application.
I-829	x				x		
I-881	x						
I-914	x						
I-914A	x						
I-918			x		x		
I-924	x						TECS is required on the applicant and the principals of the regional center, as well as on the address of the principal, and the name and address of the regional center.
I-924A	x						TECS is required on the applicant and the principals of the regional center, as well as on the address of the principal, and the name and address of the regional center, and the name and address of any affiliated Commercial Enterprises.
N-300	x						
N-336	x						
N-400	x				x		Query applicant's foreign born children between the ages of 14-18. If an applicant requests a name change, query the new name also. All required TECS checks for the applicant and children (i.e., all AKAs and name

37

National Background, Identity, and Security Check Operating Procedures

TECS Requirements by Form Type and Individual							
Form	**Individual Requiring TECS Check (designated with "x")**						**Special Instructions**
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
							variants for the applicant, primary name, and DOB for children) must be valid (no more than 180 days old) on the date of approval of the Form N-400 and on the date of the Naturalization Oath ceremony. Notwithstanding the above TECS checks, a TECS JIT check must be run on the applicant's primary name and DOB no earlier than (2) business days prior to the date of the applicant's Naturalization Oath ceremony.
N-470	x				x		
N-565	x						Derogatory information from security checks to be resolved after adjudication.
N-644	See Note*						*Query the decedent.

TECS Requirements by Form Type and Individual			
Form	**Individual Requiring TECS Check (designated with "x")**		**Special Instructions**
	Applicant	Child	
N-600	x	x	Query the applicant as well as the parent through which U.S. citizenship is derived or acquired. If the parent or legal guardian is the applicant filing on behalf of a minor child, then query the applicant as well as the child (if over 14) who will derive or acquire citizenship.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

TECS Requirements by Form Type and Individual							
Form	Individual Requiring TECS Check (designated with "x")						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
N-600K		x		x			Query the applicant as well as the child (if over 14) who will naturalize. For the purpose of this form *only*, the applicant is the parent, grandparent, or legal guardian who signs/files the form on behalf of the child.

Note: Pursuant to the Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance issued on December 26, 2018, TECS checks also are required for NTA issuance purposes. USCIS must issue an NTA after denying applications/requests or claims as described in "Updated Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Deportable Aliens," dated June 28, 2018, and the USCIS memorandum entitled "Domestic Operations Standard Operating Procedures, Form I-862, Notice to Appear" [11] dated September 8, 2006.

For DACA cases, refer to PM-602-0161, entitled "Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) When Processing a Case Involving Information Submitted by a Deferred Action for Childhood Arrivals (DACA) Requestor in Connection With a DACA Request or a DACA-Related Benefit Request (Past or Pending) or Pursuing Termination of DACA," dated June 28, 2018.

For additional information regarding TECS check requirements specific to NTA issuance, refer to Section XII of the Handbook.

USCIS personnel are authorized to perform the following types of TECS queries:

---

[11] In January of 2010, the Domestic Operations Directorate was split, as part of an agency-wide reorganization, into the Field Operations and Service Center Operations Directorates. References to Domestic Operations in the titles of memos cited in NaBISCOP should be assumed to apply to employees of both of the new directorates. The memos themselves will state whether they apply to Field Operations or Service Center Operations personnel.

National Background, Identity, and Security Check Operating Procedures

- Batch Query
- Person Query (Modernized SQ11)
- Organization and Address Query (Modernized [LE]
- NCIC III Criminal History Query (Modernized [LE]
- Others as deemed appropriate by component policy

C.   TECS – **Batch Query Procedures**

The objective of the Batch Query is to query a large number of records at the same time and confirm the existence or non-existence of information that relates to the search criteria entered.

Service centers and the National Benefits Center (NBC) are required to run a batch query on the primary names and DOBs on all new applications/petitions within 15 calendar days of initial receipt. The following CLAIMS 3 history action codes also trigger TECS batch queries:

Description of CLAIMS 3 History Action Codes	
History Action Code	Description
AA	Received
AALB	Received at the Lockbox
ABA	Received, Fee Waived
ABB	Received – Fee Collected Elsewhere
ADA	Fee Suspense Removed – Fee Accepted
ADB	Fee Suspense Removed – Fee Waived
CA	Relocated Received from Other INS Center or Office
HA	Response to Request Notice to Application/Petition Received
KEB	Date of Birth Change
KEN	Name Change

LE

Step-by-Step Batch Query Procedures	
Step	Action
1	
2	**LE**

40
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Step-by-Step Batch Query Procedures	
Step	Action
3	
4	
5	
6	
7	
8	
9	
10	
11	**LE**
12	
13	
14	
15	

LE

41

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431546

National Background, Identity, and Security Check Operating Procedures

LE

42

National Background, Identity, and Security Check Operating Procedures

LE

D.   TECS – Person Query Procedures (Modernized SQ11)

The objective of the Person Query is to confirm the existence or non-existence of information in TECS that relates to a subject of a pending application/petition.

The Person Query and NCIC **LE** must be run on the following subjects age 14 and over (see Section V, Part D Table of TECS Requirements by Form Type and Individual for specific form requirements):

- Applicant (Note: On the Form N-600K or, in some cases, the Form N-600, the adult who signs/files the application is treated as the applicant, although the child listed on the form receives the benefit.)
- Child (Person listed as receiving the benefit on Form N-600K or, in some cases, the Form N-600)
- Petitioner
- Beneficiary* (unless beneficiary is overseas)
- Derivative

43
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

LE

TECS queries are not required for the following:

- Subjects under the age of 14.
- A sole proprietorship is a business in which one person owns all the assets, owes all the liabilities, and operates in his or her personal capacity. A sole proprietorship can be operated under the name of its owner or it can elect to use a business name (Doing Business As –DBA). Sole proprietorships are considered business entities and do not require a Person Query if business is conducted under a DBA. However, sole proprietorships operated under the owner's personal name must be queried and may require an RFE or additional system checks (e.g. CLEAR/Accurint) to obtain the biographical data needed for a TECS check.
- Subjects who are deceased (except decedents on Application for Posthumous Citizenship, Form N-644).
- Aliases for beneficiaries and dependents not physically present in the United States. See the March 23, 2005 memorandum entitled "Discontinuation of IBIS Alias Name Checks for Petitions and Applications When the Beneficiary and Dependents Are Not Physically Present in the United States".
- Names found on system-generated Employment Authorization Document (EAD) A-Numbers. See the note below if it is believed that valid information may be obtained by running names from system-generated EAD A-Numbers in TECS. (A system-generated EAD A-Number will be between A100 000 000 and A199 999 999.)
- Certain cases involving Legalization/SAW applicants. For additional information see Legalization/Seasonal Agricultural Worker (SAW) (Section III.G.3) for more information within the handbook.

NOTE: If a query is conducted on an individual in cases where it is not required, document the query on a ROIT and complete the TECS memorandum as appropriate.

Step-by-Step Person Query Procedures	
Step	Action
1	Log in to TECS.
2	**LE**
3	
4	

National Background, Identity, and Security Check Operating Procedures

5	
6	
7	
8	
9	
10	
11	LE
12	
13	
14	
15	
16	

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

LE

Example of Person Query Options

LE

Example of NCIC Response Message

LE

1.   Person Search Criteria

A separate query must be conducted for every name and DOB combination identified for the subject on the application/petition or on supporting documentation in the file. Some files may contain multiple DOBs. Every alternate DOB located in the file should be queried with every

46

National Background, Identity, and Security Check Operating Procedures

name variation located in the file. See the figure below. Do not enter any information into the "middle name" field. Do not run TECS without a DOB (except when the subject's birth year does not appear on the application or on documents in the file, as described in the Section V, Part B table entitled "Examples of SQ11 Name Queries (DOB Queries)". Under certain circumstances, TECS may be queried without a DOB. These circumstances may be, but are not limited to:

> • Cases involving national security, egregious public safety, or other criminal concerns; and
> • Form I-924 and Form I-924A

An alias refers to additional names utilized by an individual. This includes but may not be limited to:

- Additional names used (birth name, nicknames, or other married names) in the application/petition, supporting documentation, or discovered during the interview or in the A-file;
- Names found in the "alias" field in CIS 9101 and 9202 screens; and
- Names entered in authorized systems and databases (excluding systems or databases that are known to produce system-generated names) or through documentation presented by the individual bearing the names.

The following items must be reviewed in the A-File/Receipt File for name and DOB combinations and aliases and require a TECS query:

- Current application/petition and supporting documentation, and
- Any previous applications/petitions in the same file that are reviewed during the course of adjudicating the current application or petition. For example:
  - When adjudicating an immigrant petition that is concurrently filed with an adjustment of status application, the supporting documentation of the immigrant petition and the portions of the A-file and supporting documentation from prior filings that are used to adjudicate the current petition must be checked at that time for aliases and DOB combinations. However, all documents in the A-file must be checked for aliases and DOB combinations at the time the adjustment of status application is adjudicated. See following two bullets regarding which documents are required to be checked for aliases and DOBs.
- All related USCIS required forms for current and previous application/petition in the file. For example:
  - Form G-325
  - Form ETA-750
  - Form ETA-9089
  - Form I 693 and Supplement to Form I-693

47

National Background, Identity, and Security Check Operating Procedures

- Any other documents in the A-file/Receipt file that establish relationship or identity including but not limited to the following:
  - Passports
  - Visas
  - Border Crossing Cards (BCC)
  - Forms I-94
  - Birth Certificates
  - Marriage Certificates
  - Divorce Decrees
  - Tax Documents
  - Diplomas/Academic Transcripts
  - Student Identification Cards
  - Military Identification Cards
  - Driver's Licenses
  - Social Security Cards
  - Business/Membership Cards

  LE

Query SUBJECT ALIASES as they appear on the application/petition and on supporting documentation in the file.

Personnel must also run any other alias found while adjudicating the form, whether in documentation or U.S. Government electronic databases and systems.

Additionally, you may check the following U.S. Government electronic databases and systems for additional name and DOB combinations and aliases:

- IDENT (Legacy US-VISIT IDENT)
- SEVIS
- CCD

Personnel must also query all additional aliases found in U.S. Government electronic database and systems during their routine adjudication or processing. For example, officers cannot ignore names, dates of birth or, aliases encountered while conducting appropriate system checks in the course of file adjudication of the respective form (see Table TECS Requirements by Form Type and Individual within the Handbook). Appropriate system checks for respective applications or petitions are defined locally and may vary. Check local policy for additional requirements.

Please note that there are US Government electronic databases and systems that are known to create name variants or system-generated aliases. The following databases/systems contain fields/sections that do not require review for name and DOB combinations and aliases:

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431553

National Background, Identity, and Security Check Operating Procedures

LE

NOTE: If listed as aliases, the names "DOE, John" and "DOE, Jane" are not considered valid aliases and should not be queried.

The following items in the A-File/Receipt File do NOT require review for name and DOB combination and aliases:

- Documentation that was not issued by a governmental (local, state, federal, foreign, etc.) or institutional authority (e.g., an education institution) as a form of identification
- Documentation that was not used by the subject to establish his/her relationship or affiliation with an entity or group
- Name as it appears in the signature block of an application/petition or signatures on supporting documents in the file

EXCEPTION: USCIS personnel are not required to search CIS for SUBJECT ALIASES for subjects not physically present in the United States, regardless of the presence of an A-Number.

See William R. Yates' March 23, 2005 memo, "Discontinuation of IBIS Alias Name Checks for Petitions and Applications When the Beneficiary and Dependents are not Physically Present in the United States".

Field offices that receive files from the National Benefits Center (NBC) do not need to conduct additional review of the file in search of any other alias name or date of birth used by the individual unless documentation is received after the NBC completes the TECS query.

NBC processing includes completing all TECS queries and resolving any positive results encountered during the query process in accordance with the NaBISCOP.

Upon receipt of an NBC-processed file, any alias names or dates of birth mentioned in the file will have been queried and resolved. All names and dates of birth encountered during the NBC file review and queried in TECS will be listed on the ROIT, with proper annotations. NBC will include a Resolution Memorandum articulating how the TECS information was resolved and the effect, if any, on the benefit sought.

If additional documentation is received after the NBC completes the TECS query, the field office must review the additional documentation for any other alias names or dates of birth that require querying and recording on the ROIT. If during the course of the interview an adjudicator becomes aware of any other alias name or date of birth, such name or date of birth will also require a TECS query and the results recorded on the ROIT. If a file does not contain

DEF-00431554

National Background, Identity, and Security Check Operating Procedures

information of any TECS queries being completed at the NBC, the field office must complete the TECS queries and resolve any positive results in accordance with NaBISCOP.

It remains the responsibility of the adjudicator to confirm that all required security checks have been completed prior to adjudication of the application or petition. For additional information see the memo "Interagency Border Inspection System Processing Completed at the National Benefits Center," dated December 7, 2005, and signed by Michael Aytes.

2.   Name and DOB Rules

In the examples contained in this section, last names are found in all capital letters.

> # LE

* Note: For more-detailed guidance about each field in the query, place the cursor in the relevant field and press the F2 button to access the Help menu.

Note: The ROIT will be notated that a [**LE**] was used and the name queried will be listed. In the first example in the table below, [**LE**] will be notated in ROIT.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Examples of SQ11 Name Queries (Name & DOB Rules)				
#	Primary Name	Instruction	Do NOT Query	MUST Query
1	**LE**		*(This section is intentionally blank.)*	**LE**
2			*(This section is intentionally blank.)*	
3			*(This section is intentionally blank.)*	

NOTE FOR NCIC QUERIES: **LE**

LE

51

National Background, Identity, and Security Check Operating Procedures

#	Last Name, First Name	DOB	NO MATCH	DNR	RELATES	Resolution Memo Completed?
1			LE			

#	Last Name, First Name	DOB	NO MATCH	DNR	RELATES	Resolution Memo Completed?
2			LE			

#	Last Name, First Name	DOB	NO MATCH	DNR	RELATES	Resolution Memo Completed?
3			LE			

a) Name and DOB Rules: Spelling Variations

Examples of SQ11 Name Queries (Spelling Variations)				
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	LE		*(This section is intentionally blank.)*	LE
2			*(This section is intentionally blank.)*	

52

DEF-00431557

National Background, Identity, and Security Check Operating Procedures

b) Name and DOB Rules: Name Variations/Aliases

Examples of SQ11 Name Queries (Name Variations/Aliases)
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1			*(This section is intentionally blank.)*	
2	**LE**		*(This section is intentionally blank.)*	**LE**
3			*(This section is intentionally blank.)*	
4			*(This section is intentionally blank.)*	

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431558

National Background, Identity, and Security Check Operating Procedures

c) Names with connectors (i.e. "DE," "Y," "DE LA,")

#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
	Examples of SQ11 Name Queries (Names with Connectors)			
1	LE		*(This section is intentionally blank.)*	LE
2			*(This section is intentionally blank.)*	

d) Name and DOB Rules: Two first names

#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
	Examples of SQ11 Name Queries (Two first names)			
1	LE		*(This section is intentionally blank.)*	LE
2			*(This section is intentionally blank.)*	

DEF-00431559

National Background, Identity, and Security Check Operating Procedures

e) Name and DOB Rules: First name only initials

Examples of SQ11 Name Queries (First name only initials)				
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	**LE**		*(This section is intentionally blank.)*	**LE**

f) Name and DOB Rules: Names with Initials

Examples of SQ11 Name Queries (Names with Initials)				
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	**LE**		**LE**	
2				
3			*(This section is intentionally blank.)*	**LE**

g) Name and DOB Rules: Names with Initials in front of the Name

Examples of SQ-11 Name Queries (Names with Initials in Front of a Name)				
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	**LE**		*(This section is intentionally blank.)*	**LE**

National Background, Identity, and Security Check Operating Procedures

h) Name and DOB Rules: Names with Periods

	Examples of SQ11 Name Queries (Names with Periods)			
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	**LE**		*(This section is intentionally blank.)*	**LE**

i) Name and DOB Rules: Name with Hyphens

	Examples of SQ11 Name Queries (Names with Hyphens)			
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	**LE**		*(This section is intentionally blank.)*	**LE**
2			*(This section is intentionally blank.)*	

56
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

3	**LE**

j)   Name and DOB Rules: Names with Apostrophes

Examples of SQ11 Name Queries (Names with Apostrophes)				
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	**LE**		*(This section is intentionally blank.)*	**LE**

k)   Name and DOB Rules: Names with Parentheses

Examples of SQ11 Name Queries (Names with Parentheses)				
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
1	**LE**		*(This section is intentionally blank.)*	**LE**

National Background, Identity, and Security Check Operating Procedures

l)   Name and DOB Rules: Names with Prefixes

#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
	Examples of SQ11 Name Queries (Names with Prefixes)			
1	**LE**		*(This section is intentionally blank.)*	**LE**

m) Name and DOB Rules: Names with Suffixes

#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
	Examples of SQ11 Name Queries (Names with Suffixes)			
1	**LE**		*(This section is intentionally blank.)*	**LE**

n) Name and DOB Rules: Found in Translations

#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
	Examples of SQ11 Name Queries (Found in Translations)			
1	**LE**		*(This section is intentionally blank.)*	**LE**

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

o) Name and DOB Rules: Foreign Alphabets

	Examples of SQ11 Name Queries (Foreign Alphabets)			
#	**Primary Name and Aliases**	**Instruction**	**Do NOT Query**	**MUST Query**
1	LE		(This section is intentionally blank.)	LE
2			ВОЛКОВ, Пётр	

LE

1. Foreign document. Name is in foreign alphabet. English translation (official or unofficial translation) is submitted.
    a. Query   LE
        i.   Do NOT query names   LE

        LE

2. Foreign document. Name is in English letters (possibly with special mark specific to the foreign language). English translation (official or unofficial translation) is submitted.
    a. Query   LE

        LE

59

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

3. Foreign document WITHOUT a translation.
   a. Name is in a foreign alphabet –Do NOT query

   LE

   LE

   b. Name is in English letters (possibly with special marks specific to the foreign language) – Do NOT query **LE**

   LE

p) Name and DOB Rules: Single Name Queries

#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
	Examples of SQ11 Name Queries (Single Name Queries)			
1	**LE**		*This section is intentionally blank.)*	**LE**
	LE			

q) Name and DOB Rules: DOB Queries
   Some files may contain multiple DOBs. Every alternate DOB located in the file should be queried with every name variation located in the file.

   LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
		Examples of SQ11 Name Queries (DOB Queries)		
1			*(This section is intentionally blank.)*	**LE**
2	**LE**		*(This section is intentionally blank.)*	
3			*(This section is intentionally blank.)*	*(This section is intentionally blank.)*

---

[12] If during the manual name harvesting process, an officer finds evidence of a year-only DOB where that year does not appear on any other DOB related to the case, then the officer should run a check in **LE** using the **LE** Any result returned **LE** he officer

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

	Examples of SQ11 Name Queries (DOB Queries)			
#	Primary Name and Aliases	Instruction	Do NOT Query	MUST Query
4	**LE**		*(This section is intentionally blank.)*	*(This section is intentionally blank.)*
5			*(This section is intentionally blank.)*	*(This section is intentionally blank.)*

should make the determination that the record relates or does not relate. If the LO record(s) relate, the officer should add the DOB associated with the LO record(s) into ELIS. ELIS will automatically run this new DOB with all names associated with the case and return the same LO record(s) as seen in modernized TECS.

[13] The officer should disposition the record(s) in ELIS and make the following notation in the comment field under the Risk and Fraud section: "DOB mm/dd/yyyy discovered during a TECS/NCIC check outside of ELIS. User pivoted t[**LE**]o complete [**LE**]which may not be executed in ELIS."
For more information, click HERE.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Examples of SQ11 Name Queries (DOB Queries)				
#	**Primary Name and Aliases**	**Instruction**	**Do NOT Query**	**MUST Query**
	LE			

* For example,

- If a 2/29 DOB from a non-leap year is found and another valid DOB is found elsewhere in the file, then:
    - Query **LE**
    - Query t~~LE~~
- If a valid 2/29 DOB and another valid DOB are found in the file, then:
    - Query **LE**

- If a 2/29 DOB from a non-leap year is found in the file and no other valid DOB found, then:
    - Query **LE**
    - Query **LE**

Example #1 **LE**

LE

Example #2: **LE**

LE

LE

63

DEF-00431568

National Background, Identity, and Security Check Operating Procedures

LE

E. TECS **LE** (Modernized **LE** and

LE

The objective of the **LE** is to confirm the **LE**

LE The objective of the

LE is to confirm the existence or non-existence of information in TECS that relates

LE

LE

LE query must be run for the following:

- Petitions for religious workers (i.e. Forms I-360RW and I-129R) including change of status and extensions of stay for these petitions.
- Application for Adjustment of Status (Form I-485) if the underlying I-360 has not been queried.

For all other case types, the query may be conducted at the discretion of USCIS personnel. The TECS **LE** must be conducted for:

- Current petitions for religious workers (i.e. Forms I-360 RW and I-129R) and supporting documentation, and
- Any previous applications/petitions (i.e. Forms I-360 RW and I-129R) in the same file that are reviewed during the course of adjudicating the current application or petition. For example:
  - o When adjudicating Religious Worker Form I-360 RW and I-129R petitions, the supporting documentation of the petition and the portions of the A-file and supporting documentation from prior filings that are used to adjudicate the current petition must be checked at that time for other addresses.

Note: The TECS **LE** must be conducted for religious organizations by the Adjudicating Officer, unless the case has already been referred to the Center Fraud Detection Operations (CFDO) or the Fraud Detection and National Security Immigration Officer (FDNS-

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP—in whole or in part—unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431569

National Background, Identity, and Security Check Operating Procedures

IO) in accordance with established fraud referral procedures. For more details, see the July 5, 2006 guidance.

- Section V.E.1 -
- Section V.E.2 -

LE

1.   LE   Search Criteria

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

LE

66

National Background, Identity, and Security Check Operating Procedures

LE

67
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

LE

F.   TECS – I-94 Query Procedures (Modernized SQ94)

The objective of the I-94 Query (I-94 Arrival/Departure Record) is to confirm the existence or non-existence of information in TECS about a non-immigrant's arrival/departure record. I-94 Query results can yield valuable information for the adjudication of other applications/petitions.

For all applications/petitions involving a change of status or extension of stay, please see the Arrival/Departure Non-Immigrant Information System (ADIS) for more information.

Note: When applicable to the application or petition, a USCIS officer must review any and all Arrival/Departure information in an appropriate DHS system.

1.   Arrival/Departure Non-Immigrant Information System Queries

Most non-immigrants entering the United States submit a record of Arrival/Departure at a Port of Entry (POE) and are assigned an admission (I-94) number. The admission number is a method of uniquely identifying a non-immigrant and ensuring a positive match in the database between records generated by that person's arrival and departure plus any updated forms.

For applications and petitions where I-94 Query is required or conducted at the officer's discretion:

- Conduct query no more than 15 days before final adjudication.
- Include a screen printout in the file OR annotate the date of the query and "No Record Found" on the form, when appropriate.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

- If "No Record Found", conduct additional search with name, date of birth, and passport number as found in subject's Form I-94, Arrival/Departure Record, or other official documentation.
- Positive match results screens must be printed and included in the file.
- Information in the I-94 record, the application/petition, and CLAIMS3 must match.
- Aliases, when found on I-94 printouts, must receive a Person Query in Modernized SQ11.
- Place printouts on the non-record side of the file. Remember that TECS printouts must be properly marked.

To conduct I-94 Query	
Step	Action
1	**LE**
2	
3	
4	
5	

2.   INQUIRY (I-94) Report

LE

I-94 Procedures	
Step	Description
1	**LE**
2	
3	
4	

69

National Background, Identity, and Security Check Operating Procedures

I-94 Screen – By Person/ I94/Other

LE

Data returned from this query will include all of the above information plus   **LE**
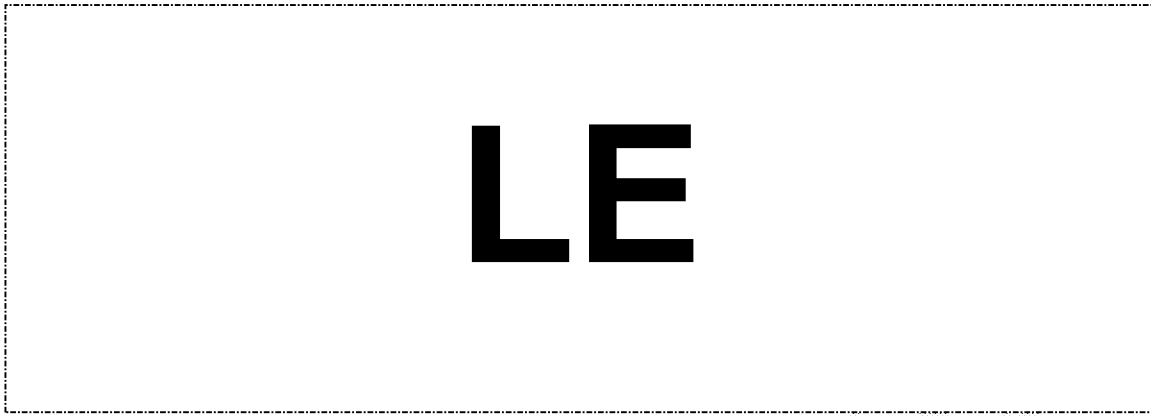
LE

70
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

LE

3. **LE**

LE

G.   TECS - NCIC III Criminal History Query Procedures (Modernized **LE**

On May 23, 2011, the Federal Bureau of Investigation (FBI) Criminal Justice Information Service (CJIS) Division informed USCIS that access to NCIC III is now strictly limited to FDNS personnel only for criminal justice purposes.

The only situations in which NCIC III may be accessed are:

- When an individual has been determined to have, or is likely to have, a link to a current or planned criminal activity and the case is referred to FDNS for further investigation with the appropriate law enforcement agency – this determination may be arrived at from an interview, tip letter, or the existence of an open investigation that indicates current or planned involvement in criminal activity;
- When a reasonable suspicion of fraud is identified that may be referred to U.S. Immigration and Customs Enforcement (ICE) for criminal investigation; or
- When an individual has been determined to be involved in current or planned terrorist activity.

71

National Background, Identity, and Security Check Operating Procedures

1.   **Process for Conducting NCIC III Queries**

a.   Determination whether to run NCIC III Checks

Pursuant to guidance issued on March 18, 2012, access to NCIC III is now strictly limited to FDNS personnel only for criminal justice purposes. The only situations in which NCIC III may be accessed are:

- When an individual has been determined to have, or is likely to have, a link to a current or planned criminal activity and the case is referred to FDNS for further investigation with the appropriate law enforcement agency – this determination may be arrived at from an interview, tip letter, or the existence of an open investigation that indicates current or planned involvement in criminal activity;
- When a reasonable suspicion of fraud is identified that may be referred to U.S. Immigration and Customs Enforcement (ICE) for criminal investigation; or
- When an individual has been determined to be involved in current or planned terrorist activity.

FDNS Officers and BCU Officers located at the Service Centers will review all cases involving fraud, national security concerns and criminal concerns to determine whether NCIC III should be run. They will evaluate whether the facts of a particular case fit the criteria cited above.

When the BCU officer has determined that a NCIC III check is permitted in cases involving national security or criminal concerns, he or she will refer the case and supporting material to the Center Fraud Detection Office (CFDO). A FDNS employee will review the recommendation and determine whether to run the check.

If the FDNS employee determines that the NCIC III criteria are met, he or she will follow the steps outlined below and indicate this decision in FDNS-DS.

b.   Performing NCIC III Checks

The FDNS employee will conduct a search of NCIC III for the subject. He or she will follow standard procedures to determine whether the NCIC III record(s) relates to the subject. For instructions for recording this step in FDNS-DS, see sections A.4 and B.4 of Documenting NCIC III Queries within the handbook.

1.   If no records relating to the subject are found, the FDNS employee must document such in FDNS-DS. If the search was requested by the BCU, the FDNS employee will then return a response to the requesting BCU officer, indicating that no relevant information was found in NCIC III.

DEF-00431577

National Background, Identity, and Security Check Operating Procedures

2.   If records relating to the subject are found in NCIC III, the FDNS employee will determine whether the arresting authority should be contacted to authorize release to adjudications. In making the determination whether to contact the arresting authority, the FDNS employee will evaluate the information in NCIC III and determine whether it relates to a criminal, fraud, or national security purpose for which it was sought. If the search was requested by the BCU and the FDNS employee determines that the NCIC III record is not relevant, he or she will then return a response to the BCU officer, indicating that no relevant information was found in NCIC III.

c.   Coordination with the Arresting Authority

If relevant information is revealed through the NCIC III query, the FDNS employee will contact the arresting authority to obtain permission to share the information with adjudications. The FDNS employee will directly contact the entity and explain USCIS's need for the information. FDNS employees will explain to the arresting authority how the information will be used. For example, information may be used as a pointer to public record information, as the basis for a request of a criminal disposition or other evidence from the applicant, or to inform questioning during an interview.

The FDNS employee must capture the arresting authority information and details regarding the information authorized for release for input to FDNS-DS. Instructions for recording this step in FDNS-DS are detailed in sections A.3 and .5 and B.3 and .5 of Documenting NCIC III Queries within the Handbook.

d.   Providing a Response to Adjudications

If the arresting authority authorizes and agrees that information may be shared with adjudications, FDNS employees will share the information in the following formats:

- National security-related information authorized for release by the arresting authority should be provided to the adjudicator or BCU officer through a Background Check and Adjudicative Assessment (BCAA); and
- Fraud and criminal information authorized for release by the arresting authority should be provided to the adjudicator or BCU officer through a Statement of Findings (SOF).

If the record owner does not agree to share the requested information, the FDNS employee must indicate this decision in FDNS-DS. If the request originated from the BCU, the FDNS employee

73

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

must also inform the requesting BCU officer about the arresting agency's decision. Instructions for recording this step in FDNS-DS are detailed in sections A.5 and B.5 of Documenting NCIC III Queries within the Handbook.

Note: Screen prints of NCIC III or IdHS (formerly known as RAP sheets) from the system must not be shared with adjudications and must be destroyed after use.

2. Documenting NCIC III Queries

An existing FDNS-DS record must be updated to reflect the NCIC III check. If the subject of the NCIC III check does not have a FDNS-DS record, the FDNS employee must create one. Depending on the reason for which the check was performed, the information will be recorded under either the NS Tab (National Security) or the Case Tab (Fraud or Criminal). Each FDNS-DS record must contain the following essential elements of information:

1. Name of the individual performing the NCIC III query – record your contact information, the date on which the query was performed, and the identities that were searched;
2. Justification – provide a brief summary of the information to clearly indicate which of the three authorized reasons for access was met (an individual has been determined to have, or is likely to have, a link to a current or planned criminal activity and the case is referred to FDNS for further investigation with the appropriate law enforcement agency; when a reasonable suspicion of fraud is identified that may be referred to ICE for criminal investigation; or when an individual has been determined to be involved in current or planned terrorist activity);
3. Query result – indicate whether or not [LE] was discovered that related to the applicant, petitioner, or beneficiary;
4. Arresting Agency Information (if applicable) – document the name of the arresting agency along with contact information (name of point of contact, phone number[s], and e-mail address[es]); indicate whether or not they authorized the use or release of any or all of the [LE] on the subject. In the event there is more than one record, record the contact information for each arresting agency; and
5. NCIC III information authorized for release (if applicable) – summarize the information from each record that was authorized for release; a copy of the document provided to adjudications or BCU Officer (BCAA or SOF) will be attached to the record in FDNS-DS.

a.   National Security Related Requests: National Security (NS) Concerns Tab

1. NCIC III query

DEF-00431579

National Background, Identity, and Security Check Operating Procedures

To record the NCIC III query:

a. Enter the subject's NS Concern. If one does not exist for the subject, create an NS Concern in accordance with the FDNS-DS NS Concerns Tab User Guide. Navigate to the Activities Sub-tab under the NS Concerns Tab. Select ⸺⸺⸺**LE**⸺⸺⸺ ⸺⸺**LE**⸺⸺ from the drop-down box under the "Type" field depending on the basis of the request. If the basis for the request does not meet the criteria for querying NCIC III, select ⸺⸺**LE**⸺⸺

b. Next, navigate to the System Checks Sub-tab under the NS Concerns Tab and click on the "New" button to generate a blank row. The "Process Phase" field automatically populates with the current Process Phase.

   - Select NCIC III from the drop-down box under the "System" field.
   - Choose the FDNS employee who conducted the NCIC III query from the pick list in the "Conducted By" field.
   - Enter the date the FDNS employee conducted the NCIC III query in the "Conducted Date" field.

2. Justification for querying NCIC III

To record the justification for querying NCIC III, in the System Check Sub-tab entry created per the instructions in this document, Section A, Part 1(b) enter the specific facts which led the FDNS employee to conduct the query in the "Comments" field. Include:

a. The source (s) of the information, ex. Tip letter, suspicious document, other background checks; and

b. A summary of the information itself.

3. Authorization to release information to adjudications (Only required if the NCIC III query produces a record, and FDNS is permitted to share the information with adjudications). If the FDNS employee would like to share information obtained from NCIC III with adjudications, the arresting agency owning the criminal history record must first be contacted for permission. The following information must be documented in FDNS-DS:

a. Arresting Agency Point of Contact name;

b. Arresting Agency;

c. Arresting Agency phone number and email address (if available); and

d. Date the Arresting Agency either gave or declined authorization.

To record authorization information, navigate to the Deconflictions Sub-tab under the NS Concerns Tab and click on the "New" button to generate a blank row. The "Deconfliction

75
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431580

National Background, Identity, and Security Check Operating Procedures

#" field automatically populates with a unique identifier, the "Start Date" field automatically populates with the date the new row was created, and the "Phase" field automatically populates with the current Process Phase.

a. Choose the arresting agency POC contacted from the pick list in the "Agency Contact Last Name" field. The "Agency Contact First Name" will then automatically populate. The "Agency" and "Contact Phone #" fields will also automatically populate if such information is already available in FDNS-DS. If the arresting agency contact, agency, or contact phone number is missing, edit the arresting agency's contact People entry to include that information. If the arresting agency's contact is not found, create a People entry for that person by clicking on the "New" button within the pick list in the "Agency Contact Last Name" field.
b. Enter the date the arresting agency either gave or declined authorization in the "End Date" field.
c. Enter the arresting agency's contact email address in the "Comments" field.

If the arresting agency requires a written request for authorization from FDNS, this may be attached in the Attachments Sub-tab.

4. NCIC III query result
    To record the NCIC III query results, in the System Check Sub-tab entry created per the instructions in Section A, Part 1(b) select the appropriate result from the "Results" field drop- down box:
    a. DNR/No record – select if there is either no record or the record does not relate;
    b. Record-Release – select if record relates, and the record owner has authorized the release of some or all of the information; or
    c. Record-No Release – select if record relates, and the record owner has declined authorization to share information.
    d. In addition, in the Activity Sub-tab entry created per the instructions in Section A, Part 1(a) select the appropriate result DNR/No record, Record-Release, or Record-No Release from the "Status" field drop-down box.

5. NCIC III information authorized for release

If the arresting agency has authorized release of information obtained from NCIC III to adjudications, provide a description of the record(s) that has been authorized to be shared in the "Comments" field of the Authorization entry created per the instructions in Section A, Part 3. Include the following information:

DEF-00431581

National Background, Identity, and Security Check Operating Procedures

a. Arrest Date;
b. Arresting agency; and
c. Disposition (if known).

Screen prints of NCIC III or IdHS (formerly known as RAP sheets) from the system must not be placed into the A-File or into FDNS-DS. FDNS will print the Background Check and Adjudicative Assessment (BCAA) and place in the A-file.

b.   Fraud and Criminal Related Requests: Case Tab

1.   NCIC III query

To record the NCIC III query, enter the subject's Case. If one does not exist for the subject, create a Case in accordance with the FDNS-DS User Guide. Navigate to the Activities Sub- tab under the Case Tab and click on the "New" button to generate a blank row. Select Background Checks from the drop-down box under the "Type" field depending on the basis of the request. If the basis for the request does not meet the criteria for querying NCIC III, select NN16-Not Justified.

2.   Justification for querying NCIC III

To record the justification for querying NCIC III, in the Activity Sub-tab entry created per the instructions in Section B, Part 1 enter the specific facts which led the FDNS employee to conduct the query in the "Comments" field. Include:

a. The source (s) of the information, ex. Tip letter, suspicious document, other background checks; and
b. A summary of the information itself.

3.   Authorization to release information to adjudications (Only required if the NCIC III query produces a record, and FDNS would like to share the information with adjudications). If the FDNS employee would like to share information obtained from NCIC III with adjudications, the arresting agency that holds the criminal history record information must first be contacted for permission. To record authorization information, in the Activity Sub-tab entry created per the instructions in Section B, Part 1 enter the following information in the "Description" field:

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP⸺in whole or in part⸺unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

      a. Arresting Agency Point of Contact name;

      b. Arresting Agency;

      c. Arresting Agency phone number and email address (if available); and

      d. Date the Arresting Agency either gave or declined authorization.

If the arresting agency requires a written request for authorization from FDNS, this may be attached in the Attachments Sub-tab.

4.   NCIC III query result

To record NCIC III query results, in the Activity Sub-tab entry created per the instructions in Section B, Part 1 select the appropriate result from the "Status" field drop-down box:

    a. DNR/No record – select if there is either no record or the record does not relate;
    b. Record-Release – select if record relates, and the arresting agency has authorized the release of some or all of the information; or
    c. Record-No Release – select if record relates, and the arresting agency has declined authorization to share information.

5.   NCIC III information authorized for release

If the arresting agency has authorized release of information obtained from NCIC III to adjudications, provide a description of the record(s) that have been authorized to be shared in the "Systems Checked" field of the SOF Sub-tab under the Case Tab. Click on the "Systems Checked" Multi-Value Group (MVG), and then click on "New." Select NCIC III from the LOVs and include a summary of the following information under the "Description" field:

    a. Arrest Date;
    b. Arresting agency; and
    c. Disposition (if known).

Screen prints of NCIC III or IdHS (formerly known as RAP sheets) from the system must not be placed into the A-File or into FDNS-DS. FDNS will produce a Statement of Findings (SOF) and place in the A-file.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

        DEF-00431583

National Background, Identity, and Security Check Operating Procedures

H.   Types of Results from TECS Queries

1.   Results of TECS Queries

The following are possible system results when conducting a | **LE** | Query:

-
-
-

> **LE**

2.   Types of Hits

a)   National Security

Any TECS hit that may indicate an NS concern must be processed in accordance with the Controlled Application Review and Resolution Program (CARRP) policy memorandum issued on April 11, 2008. Refer to section IX, Resolution: National Security Concerns (CARRP) within the Handbook. Officers may also refer to the guidance "Criteria to Consider for Determining if a NS TECS Hit Relates to an Applicant" in Part K. Resolution Process.

- Known or Suspected Terrorist (KST)
- TECS: Record number begins with the letter **LE** and ends with **LE** The record indicates the individual is a " **LE** or " **LE** The record lists the contact as NTC 24X7 lookout duty officer.
- NCIC: Record requests contact with the Terrorist Screening Center (TSC). **LE** s listed as the TSC. NIC # begins with the letter **LE** [5]
- In accordance with CARRP, the designated officer contacts the Terrorist Screening Center to confirm whether the subject of the KST hit relates to the individual seeking an immigration benefit.
- Other NS indicators:
  - o   TECS hits that indicate an individual or organization may have prior, current or planned involvement in or association with an activity, individual, or organization described in section 212(a)(3)(A), (B) or (F) or 237(a)(4) (A) or (B) of the Act.
  - o   The following TECS and NCIC Status Codes and Code Descriptions may (or may not) be indicators of an NS concern, depending on the circumstances of the case. Further inquiry by the officer is needed. These codes should not be considered a

---

[15] For information and instructions on resolving **LE** records with no corresponding TECS **LE** records ("stand-alone **LE**), please refer to Section V, Part K, Step 4C within the Handbook.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431584

National Background, Identity, and Security Check Operating Procedures

complete list of codes that the officer may encounter. The officer must verify any unfamiliar codes encountered.

TECS Table Code Descriptions	
TECS Table Code	Code Description
LE	

NCIC Offense Code Descriptions	
NCIC Offense Code	Code Description
LE	

Refer to the CARRP Guidance for a detailed list of potential indicators and additional terms and acronyms related to TECS which may or may not be indicators of an NS concern, depending on the circumstances of the case.

b)   Egregious Public Safety

Any TECS hit that may indicate it meets the definition of an EPS case as defined in Policy Memorandum 110, refer to section X.

c)   INTERPOL

The International Criminal Police Organization (INTERPOL) is the world's largest international police organization, with 188 member countries. It facilitates cross-border police co-operation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.

INTERPOL aims to facilitate international police co-operation even when diplomatic relations do not exist between particular countries. Action is taken within the limits of existing laws in different countries and in the spirit of the Universal Declaration of Human Rights. INTERPOL's constitution prohibits 'any intervention or activities of a political, military, religious or racial character.' INTERPOL does not vet the evidence substantiating arrest warrants; it is a venue for the posting of information.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

One of INTERPOL's most important functions is to help police in member countries share critical crime-related information using the organization's system of international notices. The seven types of notices and their objectives are:

	Red Notice To seek the location and arrest of wanted persons with a view to extradition or similar lawful action. View Red Notices		**Yellow Notice** To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves. View Yellow Notices
	Blue Notice To collect additional information about a person's identity, location or activities in relation to a crime.		**Black Notice** To seek information on unidentified bodies.
	Green Notice To provide warnings and intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.		**Orange Notice** To warn of an event, a person, an object or a process representing a serious and imminent threat to public safety. View Orange Notices
	INTERPOL–United Nations Security Council Special Notice Issued for groups and individuals who are the targets of UN Security Council Sanctions Committees.		**Purple Notice** To seek or provide information on modi operandi, objects, devices and concealment methods used by criminals.

Please access the INTERPOL website for more information on these notices. Information about contacting INTERPOL for more information can be found on the Liaison Branch ECN page under the FDNS Directorate.

d)   All Other Hit types

LE

81

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431586

National Background, Identity, and Security Check Operating Procedures

LE

LE

I.   Validity of Results from TECS Queries

The validity period for a TECS query is 180 calendar days, as stated in the April 26, 2006, memorandum entitled "Extension of the Interagency Border Inspection System (IBIS) Record Check Validity Period." However, a Just In Time (JIT) check must be conducted in TECS on the primary name and date of birth on the day of final adjudication (approval or denial) for any Form I-485, and within two (2) business days of the Oath ceremony for any approved Form N-400 (also see below). Note: A JIT check is not required within two (2) business days of a Form N-400 denial. See the February 6, 2009 memo entitled "Additional Guidance on Issues Concerning the Vetting and Adjudication of Cases Involving National Security Concerns" for further information. See also the Consolidated Handbook of Adjudication Procedures (CHAP) Volume 13, Part C, Chapter 7.

TECS queries must be valid at the following times:

- Time of final decision as indicated on the application/petition (i.e. approval, denial, abandonment denial, revocation (excluding automatic revocation), reaffirmation) (Note: A JIT check must be run on any Form I-485 on the day of final adjudication. No JIT check is required on any I-485 that is administratively closed.)
- Time of Naturalization ceremony. (Note: The general 180-day validity period applies not only at the time of Form N-400 approval, but also at the time of the N-400 applicant's Naturalization. Accordingly, offices experiencing a significant delay between Form N-400 approval and Naturalization must ensure that all required TECS checks—not merely for the primary name and DOB—will remain current on the date of Oath ceremony. In addition, a final TECS JIT check on the primary name and DOB must be run within no earlier than (2) business days prior to the date of the applicant's Naturalization Oath ceremony.
  For additional details, refer for Section V, Part B table of TECS Requirements by Form Type and Individual.
- When the beneficiary of the family-based immigrant petition (approved on or after July 27, 2006) adjusts status
  - This is a TECS query of the petitioner, per the Adam Walsh Act. Please see the Form I-485 entry in the table entitled "TECS Requirements by Form Type and Individual" in Part B of this Section.

82

National Background, Identity, and Security Check Operating Procedures

- When a pending application/petition is relocated from a service center to a field office or asylum office.
- When an appeal or motion is relocated to an appellate body (i.e. AAO, BIA)
- When an I-751 has been denied:
  - o "ADMIN CLOSED – OTHER" - only when the beneficiary was misclassified and a new card is being issued.
- When Conditional Residence Status has been terminated for failure to file and I-751:
  - o "DENY FAILURE TO FILE"
- When temporary evidence of lawful permanent residence is provided to an alien (i.e. ADIT stamp in passport or on I-94)
- When notices are reissued in conjunction with a name or DOB change or with Form I-824

Notwithstanding the general 180-day validity period for TECS/NCIC queries and resolutions, TECS/NCIC queries must be re-run when a USCIS officer issues a Notice to Appear (NTA) in order to initiate removal proceedings.

TECS queries must be performed on additional name and DOB variations discovered. See Person Query Procedures (Modernized SQ11) for guidance within the Handbook.

TECS queries may not be required in the following instances because no new adjudicative action is being taken; however, look to component-specific policy:

- Updating case as ADMINISTRATIVE CLOSE (Except for denied I-751s and terminated Conditional Residence Status cases as noted above)
- Updating case as CASE TERMINATED; STATUS ACQUIRED THROUGH OTHER MEANS; PETITION TERMINATED BY DOS
- Changing validity dates of a benefit
- Re-issuing notices other than a name or DOB change or Form I-824
- Re-issuing undeliverable cards
- Issuing a card where the benefit was granted overseas
- Issuing an approval notice for North American Free Trade Agreement (NAFTA) cases adjudicated by CBP on the Canadian border
- Issuing a Refugee EAD adjudicated at the Port of Entry (POE)
- Processing refugee cases, as DOS runs comparable checks on overseas applicants and CBP conducts TECS name checks on all refugee applicants at the Port-of-Entry upon arrival

DEF-00431588

National Background, Identity, and Security Check Operating Procedures

J.   Where to Place Results from TECS Queries

1.   Retaining TECS Screen Prints

All retained TECS screen prints (hard copy or electronic) must be labeled with the following language:

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C. § 552). This information shall not be distributed beyond the original addressees without prior authorization of the originator. This document and the data herein are derived from TECS and are loaned to USCIS for official use only. This document or the information contained herein should be directed to the agency from which the document/information originated or Customs and Border Protection - Freedom of Information Act (FOIA) Office. Disclosure provisions have been established by the document, Memorandum of Understanding between Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Services (USCIS) for use of TECS.

Instead of marking each page with the TECS disclosure notice, officers may attach a TECS Disclosure Notice cover sheet on top of all TECS printouts. Each individual page must still be marked "For Official Use Only – Law Enforcement Sensitive," or "FOUO/LES."

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

For Official Use Only/Law Enforcement Sensitive

WARNING

TECS documents are LAW ENFORCEMENT SENSITIVE (LES) information. They contain information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). TECS documents are to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and are not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized CBP official.

For Official Use Only/Law Enforcement Sensitive

85
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

2.   **Documentation of TECS Query**

3.   **Annotating the ROIT**

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP⸺in whole or in part⸺unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

Description of Fields on the ROIT Worksheet		
#	ROIT Field Name	Description
8	[Blank Space]	**LE**

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

4.   Explanation of the Completed ROIT

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431595

National Background, Identity, and Security Check Operating Procedures

91
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431597

National Background, Identity, and Security Check Operating Procedures

93
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

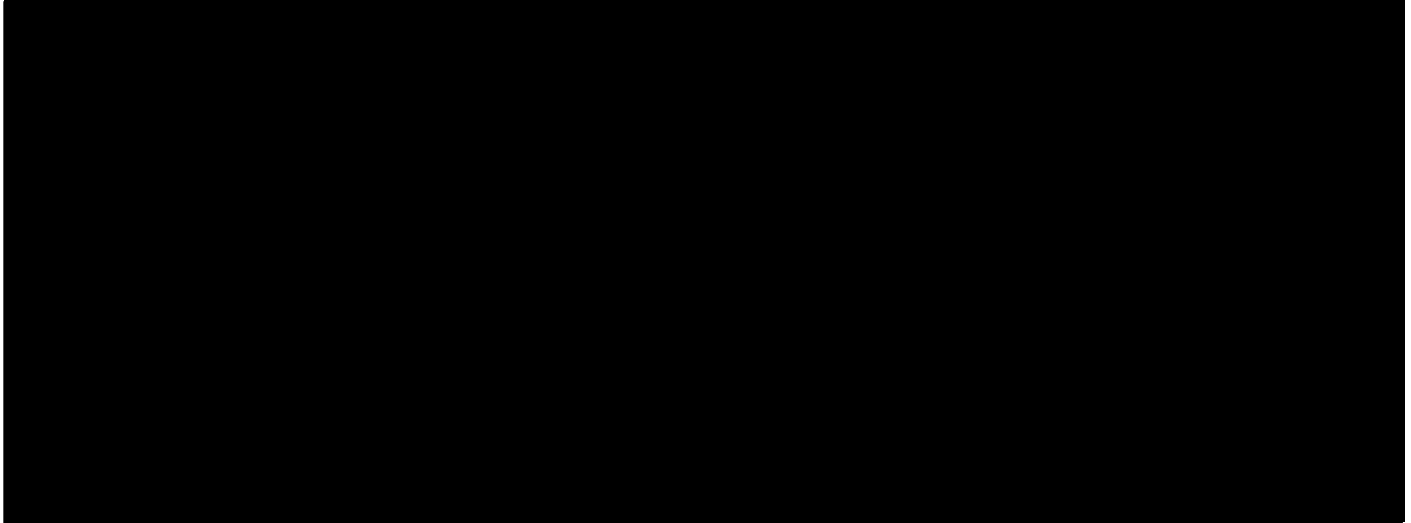| Search #	Search Criteria	Description
1		
2		
3		
4		

LE
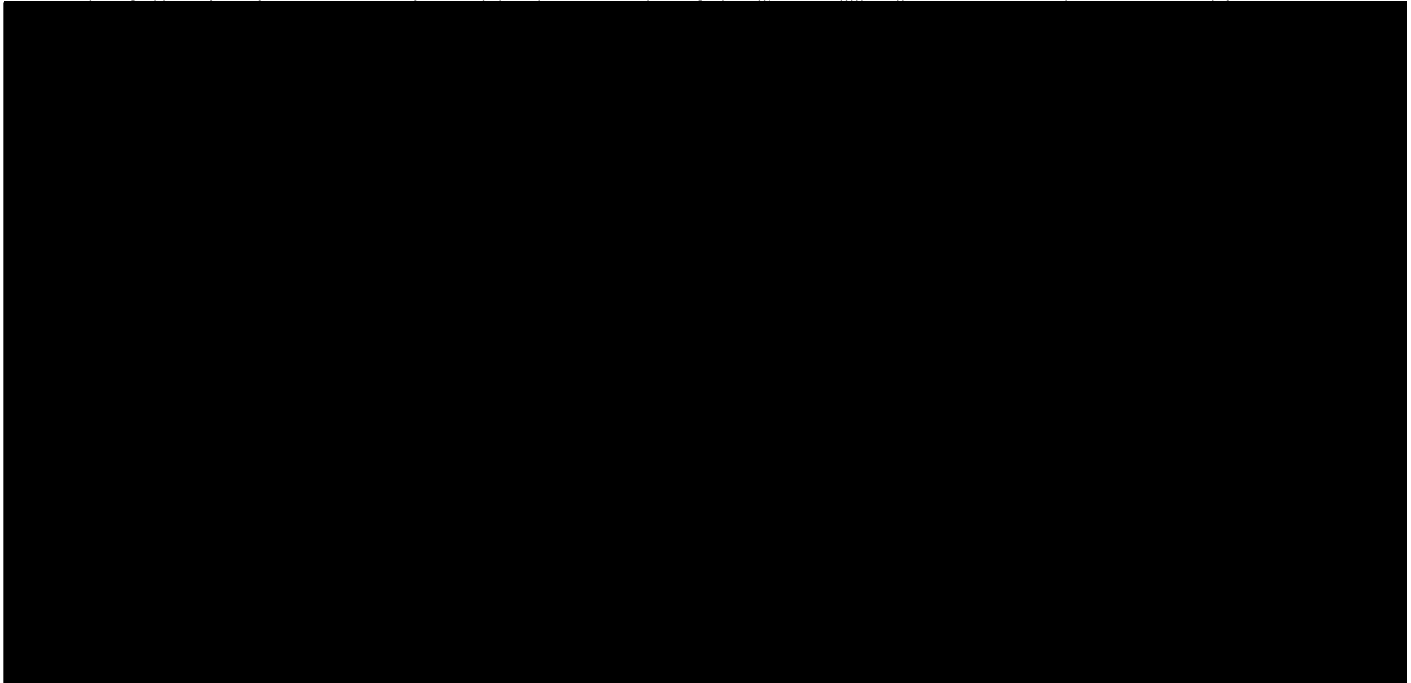
94

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
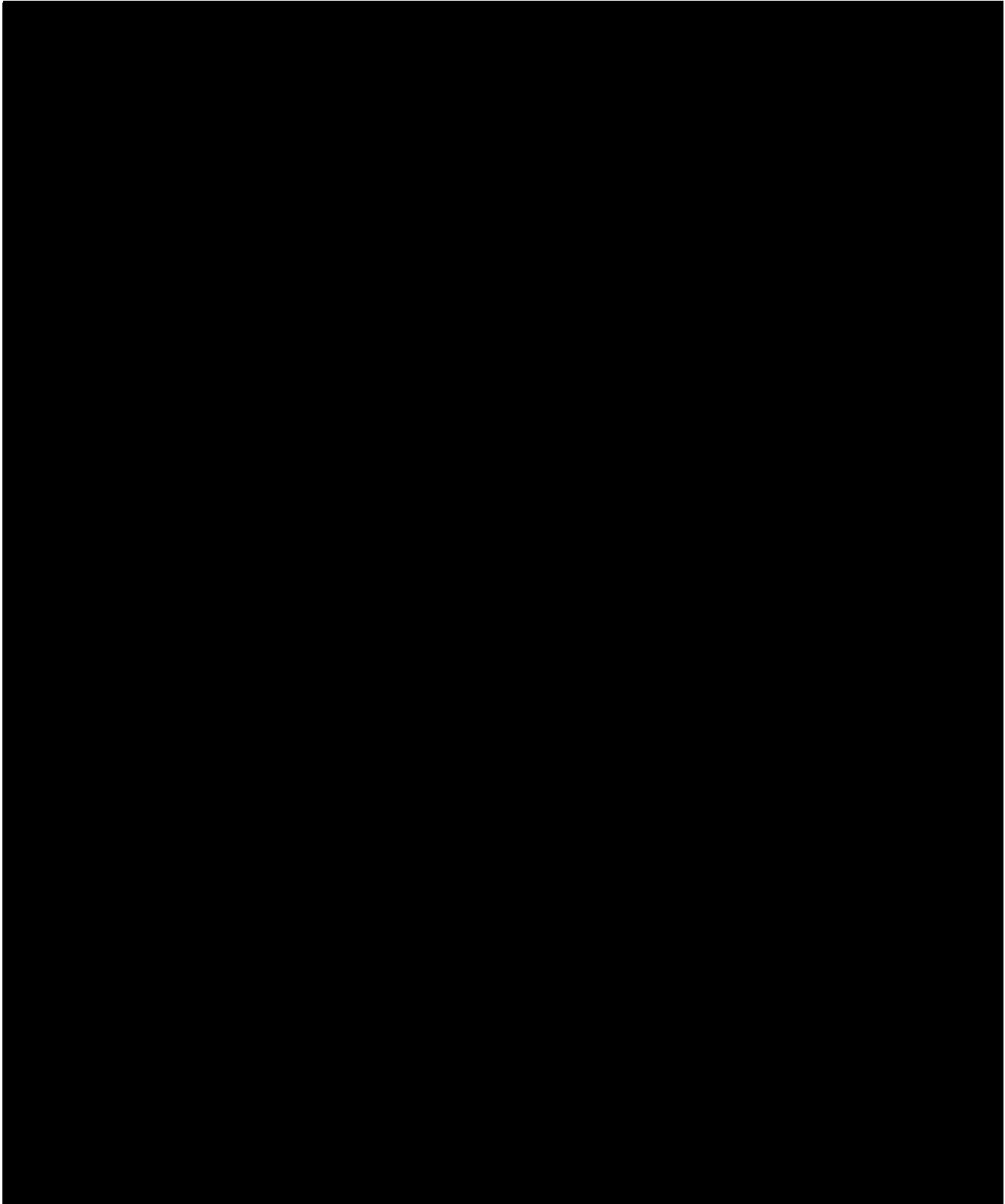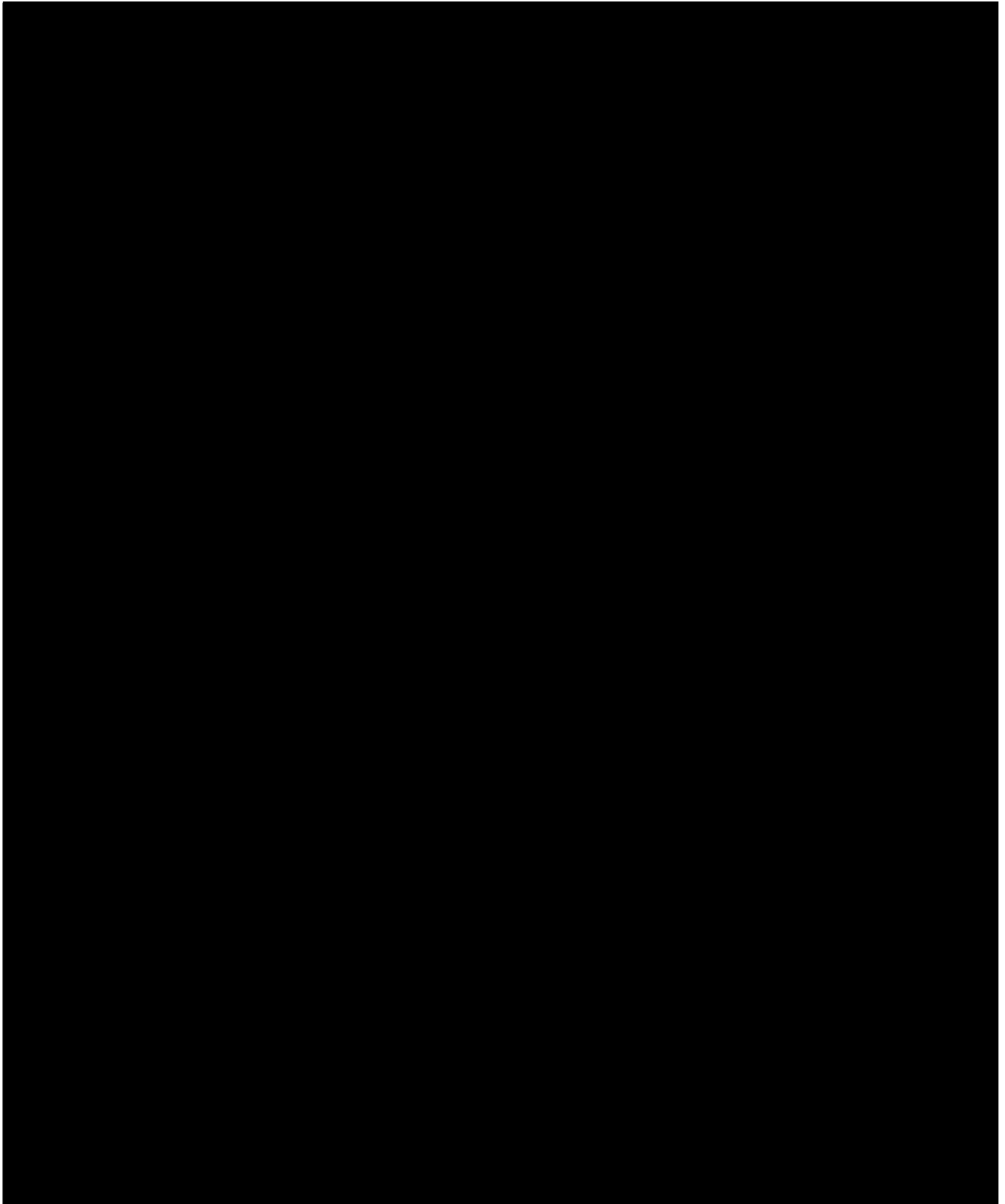
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

		LE

K.   Resolution Process

   ❋   **Step 1: Confirm Match**

Determine if the subject of the hit relates to the individual or organization seeking an immigration benefit. Refer to "Types of Hits" section on how to confirm a match within the Handbook.

For NS hits, an FDNS-IO or a designated officer has the responsibility to analyze the match and confirm whether it relates to the applicant. For Non-NS hits, refer to each Directorate's CARRP operational guidance.

Contact with the record owner may be necessary to assist in the determination. Refer to Step 1A for additional instructions when contacting the record owner.

For NS Hits	
IF	**THEN**
the NS hit is an exact match to the individual seeking an immigration benefit,	Immediately proceed to Step 2: Refer Hit as a NS Hit. The FDNS-IO or designated officer must contact the Terrorist Screening Center (TSC) to confirm the match, per local and component guidelines.
the NS hit is not an exact match but is a potential match to the individual seeking an immigration benefit,	Immediately proceed to Step 2: Refer Hit as a NS Hit. The FDNS-IO or designated officer must confirm the match by contacting the Terrorist Screening Center (TSC), per local and component guidelines.
the NS hit is clearly not a match to the individual seeking an immigration benefit,	Annotate DNR on the ROIT, place the ROIT in the file, and proceed to Step 6: Return to Work Flow.

Criteria to Consider for Determining if a NS TECS Hit Relates to an Applicant:

When determining whether a **TECS hit relates or does not relate** to the individual seeking an immigration benefit, the officer should weigh various personal identifiers. There is no specific number of data elements that must match or not match. However, officers should give more weight to biometric data than biographic data and physical descriptors. If the officer is unable to determine that the TECS hit clearly does not relate to the individual seeking an immigration benefit or the petitioner of an immigration petition, then the officer must refer the hit to FDNS for TSC vetting.

National Background, Identity, and Security Check Operating Procedures

The officer will use the following personal identifiers to determine if the LE subject **clearly does not relate** to the individual seeking an immigration benefit. While this list is non-exhaustive, it contains the most commonly seen personal identifier-related elements.

Biometric Data
- Fingerprint Identification Number (FIN)
    - o Note: In Modernized TECS, officers can see if the subject of the TECS hit has a FIN number. If such information exists, officers can compare the FIN number of the TECS hit to the FIN number of the applicant. In addition, using the FIN numbers of the TECS hit and the applicant, officers will typically be able to review photos or other personal identifier-related elements in CPMS and PCQS.

Biographic Data
- Alien registration number (A-number)
- Name
- Date of birth (DOB)
- Country of birth (COB)
- Country of citizenship (COC)
- Gender
- Immigration history
    - o Example: The individual seeking an immigration benefit has a Form N-400 pending and a search of the immigration history shows the individual's first encounter with USCIS was in 2010. However, when researching the subject in the LE TECS hit, the officer discovers that the subject is currently detained, in removal proceedings and filed a defensive asylum claim. Thus, the removal proceedings and detention may indicate that the individual seeking an immigration benefit and the subject in the LE ECS hit are two different individuals.

Physical Descriptors
- Photographs
    - o Note: If both the individual seeking an immigration benefit and the subject in the TECS hit have A-numbers, officers will typically be able to review their photos in CPMS or PCQS.
- Height
- Weight
- Eye color
- Hair Color
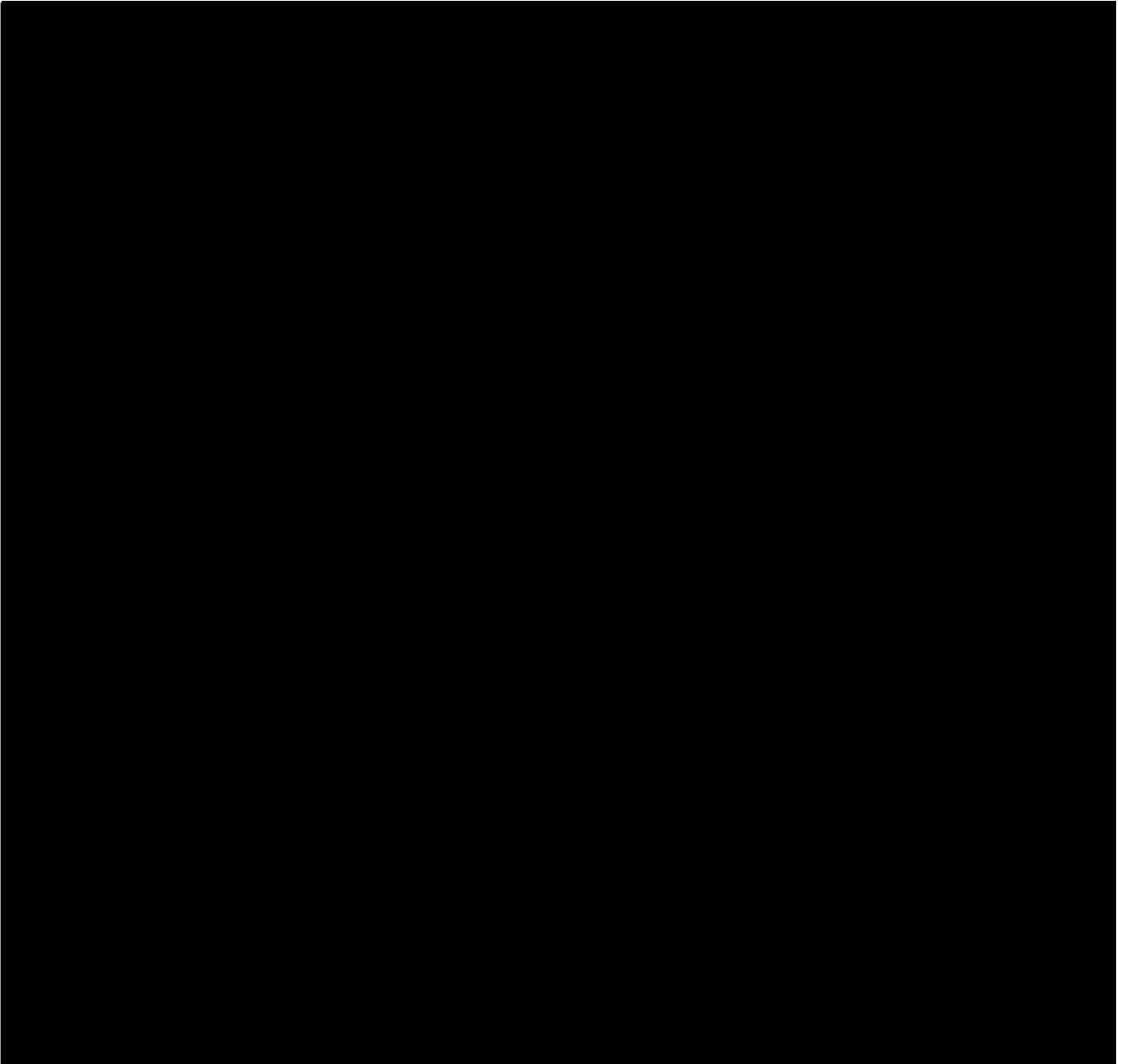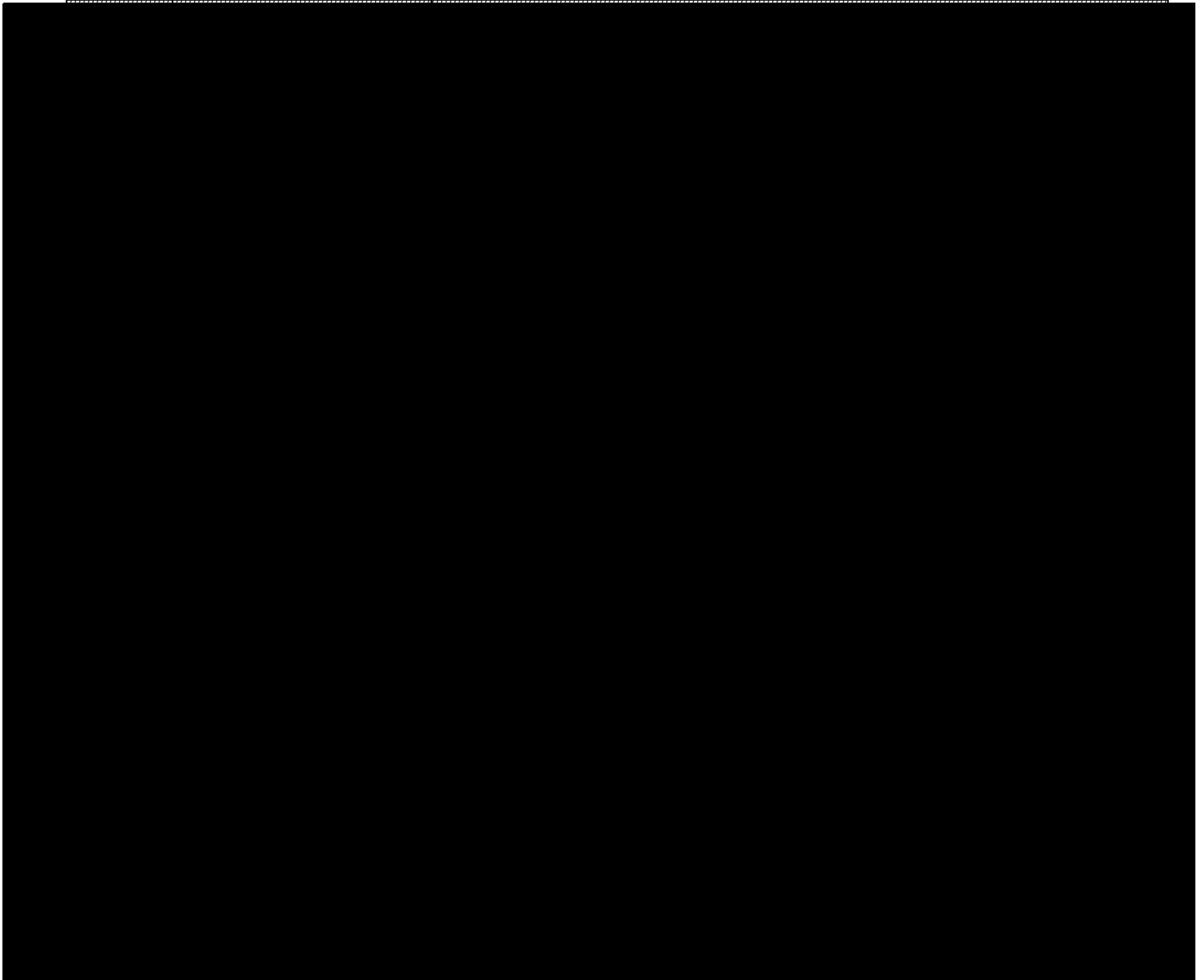
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

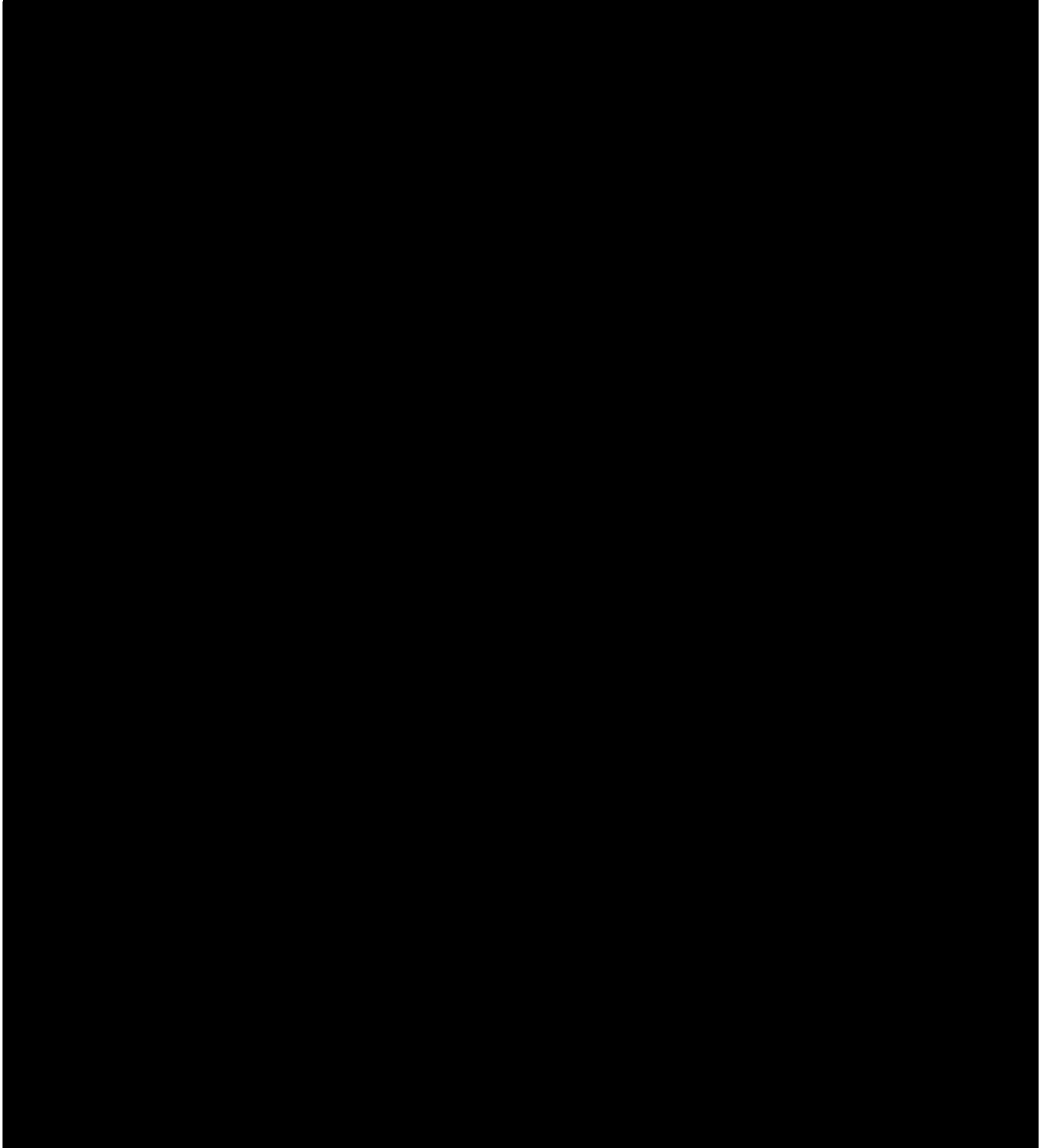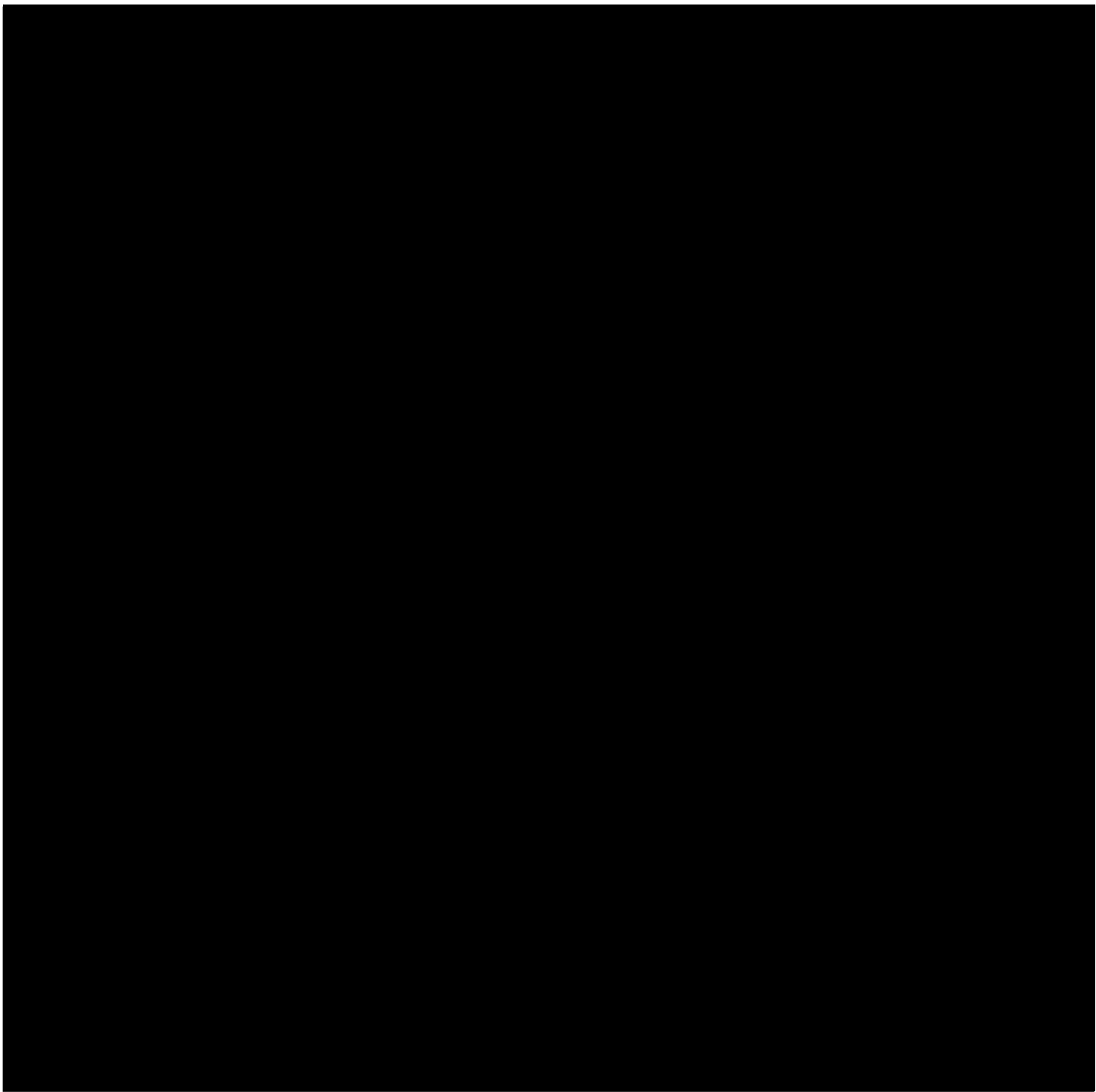**National Background, Identity, and Security Check Operating Procedures**

For All Other Hits	
IF	**THEN**
the subject of the hit does not relate to individual or organization seeking an immigration benefit,	annotate DNR on the ROIT, place the ROIT in the file, and proceed to Step 6: Return to Work Flow.
the subject of the hit relates to individual or organization seeking an immigration benefit,	Proceed to Step 2: Refer Hit.
a determination cannot be made,	Proceed to Step 2: Refer Hit.

❋ **Step 1A: Contact with Record Owner**

Information Sharing

Each office or center may have local policy regarding who has the authority to contact the record owner. Refer to local policy for roles and responsibilities and CARRP Policy for NS Hits.

In all instances when the record owner or another agency is contacted, USCIS officers must be aware of any limitations or restrictions on information sharing and adhere to the above-mentioned disclosure provisions previously referenced in the document. Refer to Section III.G, Confidentiality.

Documenting Contact with Record Owner

Any contact with the record owner must be documented in the file. The documentation may take different formats such as a memorandum to file, annotations on the processing worksheet for the specific form (i.e. NQP sheets), annotations on the TECS hit printout or e-mail correspondence; however, do NOT use Post-It notes or other half-page paper that can accidentally be destroyed or lost to document the contact.

The documentation should clearly indicate the date of the contact, the name of the contact, and pertinent information obtained during the phone call. If the contact was for a case with NS concerns being handled under the CARRP process, then FDNS-DS must be updated with information on the contact.

USCIS Liaison CBP

USCIS has placed a Liaison to CBP at the National Targeting Center, in order to centralize all requests from USCIS to CBP/NTC record owners. For any TECS records created by CBP and/or NTC, please send all record owner requests/deconfliction requests to ▮▮▮▮▮▮▮@uscis.dhs.gov. For specific procedures, please refer to the NTC RFA Procedures on the FDNS Liaison ECN Page.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

• **Step 2: Refer Hit**

---
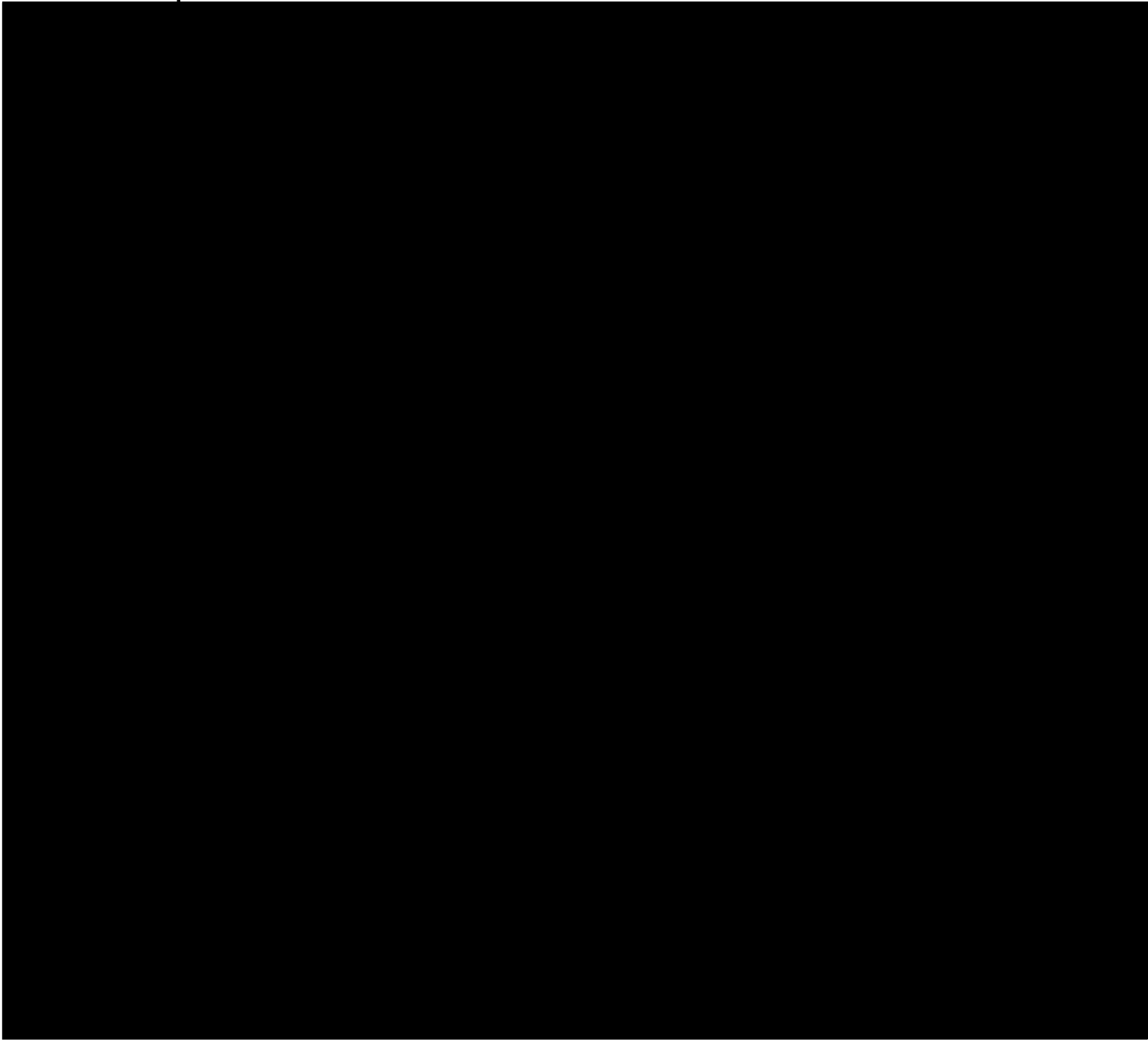
[16] Teleworkers must coordinate with their Supervisors and BCU/FDNS-OPS Supervisors on an estimated delivery date for file.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431603

National Background, Identity, and Security Check Operating Procedures

99

National Background, Identity, and Security Check Operating Procedures

100

DEF-00431605

National Background, Identity, and Security Check Operating Procedures

101

National Background, Identity, and Security Check Operating Procedures

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431607

National Background, Identity, and Security Check Operating Procedures

Below are basic steps which should be taken or considered by the officer when resolving each hit.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP⸺in whole or in part⸺unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

* **Step 4A: Resolution of National Security Concerns**
NS hits are reviewed in accordance with the April 11, 2008, memorandum entitled "Policy for Vetting and Adjudicating Cases with National Security Concerns," and respective operational guidance which implemented the Controlled Application Review and Resolution Program (CARRP) Refer to Section IX, Resolution: National Security Concerns (CARRP) for additional guidance.

• **Step 4B: Resolution of Egregious Public Safety and Other Criminal Cases Egregious**
Public Safety and other criminal cases are reviewed in accordance with PM-602-0050.1, entitled "Updated Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Deportable Aliens", dated June 28, 2018, and the USCIS Memorandum entitled and the USCIS memorandum entitled "Domestic Operations Standard Operating Procedures, Form I-862, Notice to Appear"[17] dated September 8, 2006.

For DACA cases, refer to PM-602-0161, entitled "Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) When Processing a Case Involving Information Submitted by a Deferred Action for Childhood Arrivals (DACA) Requestor in Connection With a DACA Request or a DACA-Related Benefit Request (Past or Pending) or Pursuing Termination of DACA," dated June 28, 2018 on the ECN.

Refer to Resolution: Egregious Public Safety Concerns & Other Criminal Cases, Section X of this Handbook for additional guidance. Refer to component-specific guidance for

---

[17] In January of 2010, the Domestic Operations Directorate was split, as part of an agency-wide reorganization, into the Field Operations and Service Center Operations Directorates. References to Domestic Operations in the titles of memos cited in NaBISCOP should be assumed to apply to employees of both of the new directorates. The memos themselves will state whether they apply to Field Operations or Service Center Operations personnel.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP—in whole or in part—unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

additional information. General procedural information related to the background check process for NTAs will be added to the NaBISCOP upon completion.

- **Step 4C: Resolution of Other Commonly Encountered TECS Hits**

National Targeting Center (NTC)

- Known or Suspected Terrorist ☐ **LE** ☐ ee Step 3A: KST Hits in section V of the handbook. .

- ☐ **LE** ☐

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

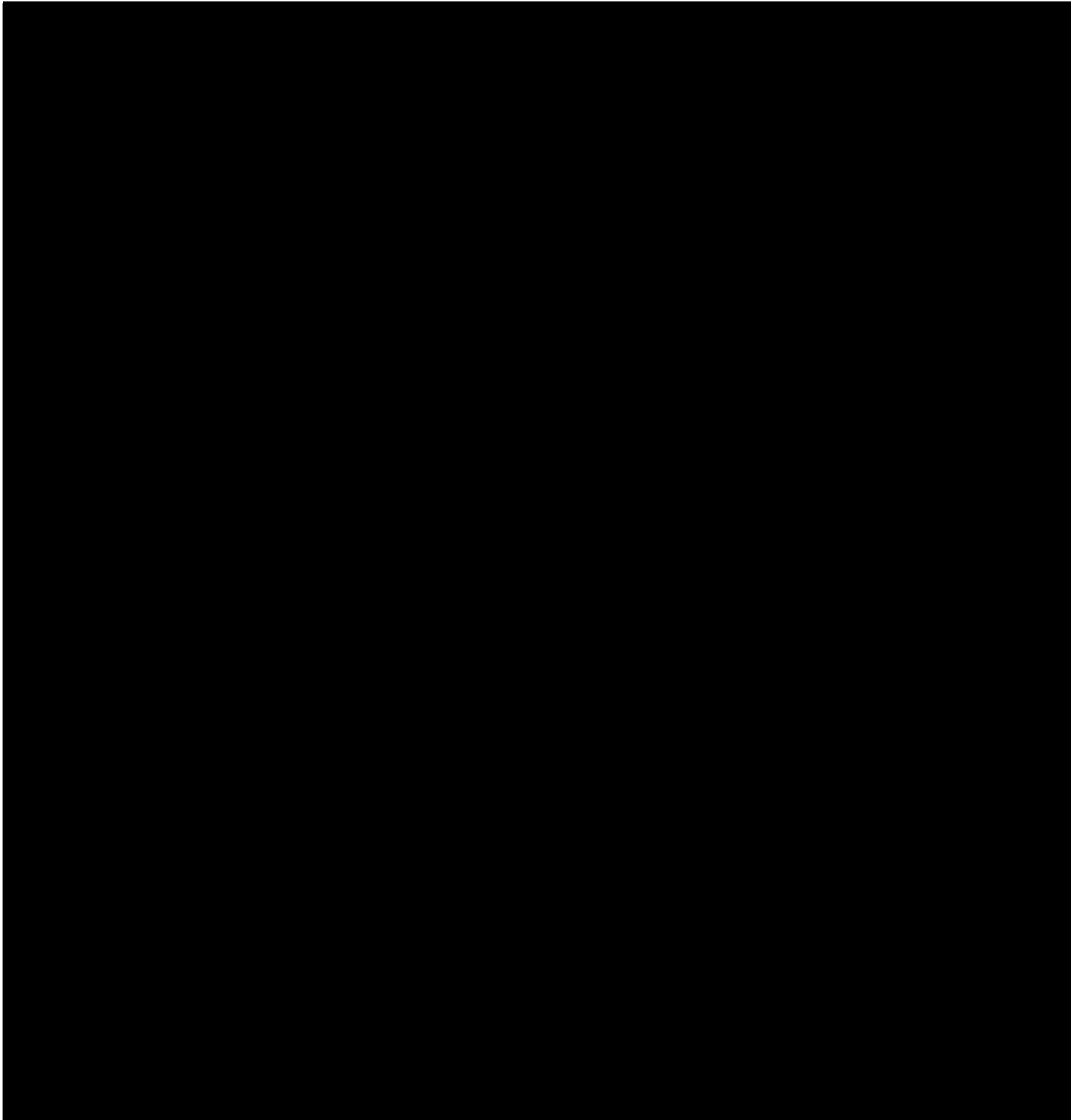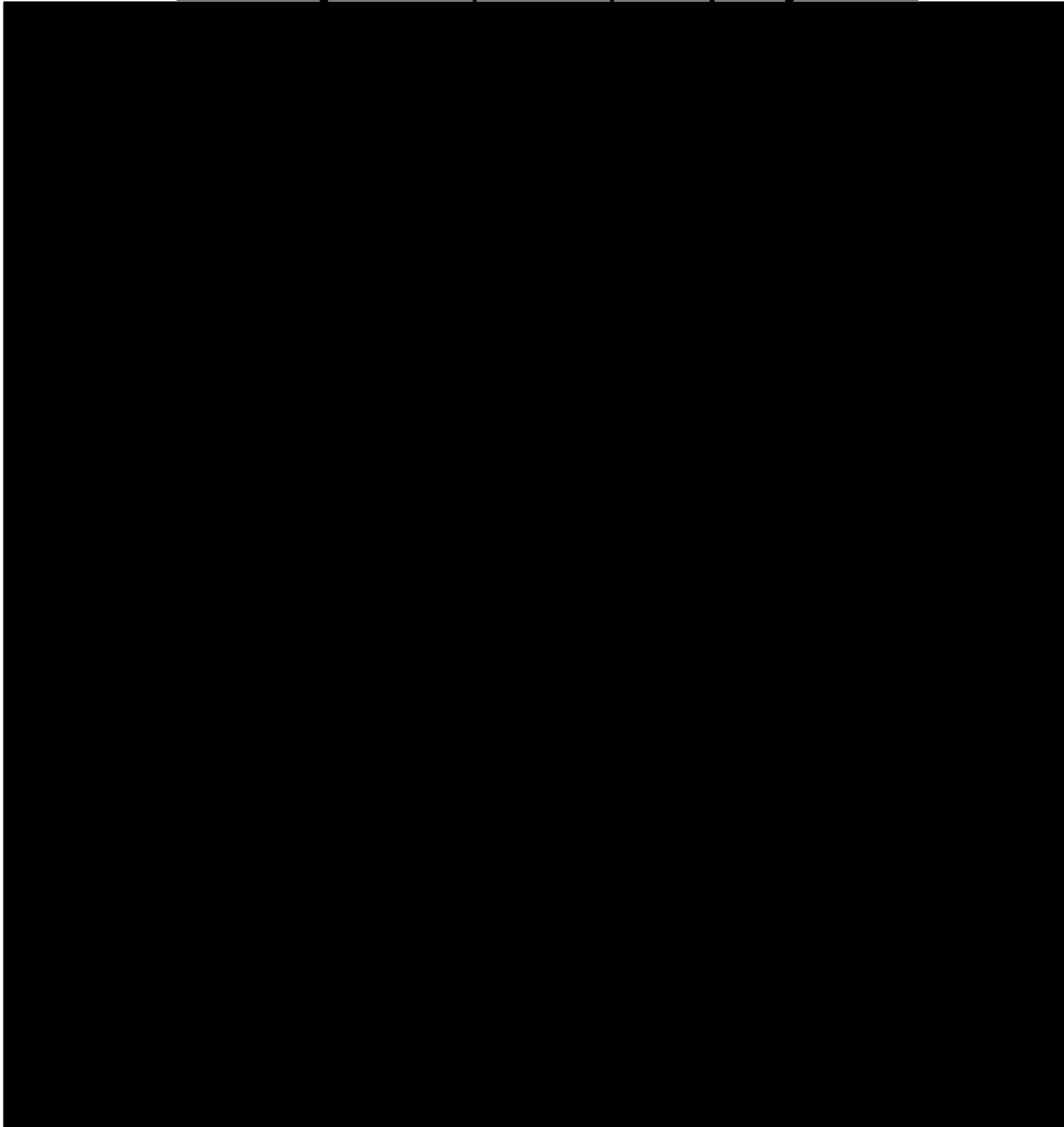**National Background, Identity, and Security Check Operating Procedures**

INTERPOL

- For contact information and guidance on the resolution of INTERPOL-related TECS hits, please refer to the USCIS-FDNS Liaison Branch page on the FDNS ECN[18].
- Officers must use extreme caution when dealing with cases involving asylum, refugees, VAWA, T and U Visas, and the Adam Walsh Act (AWA). Consult with local chain of command and local USCIS counsel. Be mindful of disclosure of Personally Identifiable Information. See Section III(E), Personally Identifiable Information (PII), for more information in the Handbook
- A suggested format to submit your request to INTERPOL can be found on the Liaison Branch ECN page.
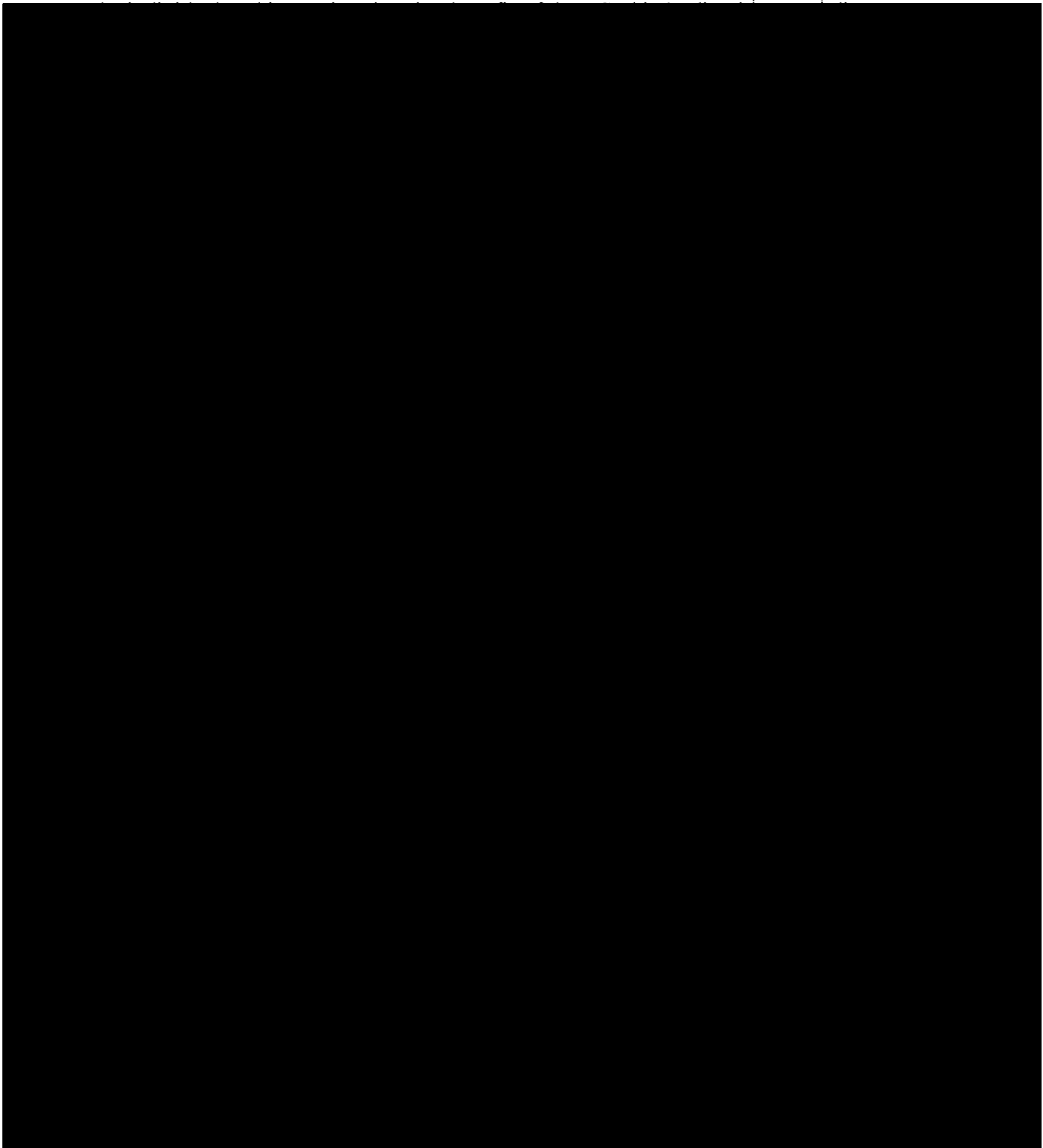
NCIC Outstanding Wants and Warrants
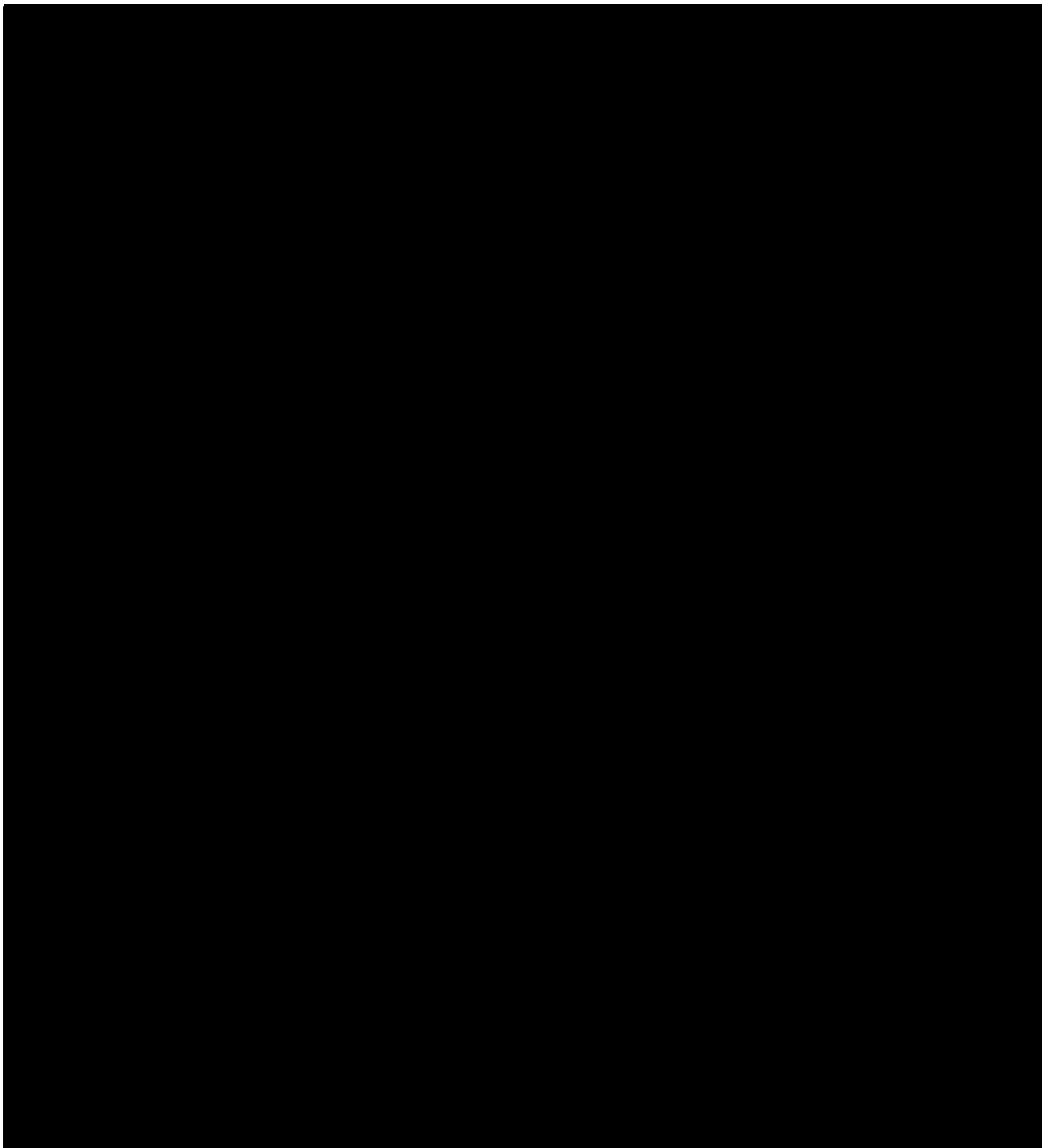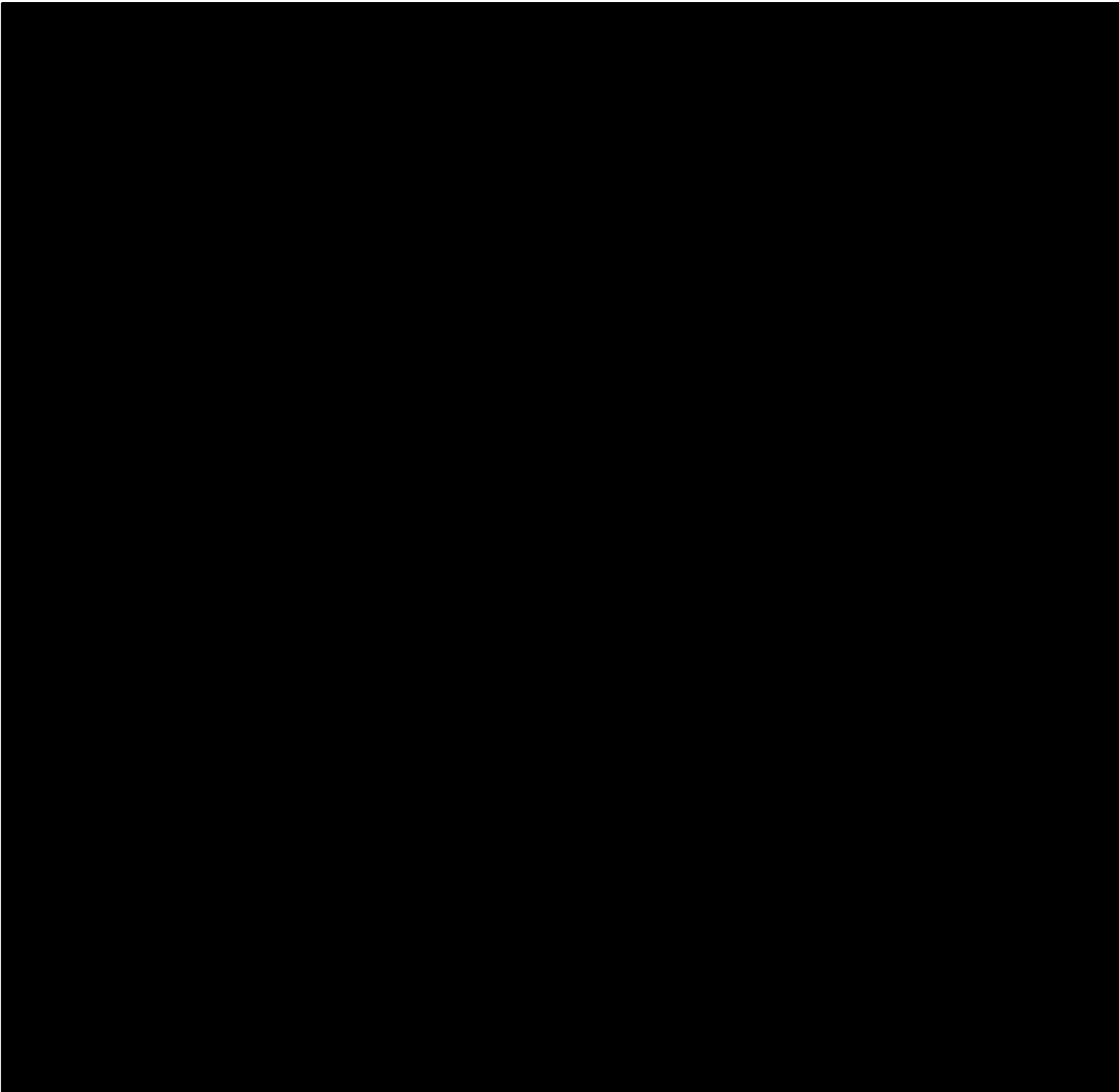
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

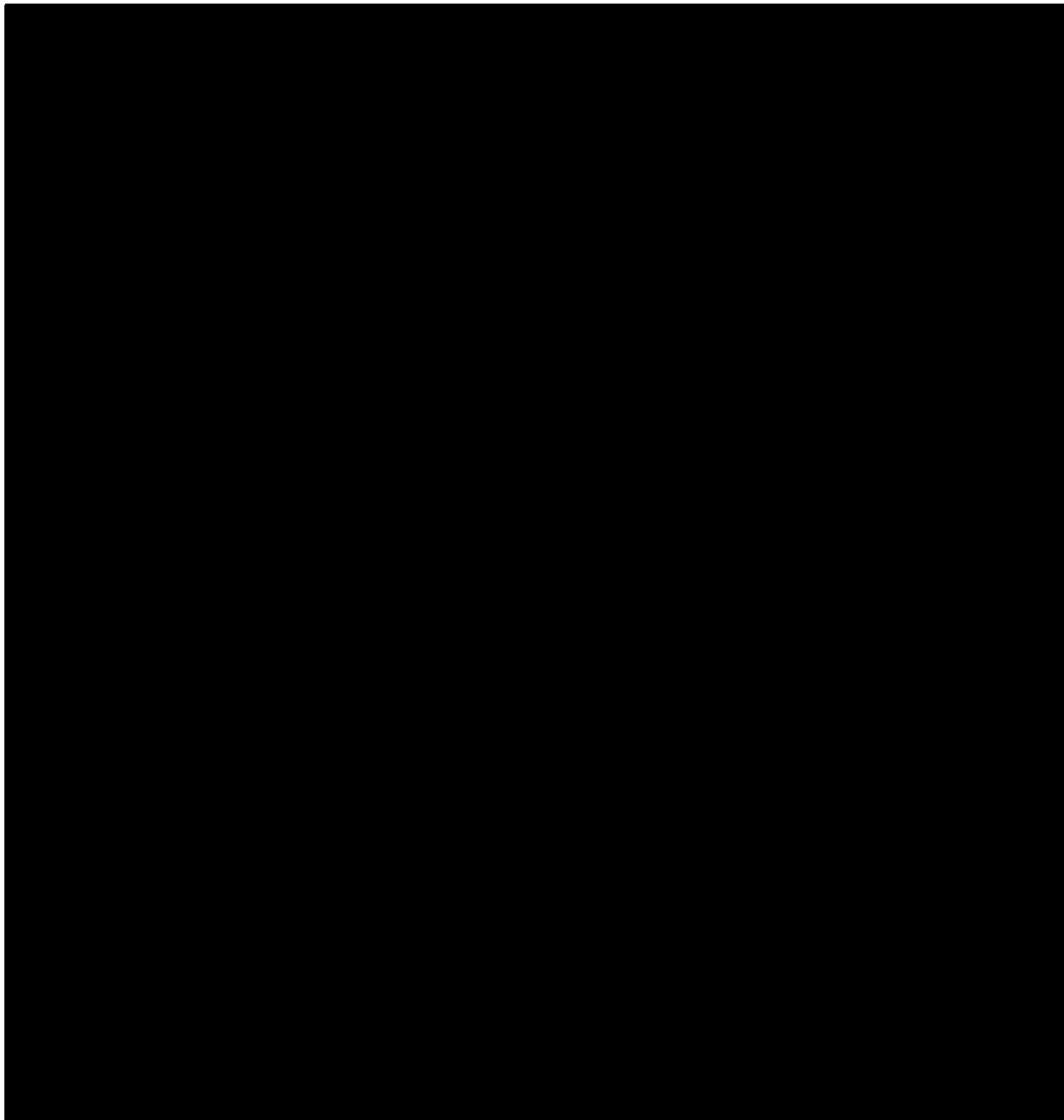# National Background, Identity, and Security Check Operating Procedures

TYPE: AM (Administrative) BODY:

<<<For information only>>>

<<<Subject is not in physical custody>>>

Subject is applying for an immigration benefit. [name], DOB [XXXXX],

WNO/OCA (warrant number).

Subjects last known address as of (date) is: [XXXXXXX]

Thank You, (Officer Name) DHS/USCIS (Officer Phone Number)

OR:

I am an officer with US Citizenship & Immigration Services. The following data is forwarded to you in response to an ncic warrant entered by your ORI. Important: the subject is not in custody. This message is being sent for notification only. If additional action or information is needed, please contact the local USCIS POC(S). the USCIS POC(S) is Officer XXXX (XXX) XXX-XXXX reference A-Number. This notice relates to ⌐ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ‾ ⌐
LE
Offense: Burglary, Name: Doe, John, DOB: 01/01/1990, SSN# XXX-XX-1234, SEX: M, RACE: W. The following info was supplied on the subject's immigration filing - Address: 123 Main Street, Anytown, US 12345, Phone# 123-456-7890. Remarks: none. Sent by: ISO Smith phone# 123-456- 7890. End of message.

SECTION 1367 DISCLOSURE

Please note that information on certain individuals may be subject to to 8 U.S.C. Section 1367 restrictions. 8 U.S.C. Section 1367 applies to any information about a protected individual. This definition includes records or other information that do not specifically identify the individual as an applicant for or beneficiary of T nonimmigrant status, U nonimmigrant status, or relief under VAWA. Section 1367 information[19] covers information relating to applicants for and beneficiaries of the immigration benefits described below:

---

[19] Any information relating to aliens who are seeking or have been approved for nonimmigrant or immigrant status as (1) battered spouses, children, or parents under provisions of the Violence Against Women Act (VAWA); (2) as victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T nonimmigrant status); (3) or as aliens who have suffered substantial physical or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the investigation or prosecution of

108

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP·‑·‑in whole or in part·‑·‑unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431613

National Background, Identity, and Security Check Operating Procedures

1.   Relief under the Violence Against Women Act, including VAWA self-petitioners, as defined by Section 101(a)(51) of the INA. The following is a non-exhaustive list of forms that may be used by VAWA self-petitioners:

    a. Form I-360, Petition for Amerasian, Widow, or Special Immigrant;

    b. Form I-751, Petition to Remove the Conditions of Residence, where a waiver of the joint petition requirement is requested because of battery or extreme cruelty by certain family members.

2.   VAWA Cancellation of Removal (also known as "Suspension of Deportation" prior to 1996) under Section 240A(b)(2) of the INA.

3.   T Nonimmigrant Status, as defined by Section 101(a)(15)(T) of the INA.

    a. Form I-914, Application for T Nonimmigrant Status, and relevant supplements.

4.   U Nonimmigrant Status, as defined by Section INA 101(a)(15)(U) of the INA.

    a. Form I-918, Petition for U Nonimmigrant Status, and relevant supplements.

    b. Form I-929, Petition for Qualifying Family Member of a U-1 Nonimmigrant.

WHEN IN DOUBT, CONTACT AND COORDINATE WITH LOCAL OCC

Clarifying Meaning of "Hit" and "Record" for Resolutions		
Hit(s)	Vs.	No Hits
Relates	Vs.	Does Not Relate (DNR)
Record	Vs.	Entry

-
-

LE

-

---

that activity (U nonimmigrant status). This includes information pertaining to qualifying family members who receive derivative T, U, or VAWA status.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

-

  LE

-

LE

Standalone LE

LE

110
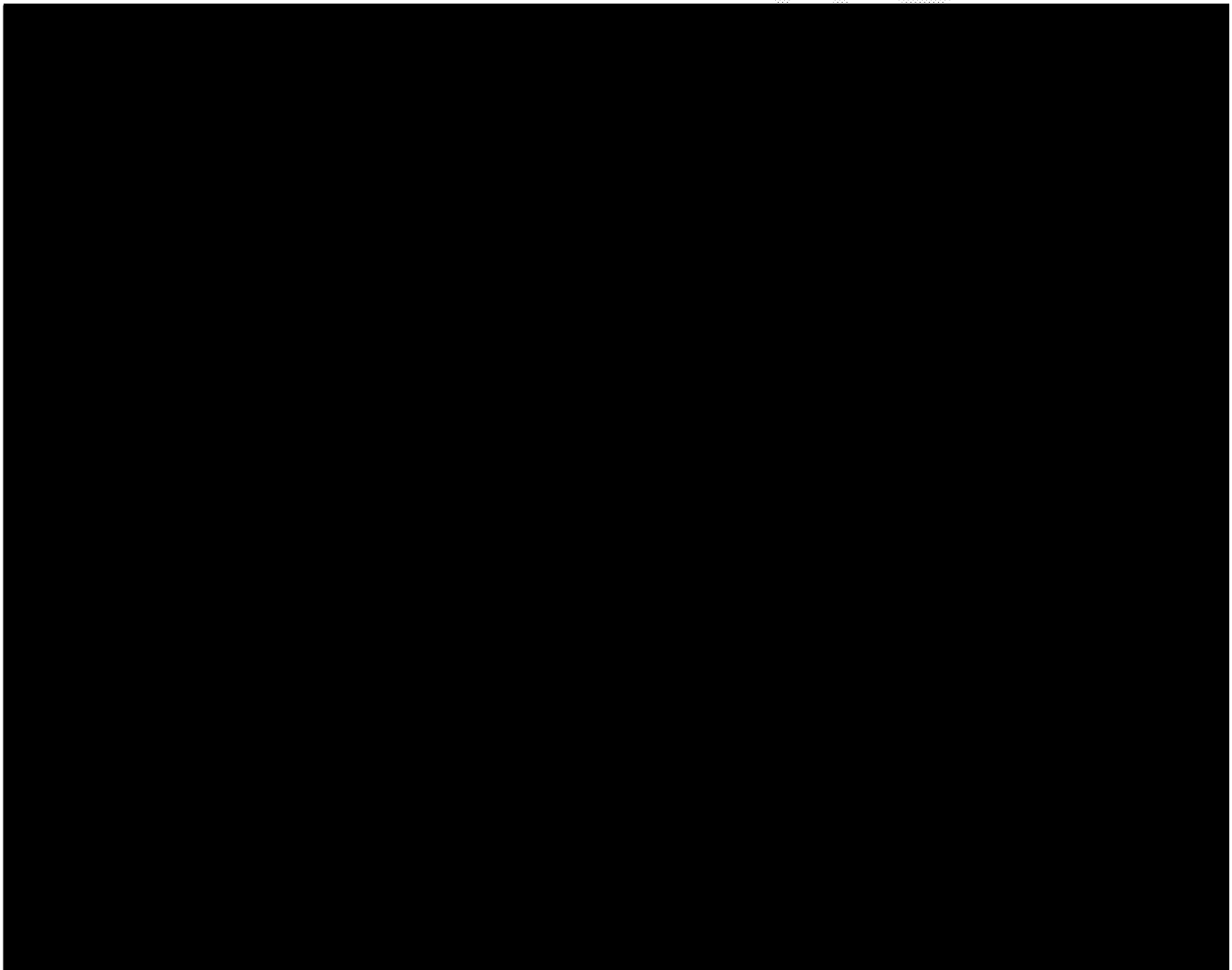FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431615

National Background, Identity, and Security Check Operating Procedures

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431616

National Background, Identity, and Security Check Operating Procedures

For instructions on how to resolve these TECS records, please refer to the paragraph titled, "CBP Encounters" below.

- Please note that Archived Records must be checked in CARRP cases.

CBP Encounters
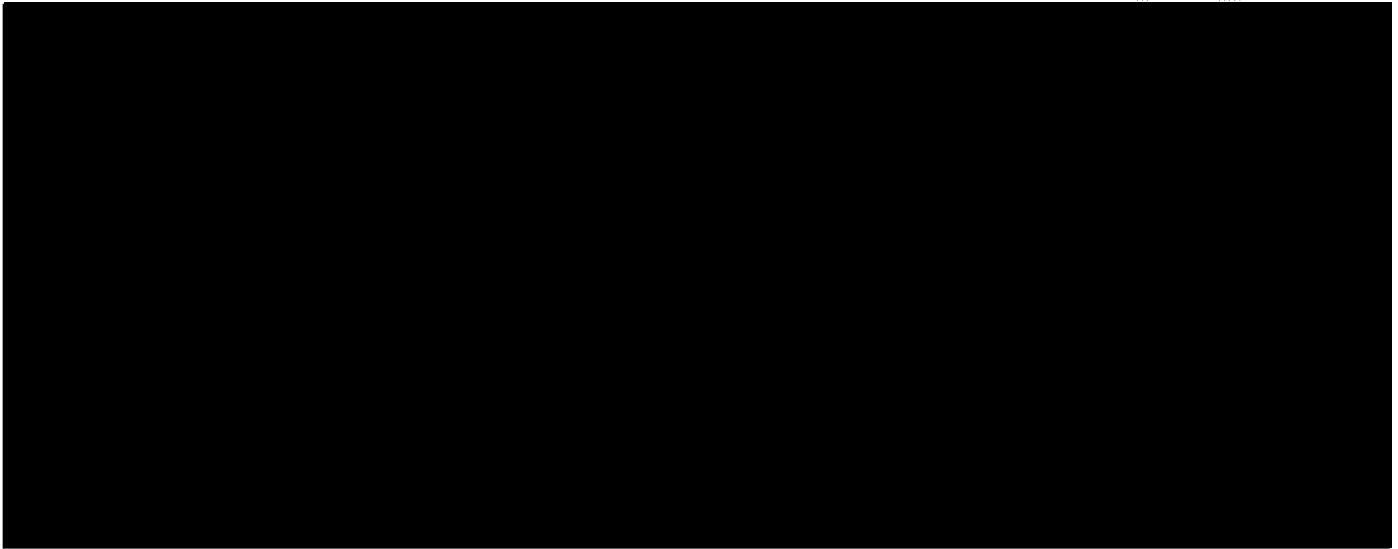
Absconders
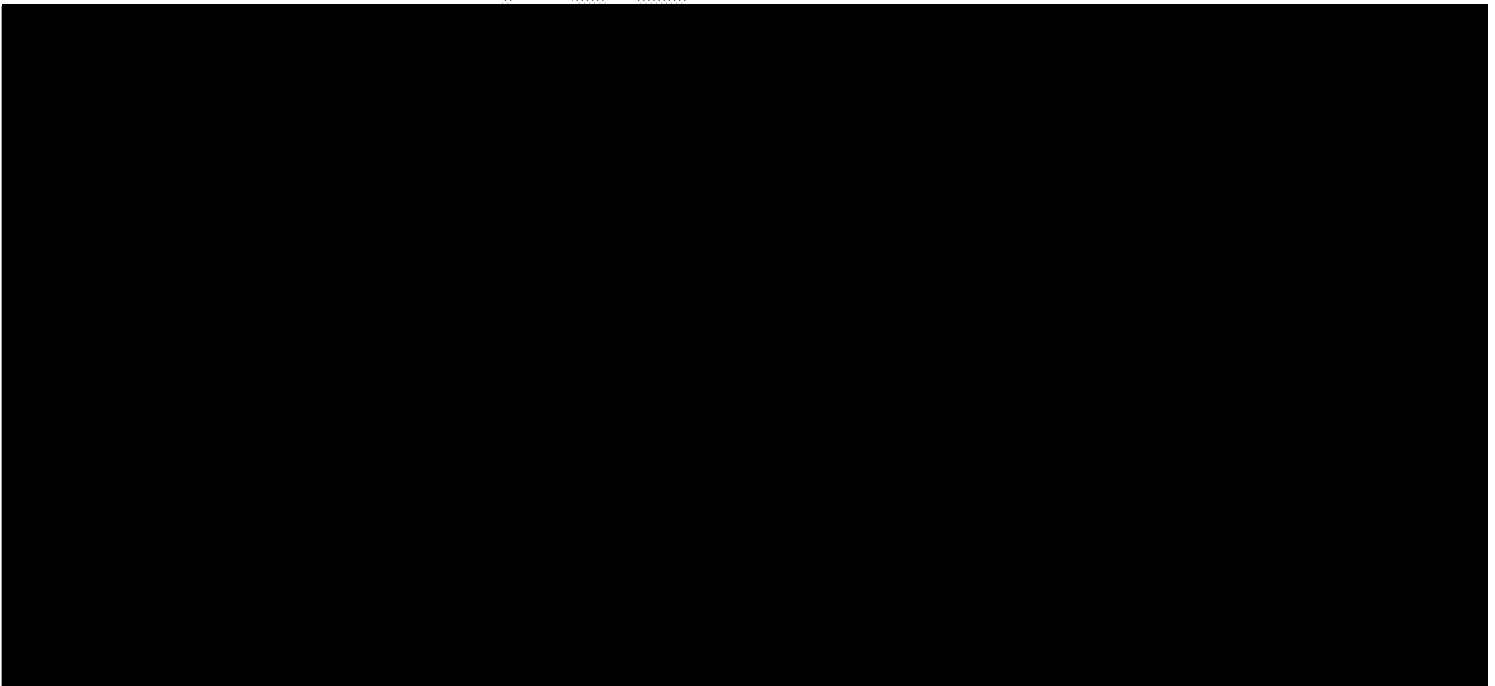
112

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431617

National Background, Identity, and Security Check Operating Procedures

- NBC: Officers should follow the same process to resolve an absconder hit as any other hit type, with the following exception: At the time of resolution and after determining the subject of the record is an active absconder, the officer must capture **LE**

LE

- Service Centers: BCU or FDNS-Operations personnel should follow the same process to resolve an absconder hit as any other hit type, with the following exception: At the time of resolution and after determining the subject of the record is an active absconder, BCU or FDNS-Operations must capture **LE**

LE

LE

National Background, Identity, and Security Check Operating Procedures

[REDACTED]

LE

Consular Lookout and Support System (CLASS) Hits

- **LE**

Refugee Processing Center (RPC) Hits

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Policy Relating to CCD

- See the June 17, 2008, memorandum entitled "Access to the Department of State's Consular Consolidated Database (CCD); Use of CCD Visa Data Safeguards Regarding Disclosure of Visa Data in Immigration Adjudications".
- See the Asylum Division policy memorandum entitled "Disclosure of Consular Affairs Visa Data in Asylum Adjudications," dated January 24, 2008.

LE

- **Step 5: Completion of Resolution Memorandum**

The resolution memorandum is the formal documentation of the reconciliation of a relating hit. This is a mandatory action that must be completed before rendering a final adjudicative decision. Before completing the adjudication, the officer should ensure that each resolution memorandum completely resolves the hit. Each resolution memorandum must be an original (without alterations or correction tape/ink), bearing an original signature.*

* For forms that are digitally ingested and adjudicated in case management services (i.e., in ELIS, C3, GLOBAL or InFACT), electronic resolutions may take the place of a physical file/paper- based resolution memorandum and should include all required resolution content listed below.

For a relating hit, a separate resolution memorandum must be completed for EACH:
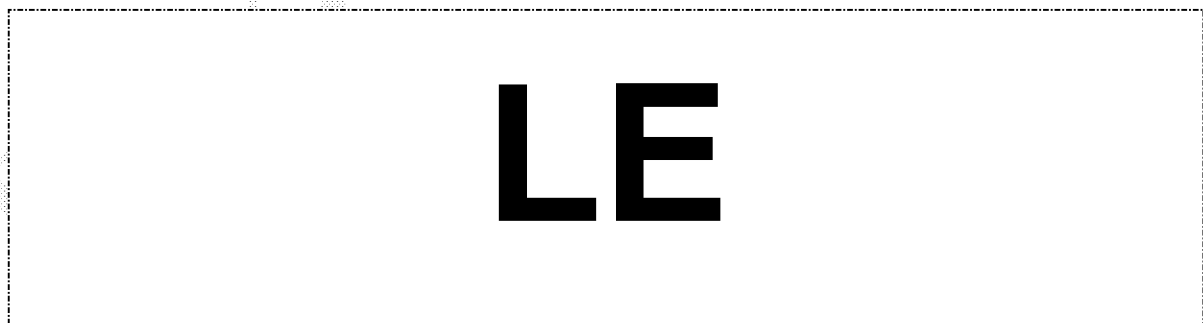
115
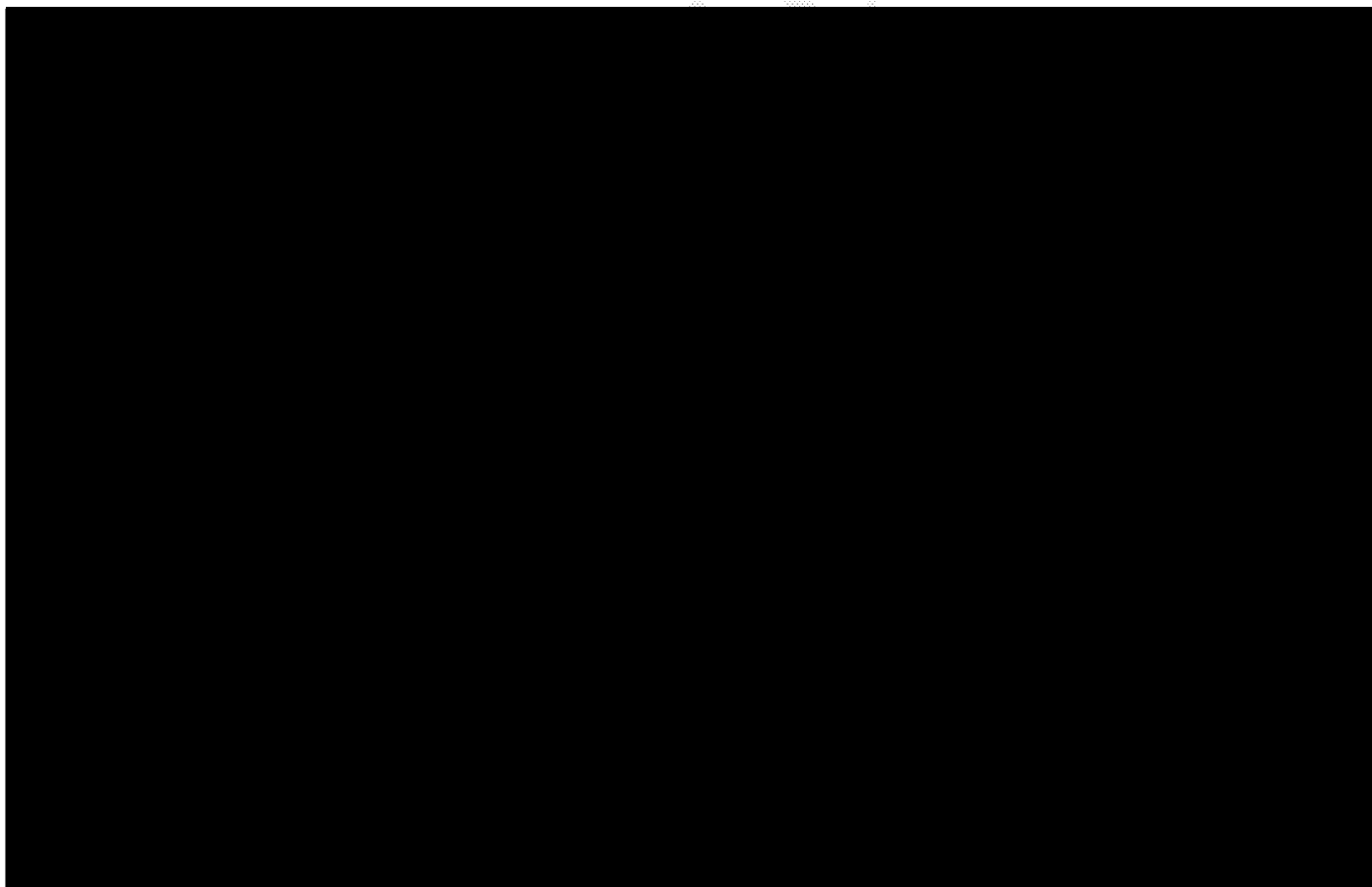
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

- Subject with a relating hit; and
- File containing a relating hit.

Note: If the hit relates to both the petitioner and the beneficiary (for example, a protection order), then only one resolution memorandum needs to be created to cover both subjects.

   a.   Format of Resolution Memorandum

Formats for the resolution memorandum may be developed locally.

Content

- A-Number or Receipt number
- Primary Name and DOB
- The Alias(es) related to the Hit (follow local office procedures)
- Applicant/Requestor/Petitioner/Beneficiary/Derivative/Household Member
- Related TECS and/or NCIC record number(s)
- Summary of the findings
  - Indicate any communication with the record owner (For example, date/name of record owner, results of conversation/e-mail, etc). If unsuccessful, document any efforts to contact the record owner, and articulate those efforts and any supervisory review or chain of command review for final resolution.
  - Document the results of any system checks that may have been accomplished. For example, SEVIS, EARM, ADIS, etc. (if required).
  - Summarize how or if the TECS record may affect eligibility of the immigration benefit sought (pursuant to local office procedures).
- Completion date of resolution memorandum
- Name or identifying number of authorized personnel who resolved the hit(s)
- Signature of supervisor or authorized personnel: an electronic signature or signature stamp may be used by the supervisor or authorized officer

The resolution memorandum should NOT include:

- Abbreviations (e.g., EARM codes) without definitions (citations such as from 8 CFR or the Act are acceptable);
- Subjective comments, personal opinions; or
- Conclusive statement or recommendations of adjudicative actions:
  - "The person is inadmissible." However, the person "appears" to be inadmissible would be an appropriate statement.
  - "This application is deniable." However, "This applicant appears ineligible based on…"

National Background, Identity, and Security Check Operating Procedures

Note: Various formats have been used to report and resolve NS concerns as USCIS policy and procedures evolve. Officers may find any of the following documentation in a file to record the existence of an NS concern:

- Significant Incident Report (SIR);
- National Security Notification (NSN);
- Case Resolution Record (CRR);
- National Security Record (NSR);
- Background Check Assessment (BCA);
- Background Check and Adjudicative Assessment (BCAA);
- Memorandum to the File;
- CARRP Worksheets; or
- Statement of Findings (SOF).

b.   Who May Complete a Resolution Memorandum

For cases other than national security which are processed by designated officers in accordance with CARRP, the following officers may complete resolution memoranda:

- **Service Centers**: USCIS officers may complete resolution memoranda. Each memorandum requires concurrence from a supervisor or a certified officer. Service centers may develop a local certification process.
- **National Benefits Center**: USCIS officers may complete resolution memoranda. Each memorandum requires concurrence from a supervisor or a certified officer, as per local policy.
- **Field Office**: USCIS officers may complete resolution memoranda. Each memorandum requires supervisory concurrence.
- **Overseas Office**: In USCIS offices outside of the United States where there are two officers, including an immigration services officer (ISO) and a field office director (FOD), the memoranda will require supervisory concurrence. In offices where there is only an FOD, no supervisory concurrence is required.

c.   Validity of Resolution Memorandum

Any USCIS office may accept a resolution memorandum completed by an authorized officer at any USCIS center or field office, as valid evidence that a TECS hit has been resolved.

TECS query results are valid for 180 calendar days, *unless* the form type in question requires a JIT check. Refer to .Part I. of this Section,   "Validity of Results from TECS Queries," for additional details.

<u>National Background, Identity, and Security Check Operating Procedures</u>

If a resolution memorandum is not completed within 180 calendar days after the TECS query is conducted at the time of adjudication, USCIS personnel MUST:

- Re-query all name and DOB variations.
- Record the results of those queries on the ROIT.
- If the query results in a new hit, the personnel should proceed to Step 1, Confirm Match, as instructed above.
- If the query results in the same TECS record previously resolved by the resolution memorandum, a USCIS officer may revalidate the expired resolution memorandum. See section (d), "Revalidation of Expired Resolution Memorandum," directly below.

If, after completion of a Resolution Memorandum, a new alias is discovered, USCIS personnel must query that alias and record the results of that query on the ROIT. If the query results in a new hit, personnel should vet the hit and refer any relating hit to the authorized officer, as instructed above. If the query results in the same TECS record previously resolved, USCIS personnel may consider the hit to be resolved and revalidate the expired resolution memorandum.

d.   <u>Revalidation of Expired Resolution Memorandum</u>

To revalidate a resolution memorandum, the officer must annotate the resolution memorandum with:

- Initials or identifying number of the officer;
- New date of TECS queries; and
- The phrase "No new information found".

e.   <u>Service Center Archive Policy</u>

- Service centers are required to physically and/or electronically archive each resolution memorandum completed.
- NBC is not required to archive each resolution memorandum completed, per local policy.
- Go to Step 6: Return to Work Flow.

Step 6: Return to Work Flow
After completing a resolution memorandum, the application/petition should be returned to its appropriate place in the normal workflow. Upon resolution of a referred case, the officer can route the case directly for adjudication according to local procedure.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

Go to the next step, Record of Proceeding (ROP).

❖ **Record of Proceeding (ROP)**

Resolution memorandums, ROITs, and screen prints must be placed on the non-record side of the file (right side).

1. Transferring the file within DHS?
   If the application/petition will be transferred to another office within DHS, the resolution memorandum(s), ROIT(s), and screen prints should remain in the file.

2. File unavailable?
   Attach the documents to the loose application/petition, create a T-file for future consolidation with supervisory concurrence, and route them to the A-file pertaining to that application/petition.

3. Subject doesn't have an A-file or Receipt file?
   Either electronically archive the documents or retain them in a work folder and store in an area designated for TECS resolutions.

4. Sending the petition to the National Visa Center (NVC) or Kentucky Consular Center (KCC)?
   Do NOT forward any documentation specifically disclosing information from TECS or screen prints to the NVC or KCC. Remove and shred screen prints at the time of final adjudication. However, the resolution memorandum(s) and ROIT(s) should remain with the copy of the petition and have the appropriate markings.

5. Hit does not relate?
   If you have printed hits that Do Not Relate (DNR) to the subject, shred them or otherwise dispose of them according to USCIS procedures for disposing of sensitive information. DO NOT place them in the file.

   For NCIC screen prints which contain portions of two separate hits, one which relates and one which does not, redact the personal identifying information with a thick marker for the subject that does not relate. Identifying information includes, but is not limited to the following: names, aliases, SSNs, A-Numbers, and FBI numbers.

6. Hit relates to the petitioner?
   Place the TECS printouts for the petitioner in the appropriate applicant or beneficiary file. In those few instances when the application/petition will not be matched to the A-file, the documents should remain with the application/petition, placed on top of the ROP.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

ROIT should be directly under the resolution memorandum. Supporting screenshots and documents such as TECS, NCIC, and [LE] hould be placed directly under the ROIT. These documents must be placed on the non-record side (right side).

The order of the ROIT, resolution memorandum, and supporting documents supersedes all other instructions; however, the combined TECS materials will continue to be filed according to the applicable ROP policies such as N-400 (NQP), I-485, I-129s, Asylum, etc. Additional guidance for ROP may be found in the Records Policy Manual.

Remember: All TECS screen prints must be labeled in accordance with the USCIS CBP MOU on TECS.

L.   Other Procedures Relating to TECS Queries

1.   Discretionary Authority

USCIS officers are encouraged to conduct additional TECS queries when they believe the queries would result in more complete and accurate information or would yield information that may improve the quality of the adjudication. Officers should follow local policy for such cases. Below are some examples to illustrate the different queries and search criteria that may be warranted if not already required per policy:

LE

---
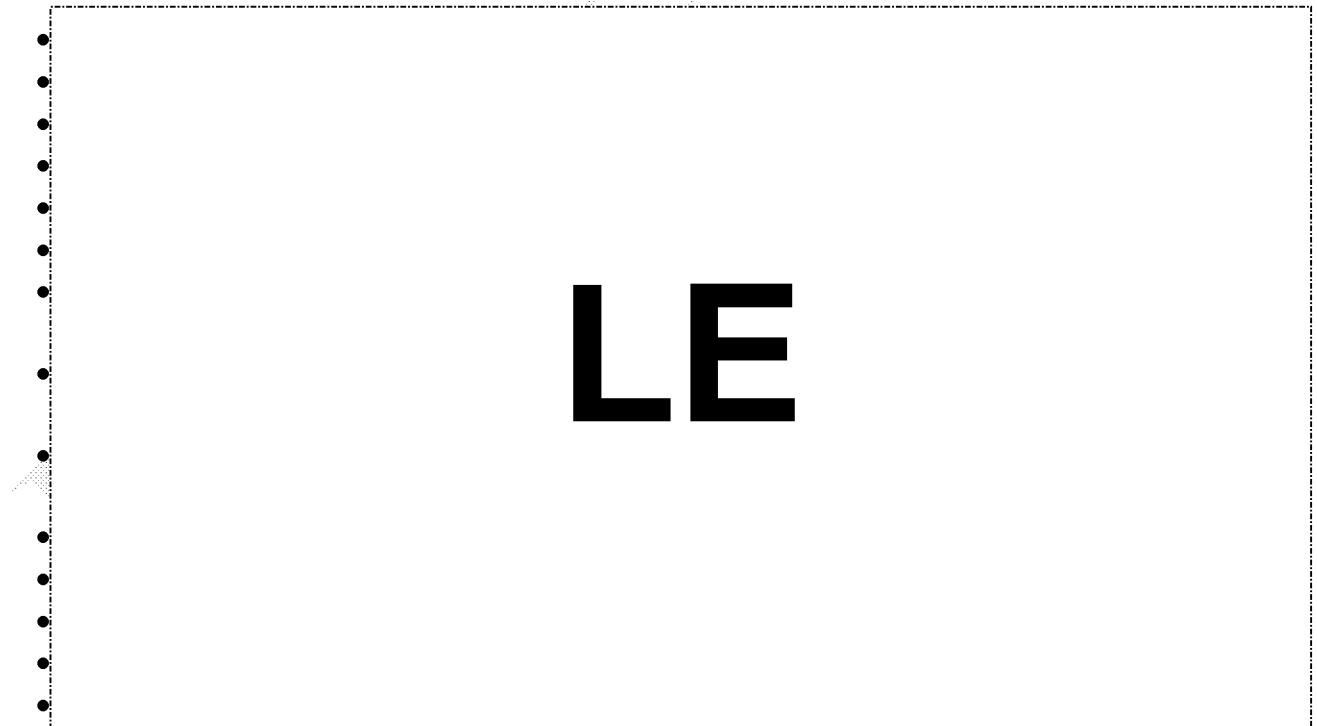
[22] CARRP designated officers must query [LE] s for CARRP Cases.

T20

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

-
-
-
-

LE

-
-

-
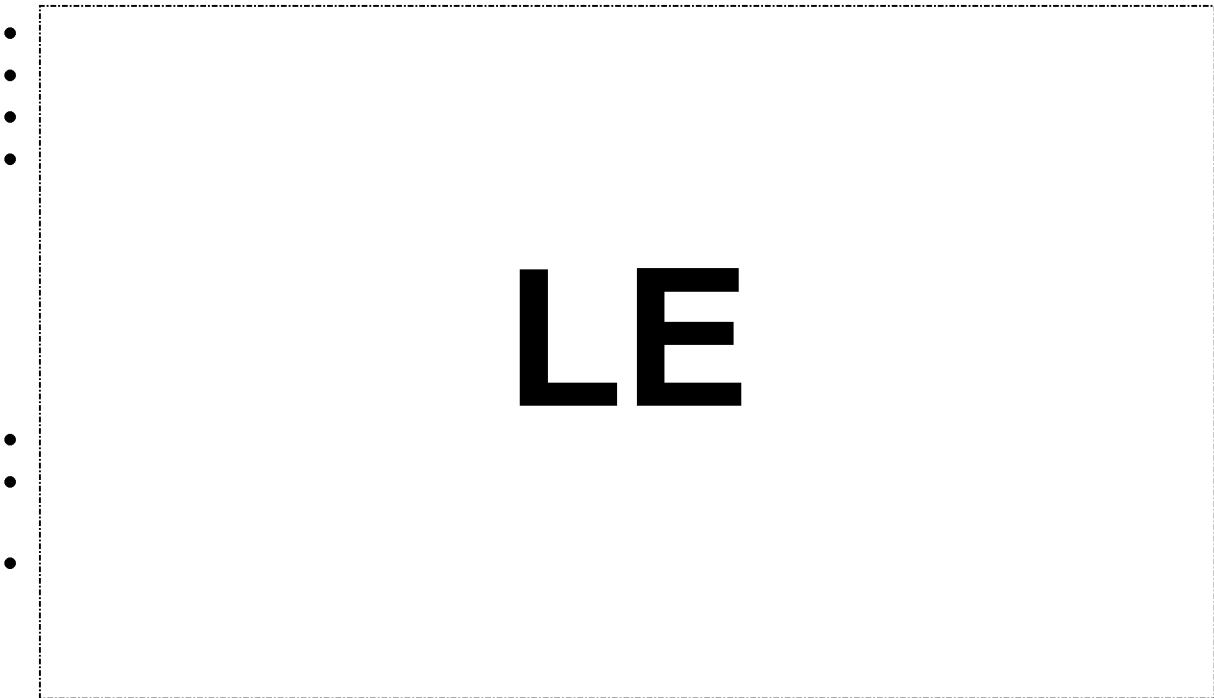
2.   Information Sharing Best Practice

The best way to share information with another agency that is a TECS user is to provide only the
LE Since that agency will then be directly accessing the information, the Third
Agency Rule will not apply.

3.   Adam Walsh Act

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431626

National Background, Identity, and Security Check Operating Procedures

M.   **LE**   Hits

LE

N.   Best Practices: TECS Queries – Query Defaults

1.   Update Self User Profile

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

LE

123
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431628

National Background, Identity, and Security Check Operating Procedures

3.   TECS Usage

Data in TECS is "For Official Use Only (FOUO)," and access is granted on a need-to-know basis for official use only. According to DHS Management Directive 11042.1, there are numerous additional caveats (i.e. "Law Enforcement Sensitive") used by various agencies to identify unclassified information as "Sensitive but Unclassified (For Official Use

Only)." Regardless of the caveat used for identification, the reason for designation does not change.

All TECS users must be certified through an online security certification test and must be re-certified every two years. Abuse or misuse of TECS could result in loss of access, termination of employment, and/or criminal prosecution.

Mandatory TECS usage requirements:

- Never leave a terminal unattended while logged into TECS.
- Never leave TECS materials unattended in unprotected places.
- Never store TECS information or records on the hard drive.
- Ensure all TECS printouts are secured or destroyed.
- Never confirm or deny the existence of a TECS record to the public or unauthorized users.
- Only use TECS to perform official duties required by your job. Use of TECS for personal reasons is strictly prohibited. Browsing is not permitted. Do not query friends, family members, well-known personalities (unless in the course of official use) or yourself; do not access TECS simply out of curiosity.

4.   Record Level & Disclosure

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP in whole or in part unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431629

<u>**National Background, Identity, and Security Check Operating Procedures**</u>

> # LE

5.   TECS Equipment and Technical Assistance

Guidelines regarding TECS equipment and technical assistance include:

<u>TECS Mod/Portal</u>

> # LE

125
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431630

National Background, Identity, and Security Check Operating Procedures

LE

- For help concerning TECS access issues, contact the local system control officer (SCO).
- For technical help concerning TECS issues, contact the TECS Help Desk at (703) 921‑ ▇▇▇▇
- All workstations' Virtual Terminal Access Module (VTAM) identification (ID) addresses and Internet Protocol (IP) addresses will be statically assigned and coordinated with TECS personnel prior to installation or changes.

Questions about the technical aspects of TECS should be referred to CBP as the owner of the system. Refer all inquiries about TECS system to:

<div align="center">

U.S. Customs and Border Protection
Office of Regulations and Rulings
Regulations and Disclosure Law Branch
1300 Pennsylvania Avenue, N.W. Washington, DC 20229

126
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

</div>

DEF-00431631

National Background, Identity, and Security Check Operating Procedures

6.   Third Agency Rule in the USCIS-CBP MOU

The 2006 Memorandum of Understanding between USCIS and CBP on the use of TECS, sets out a system specific Third Agency Rule. This MOU provision uses a different definition of "agency" than is used under the Privacy Act and only applies to TECS records. Under the MOU, information from TECS could not be shared by USCIS with other DHS components (e.g. ICE,

Transportation Security Administration (TSA), U.S. Coast Guard) without CBP's permission. Nonetheless, with regard to sharing information within DHS, the MOU between

CBP and USCIS has now been superseded by the February 1, 2007, memorandum of Secretary Chertoff, establishing a "one agency" policy within DHS. In accordance with that policy, USCIS may share TECS information with other components of DHS without prior permission from CBP.

7.   Privacy Act and the Third Agency Rule

Information on a USC or an LPR that can be released under the Privacy Act must also be vetted under the Third Agency Rule prior to release.

O.   CBP Vetting

LE

LE Several USCIS field office locations have begun utilizing this new service. As USCIS increases implementation of CBP Vetting, more guidance will be issued by USCIS, including updates to this document, as appropriate.

For any administrative issues, please reach out to either, Laura Holder or Dan Williams, the USCIS CBP Vetting Administrators

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.
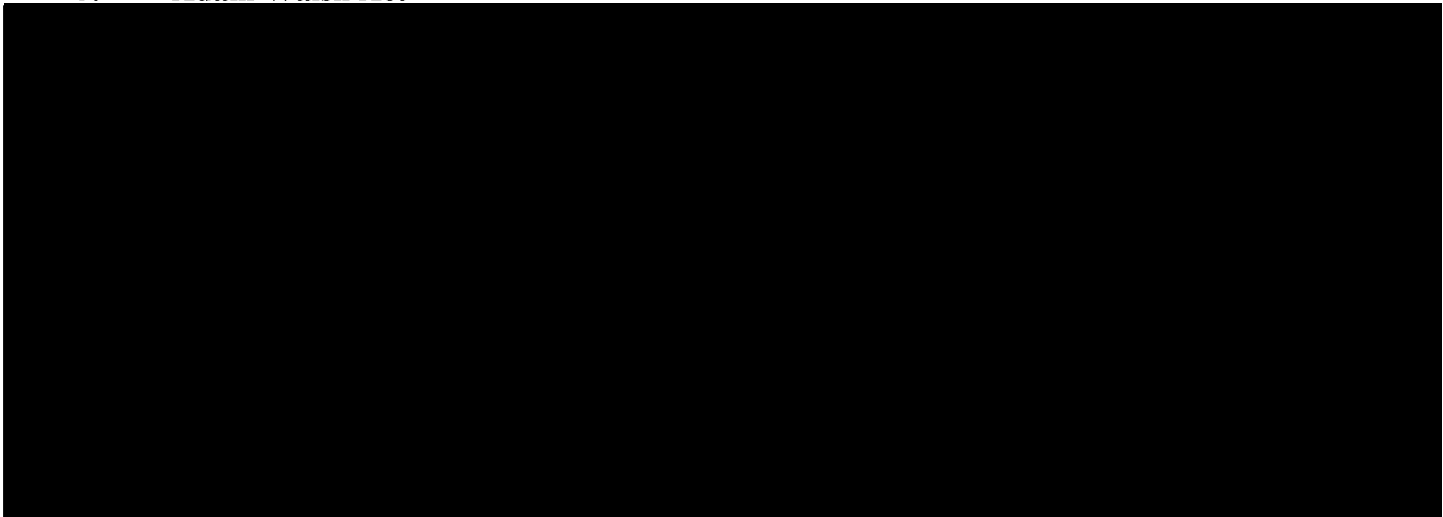
National Background, Identity, and Security Check Operating Procedures

VI.   Security Check: FBI Name Check

A.   FBI Name Check

The FBI's National Name Check Program (NNCP) researches and disseminates, in accordance with applicable laws, orders, rules and policy, information contained in the FBI's files in response to FBI Name Check requests. The FBI Name Check searches the FBI's Automated Case Support system and Sentinel, which contain personnel, administrative, applicant, intelligence, and criminal files that have been compiled for law enforcement purposes. NNCP staff review and analyze potential identifiable documents to determine whether a specific individual has been the subject of or been mentioned in any FBI investigation(s), and if so, whether relevant information, if any, may be disseminated to the requesting agency. The records are searched to determine whether an individual has a record that might have an impact on the individual's eligibility for the benefit sought. In most instances, applicable information found in the FBI's Name Check search will be returned as Letterhead Memorandums (LHMs) or Reports.

LE

128

National Background, Identity, and Security Check Operating Procedures

B.   Who Requires FBI Name Checks

The table below lists those forms and individuals requiring FBI Name Checks under current agency guidance. Individuals requiring FBI Name Checks are designated with an "x." If a form is not included in this table, then an FBI Name Check should not be initiated.

Please note that name checks may be requested by other agencies and its results may be included in the A-file

FBI Name Check Requirements by Form Type and Individual						
Form	**Individual Requiring FBI Name Check (designated with "x")**					**Special Instructions**
	Applicant	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-192	x					
I-485	x					FBI Name Check not required on an individual who is more than 80 years and one day old.
I-589	x			x		
I-590	x			x	x	**LE**
I-601	x					Except when filed Overseas. See Section IV, Part C for more information on applications filed overseas.
I-601A	x					Except when filed Overseas. See Section IV, Part C for more information on applications filed overseas.
I-687	x					
I-698	x					

129

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

FBI Name Check Requirements by Form Type and Individual						
Form	**Individual Requiring FBI Name Check** (designated with "x")					**Special Instructions**
	Applicant	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-730			x			When the beneficiary is in the U.S.
I-881	x					
N-400	x					

Note: Pursuant to the Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance issued on December 26, 2018, FBI Name Checks also are required for NTA issuance purposes, in some cases for applicants/requestors not previously required to undergo a Name Check. USCIS must issue an NTA after denying applications/requests or claims as described in "Updated Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Deportable Aliens," dated June 28, 2018, and the USCIS memorandum entitled "Domestic Operations Standard Operating Procedures, Form I-862, Notice to Appear" [23] dated September 8, 2006.

For DACA cases, refer to PM-602-0161, entitled "Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) When Processing a Case Involving Information Submitted by a Deferred Action for Childhood Arrivals (DACA) Requestor in Connection With a DACA Request or a DACA-Related Benefit Request (Past or Pending) or Pursuing Termination of DACA," dated June 28, 2018.

For additional information regarding FBI Name Check requirements specific to NTA issuance, refer to Section XII, Security Checks Required for Issuance of Form I-862 – Notice to Appear and Form I-863 – Notice of Referral to an Immigration Judge in the handbook.

C.   FBI Name Check Procedures
These procedures apply to forms that require FBI Name Checks under current agency guidance; see Section VI, Part B: Who Requires FBI Name Checks for a complete list. Users should query a response to a name check in the name check database by using the Alien Registration Number

---

[23] In January of 2010, the Domestic Operations Directorate was split, as part of an agency-wide reorganization, into the Field Operations and Service Center Operations Directorates. References to Domestic Operations in the titles of memos cited in NaBISCOP should be assumed to apply to employees of both of the new directorates. The memos themselves will state whether they apply to Field Operations or Service Center Operations personnel.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

(A-Number), Tracking ID, or Receipt Number of the applicant. When querying the system by name, it is recommended to broaden the search by changing the '

LE

LE

FBI Name Checks that return to USCIS with

LE

LE are not considered an error or an alias, and do not require a manual FBI Name Check to be completed with the proper spacing, such as

LE

"FBI Name Check Search Criteria"

Name Check - Search

LE

131

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431636

National Background, Identity, and Security Check Operating Procedures

132

National Background, Identity, and Security Check Operating Procedures

133

National Background, Identity, and Security Check Operating Procedures

Name Check - Search

LE

134

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

D.   Types of Results from FBI Name Checks

The results of the FBI Name Check are based on a name and birth year query in the FBI's Automated Case System (ACS). This security check is not biometric.

"Example of the FBI Name Check Response"

The table below shows the various response codes used by the FBI, how the response codes translate into responses for USCIS, and how USCIS may proceed upon receipt of a particular response.

135

DEF-00431640

National Background, Identity, and Security Check Operating Procedures

FBI Response Codes resulting from FBI Name Checks		
FBI Response Code	**USCIS Response**	**USCIS Action**

LE

136
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

LE

1.   **Overview of the Positive Response**

LE

137
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

NBC Triage of Positive Responses

The National Benefits Center (NBC) LHM team categorizes all LHMs in one of the four categories (National Security, Egregious Public Safety, Fraud, or Criminal Only/Other). The LHMs categorized as National Security are referred to the NBC National Security Section and triaged by the NBC Controlled Application Review and Resolution Process (CARRP) teams. The LHMs categorized as Egregious Public Safety are referred to the NBC Background Check Unit (BCU) for triage and processing. The LHMs categorized as Fraud are referred to the NBC FDNS Fraud Section for triage and processing. The LHMs categorized as Criminal Only/Other are interfiled and the A-file is returned for normal processing.

NOTE: The NBC does not review the content of an LHM for eligibility determinations.

UNCLASSIFIED LHMs: Unclassified LHMs are interfiled in the appropriate A-file for non-ELIS cases if the A-file is located at the NBC. Interfiling will include attaching an LHM FOUO coversheet as well as attaching the LHM to a purple backing for easier identification. If the A-file is located at the Field Office, the NBC LHM team will notify the Field Office having jurisdiction over the application via e-mail that an unclassified LHM is available for viewing in the Customer Profile Management System (CPMS). For ELIS applications, the NBC LHM team will categorize the LHM in CPMS, and will complete the appropriate referral in ELIS if applicable, but will not interfile the unclassified LHM as the unclassified LHM is available for viewing in CPMS.

CLASSIFIED LHMs: Non-ELIS cases located at the NBC will have a 4b memo interfiled in the A-file to indicate the existence of a classified LHM. The LHM can be accessed through the Citizenship and Immigration Data Repository (CIDR), on the HSDN Network. If the FCO does not have access to HSDN, they will need to contact their District or Region for assistance in gaining access to view the classified LHM. If the A-file is located at the Field Office, the NBC LHM team will notify the Field Office having jurisdiction over the application via e-mail that a classified LHM is available for viewing in CIDR. For ELIS applications[24], the NBC LHM team also categorizes the LHM in CPMS, and will complete the appropriate referral in ELIS if applicable, but will not interfile the 4b memo as CPMS and ELIS both indicate the existence of a classified LHM.

The information in the LHM belongs to the FBI. Therefore, it cannot be shared with a Third Agency without permission from the FBI.

---

[24] If a recent LHM has been generated, the previous LHM will not be replaced by the recent one. Officers will be able to review all related LHMs.

DEF-00431643

National Background, Identity, and Security Check Operating Procedures

Classified LHMs may only be accessed by individuals who have been granted an NSI security clearance. Security clearances are granted only to individuals who have been identified by a formal request from their supervisor to have a need to access classified information in the performance of their assigned job duties. For more information see the USCIS Security Handbook Chapter 8: Classified National Security Information (NSI).

As with the results of any security check, USCIS must first confirm whether the results relate to the individual seeking an immigration benefit by reviewing the response.

2.   Positive Response: LHM

LE

139
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

Example of a Third Agency Referral Document

LE

140
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
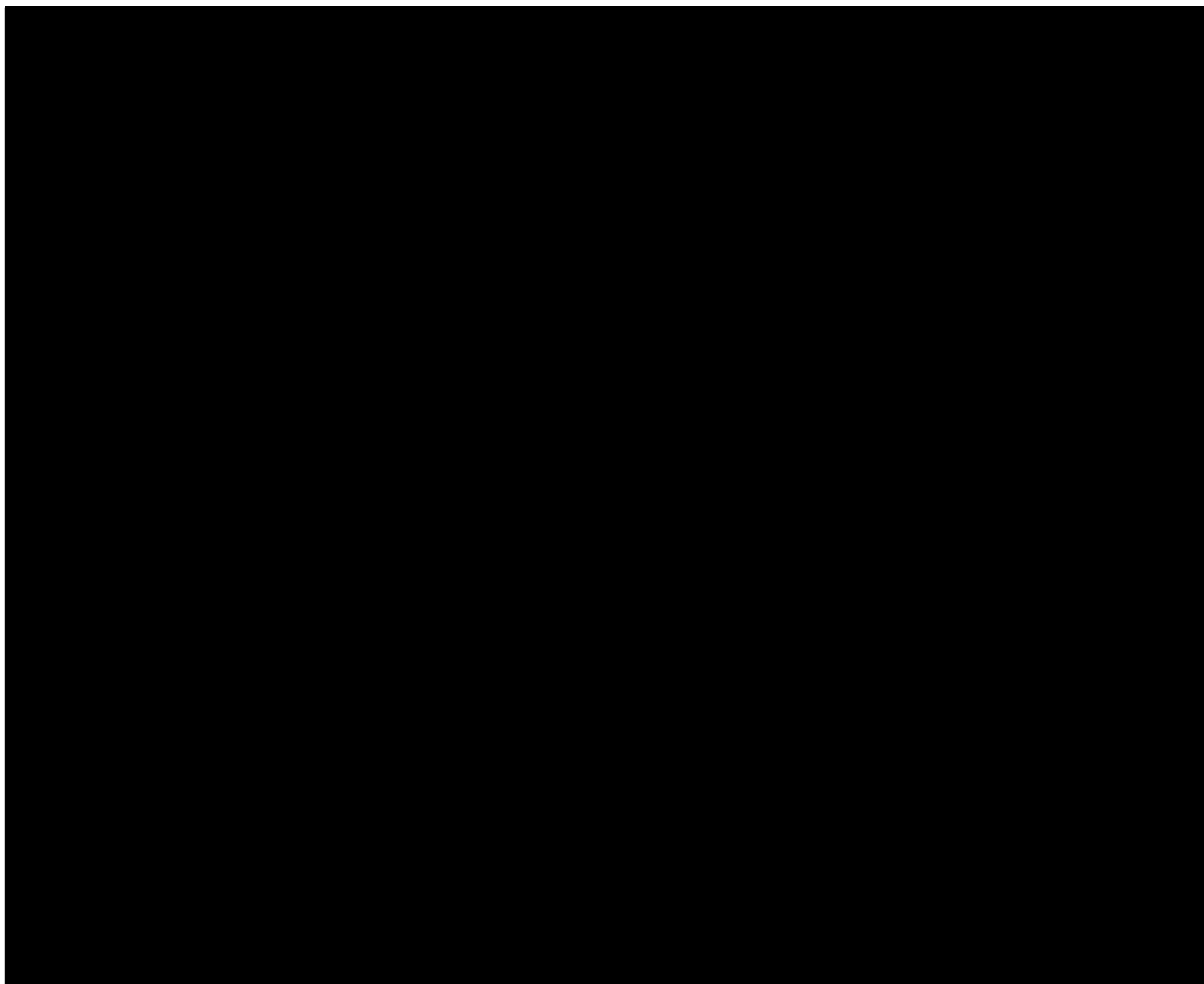<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP⸺in whole or in part⸺unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431645

National Background, Identity, and Security Check Operating Procedures

LE

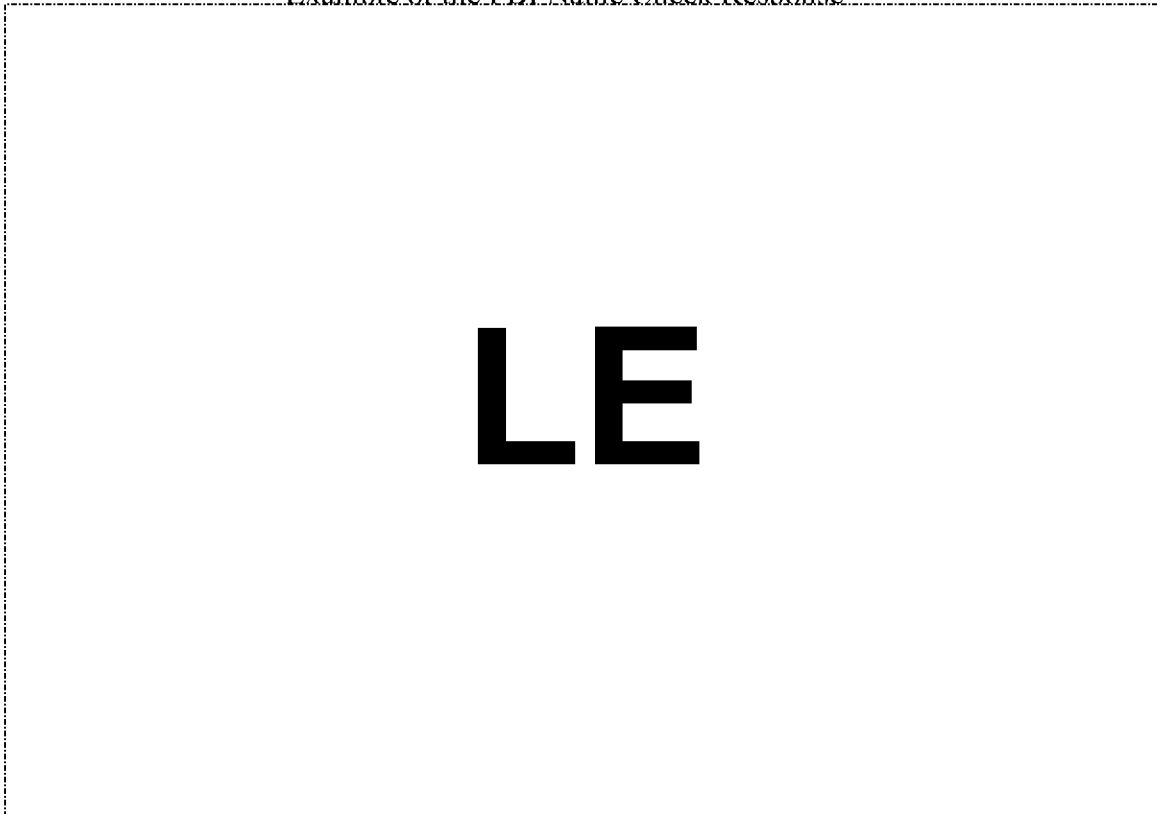FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431646

National Background, Identity, and Security Check Operating Procedures

LE

4.   Positive Response: Miscellaneous Issues

a) *No LHM or* **LE** *Found in CPMS or CIDR*

If CPMS indicates a positive name check response, the associated LHM should be available for viewing in either CIDR or CPMS within one month. If CPMS indicates a positive name check response was received more than one month ago and the unclassified LHM is not available for viewing in CPMS or the classified LHM is not available for viewing in CIDR please follow guidance below.

For Positive Responses to the FBI Name Checks processed by the FBI after February 1, 2008, the field may send an electronic inquiry to ▮▮▮▮▮@uscis.dhs.gov, referencing "LHM" in the

142

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

subject line. The NBC LHM team will reach out to the appropriate contacts to have the missing LHM uploaded into CPMS or CIDR as appropriate.

If an FBI Name Check indicates an electronic Positive Response in a USCIS system processed prior to June 2004, and the hard copy Positive Response cannot be located, the field should submit a Name Check request on the manual spreadsheet in accordance with the December 21, 2006, memorandum entitled "FBI Name Check Policy and Process Clarification for Domestic Operations," asylum officers should submit their request to check primary names through GLOBAL; aliases should be submitted through the manual process.

Unclassified LHMs and [LE] received by HQFDNS from June 2004 to February 2008 were uploaded into FDNS-DS.

If the electronic Positive Response indicates that it was processed between June 2004 and February 2008, please check the A-file first for a hard copy. If the hard copy is not located in the A-file, request assistance to locate the hard copy response through your chain of command to HQFDNS.

b)   *NS and EPS Concerns in Positive Responses*
NS or EPS Concerns must be handled in accordance with established USCIS policy and guidance. Additional guidance is in section IX for NS concerns and section X for EPS concerns.

National Security Indicators:
The following terms may be contained in LHMs. They relate to law enforcement investigations, and are examples of indicators of an NS concern:

-
-
-
-
-
-
-
-
-
-

    LE

-

143

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431648

National Background, Identity, and Security Check Operating Procedures

More indicators are listed in the Guidance for Identifying National Security Concerns issued with the CARRP operational guidance on April 11, 2008.

<div style="border:1px dashed">

LE

</div>
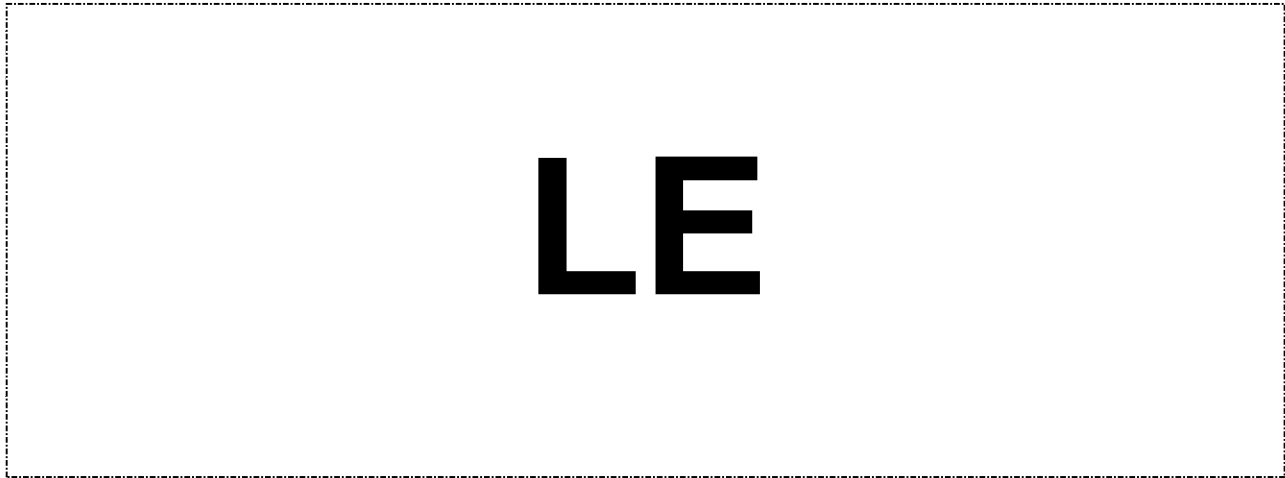
c) *Request for Assistance to HQFDNS for* [**LE**]

<div style="border:1px dashed">

LE

</div>

Send a request for assistance to ████████@uscis.dhs.gov. When sending a request containing PII, officers must comply with the PII requirements explained in the PII manual. The request should be marked "For Official Use Only (FOUO)" and include the following information:

- Subject: Request for Assistance: FBI Name Check [**LE**]
- Full Name (Applicant, Petitioner, Beneficiary, Derivative or Company);
- A-Number;
- Pending Application(s) and/or Petition(s) Form Type(s);
- Nature of assistance requested [**LE**] **LE**
- Requesting officer and Contact Information;
- FDNS-DS NS concern number (if applicable);
- Litigation case information (e.g., court deadline), if relevant; and
- Next court date, if relevant.

If a case requires immediate action due to pending litigation or another urgent matter, officers must ensure that the e-mail sent to the mailbox above is marked urgent and includes the court date or any other deadlines.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

<u>**National Background, Identity, and Security Check Operating Procedures**</u>

VII.   Security Check: FBI Fingerprint Check

A.   FBI Fingerprint Check

The FBI Fingerprint Check provides summary information of an individual's administrative or criminal record within the United States. The FBI Fingerprint Check is conducted through the Next Generation Identification (NGI) system (formerly known as IAFIS). The NGI is a national fingerprint and criminal history system maintained by the FBI's CJIS Division.

State, local, and federal law enforcement agencies submit fingerprints and corresponding administrative or criminal history information to the NGI. Participation by state and local agencies is not mandatory, so the FBI Fingerprint check does not contain records from every jurisdiction. The information contained in the record is obtained using prior fingerprint submissions to the FBI related to arrests and, in some instances, federal employment, naturalization, or military service.

National Background, Identity, and Security Check Operating Procedures

CPMS Query – Fingerprint Check

LE

From this view, the CPMS user may retrieve the IdHS (formerly known as RAP sheet) associated with an "IDENT" response by clicking "FBI Response Text."

B.   Who Requires FBI Fingerprint Checks
Several applications and petitions require individuals to submit to a search of their fingerprints in the FBI's Next Generation Identification (NGI) (formerly known as IAFIS). Generally, applicants ages 14 and over must be fingerprinted. If an applicant turns 14 during the course of adjudication, then an FBI fingerprint check must be performed for the individual.

Several applications/petitions have upper-age limits also, typically age 75 or 79. Check your component's operational guidance for the upper-age limit requirement. The table below lists those forms and individuals requiring FBI Fingerprint Checks. Individuals requiring FBI Fingerprint checks are designated with an "x."

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

Form	FBI Fingerprint Check Requirements by Form Type and Individual						Special Instructions
	Individual Requiring FBI Fingerprint Check (designated with "x")						
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-90	X						
I-129 F			X				Fingerprints may be required per Adam Walsh Act SOP of September 24, 2008.
I-130			X				Fingerprints may be required per Adam Walsh Act SOP of September 24, 2008.
I-131	X						Form is multi-purpose. Biometrics are required for applicants for a re-entry permit and refugee travel documents. An FBI Fingerprint check might be required for applicants for humanitarian parole.
I-192	X						
I-485	X						
I-539	X				X		Exceptions are the following: certain A, G, and NATO nonimmigrants are not required to pay a fee, and attend a biometric appointment.
I-589	X				X		
I-590	X				X	X	Refugee applicants aged 14 – 79 are fingerprinted overseas with mobile units or FD-258 and, by CBP at the POEs upon arrival. For certain refugee applicants, FBI biographic checks are conducted through the SAO process.
I-600			X	X		X	HH members 18 years of age and older; Beneficiaries between 14-16 years old.

148

National Background, Identity, and Security Check Operating Procedures

| Form	Individual Requiring FBI Fingerprint Check (designated with "x")						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-600A	X					X	HH members 18 years of age and older.
I-601	X						See Section IV, Part C for more information on applications filed overseas.
I-601A	X						
I-687	X						
I-698	X						
I-730				X			If beneficiary is in the United States.
I-800			X	X		X	HH members 18 years of age and older; Beneficiaries between 14-16 years old.
I-800A	X					X	HH members 18 years of age and older.
I-817	X					X	
I-821	X						
I-821D		X					
I-829	X				X		
I-881	X						
I-914	X						
I-918			X				
N-400	X						

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431654

National Background, Identity, and Security Check Operating Procedures

FBI Fingerprint Check Requirements by Form Type and Individual						
Form	**Individual Requiring FBI Fingerprint Check (designated with "x")**					**Special Instructions**
	Petitioner		**Beneficiary**	**Derivatives**	**Household (HH) Members**	
	Conditional Resident (CPR)	**USC/LPR through whom CPR status acquired**				
I-751	X*			X		* Fingerprints are required for the Conditional Permanent Resident (CPR) only (not for the USC/LPR through whom the CPR status acquired)[25]

Note: Pursuant to the Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance issued on December 26, 2018, FBI Fingerprint Checks also are required for NTA issuance purposes, in some cases for applicants/requestors who have not previously submitted biometrics to USCIS. USCIS must issue an NTA after denying applications/requests or claims as described in "Updated Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Deportable Aliens," dated June 28, 2018, and the USCIS memorandum entitled "Domestic Operations Standard Operating Procedures, Form I-862, Notice to Appear" [26] dated September 8, 2006.

For DACA cases, refer to PM-602-0161, entitled "Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) When Processing a Case Involving Information Submitted by a Deferred Action for Childhood Arrivals (DACA) Requestor in Connection With a DACA Request or a DACA-Related Benefit Request (Past or Pending) or Pursuing Termination of DACA," dated June 28, 2018.

For additional information regarding FBI fingerprint check requirements specific to NTA issuance, refer to Section XII of this Handbook.

---

[25] Refer to the SCOPS I-751 Adjudication SOP.
[26] In January of 2010, the Domestic Operations Directorate was split, as part of an agency-wide reorganization, into the Field Operations and Service Center Operations Directorates. References to Domestic Operations in the titles of memos cited in NaBISCOP should be assumed to apply to employees of both of the new directorates. The memos themselves will state whether they apply to Field Operations or Service Center Operations personnel.

National Background, Identity, and Security Check Operating Procedures

1.   Waiver of Fingerprints Due To Health Issues

An individual may be unable to provide any fingerprints or legible fingerprints due to various circumstances (e.g., a birth defect, physical deformity, or skin condition), and may be granted a waiver of the fingerprint requirements. Only an individual in charge of biometrics collection (i.e., ASC immigration services officer (ASC-ISO) or designated overseas officers) may grant a fingerprint waiver. To qualify for a waiver, an applicant must be scheduled for and appear at a biometrics appointment so a determination can be made as to whether they are eligible for a fingerprint waiver.

If a fingerprint waiver is granted, the following occurs:

- The ASC-ISO or designated officer annotates the biometrics appointment notice and issues an Applicant Police Clearance Notice. The annotations to the biometrics appointment notice detail the condition(s) that warrant(s) the fingerprint waiver.
- The individual granting the waiver (i.e. ASC-ISO) provides a copy of the annotated biometrics notice and the original Applicant Police Clearance Notice to the individual requesting the fingerprint waiver. The Applicant Police Clearance Notice instructs an individual who was unable to have biometrics collected to obtain police clearances and arrest reports (if any) from every jurisdiction (inside and outside of the United States) where they resided or were physically present for six (6) months or more during the past five (5) years, and to bring the clearances to their interview or examination.
  - o If an individual is unable to obtain police clearance(s) from a jurisdiction <u>outside the United States</u> where they resided or were physically present for six (6) months or more within the past five (5) years, the individual must provide a <u>detailed</u> sworn statement, attestation, or written description of the reason why they are unable to obtain police clearances from jurisdictions <u>outside the United States</u>. This description must include steps that were taken to attempt to procure police clearances and should include any supporting documentation the individual possesses.
  - o Asylum and refugee applicants and derivatives and individuals who hold or have held asylum- or refugee-based status are not required to procure police clearance(s) from the country or countries in which they experienced or fear persecution, but must still provide a sworn statement, attestation, or written statement explaining that this is the reason they cannot procure police clearance(s) from that country or countries.
  - o USCIS will ultimately determine on a case-by-case basis whether the written description and supporting documentation is sufficient to excuse the absence of police clearances from jurisdictions<u> outside the United States</u>.

DEF-00431656

National Background, Identity, and Security Check Operating Procedures

- o USCIS should only excuse the absence of police clearances in the most exceptional circumstances, when an individual is unable to obtain a police clearance from every jurisdiction inside the United States where the individual resided or was physically present for six (6) months or more within the past five (5) years.
- The ASC sends the original annotated biometrics notice and a copy of the Applicant Police Clearance Notice to the service center having jurisdiction over the biometrics site, which should in turn forward the documents to the A-file.
- At the time the fingerprint waiver is granted, ASC personnel inform the applicant that police clearances will be required and give the applicant a notice explaining the documentation required. USCIS personnel will administer the Record of Sworn Statement (Fingerprints) to the person seeking the waiver, if an interview is normally required for the application and/or petition in question.

If the individual admits to a criminal history during the completion of the Record of Sworn Statement (Fingerprints), or police clearance documents indicate a criminal record, the USCIS officer requests submission of all related arrest records and court dispositions. However, if the IdHS is interfiled and contains the disposition of the crime and the crime does not affect eligibility to benefits sought, the related arrest records and court dispositions may not be needed. In such case, the officer should annotate "Do not request arrest records and court dispositions" on the worksheet.

2.   Age-related Exemptions
An applicant who is at least 75 years old or is at least 79 years old for some applications is exempt from fingerprinting requirements. To see specific procedures and requirements for completing the Record of Sworn Statement (Fingerprints) or requesting police clearance documents, please see the specific form guidance.

C.   FBI Fingerprint Check Procedures
For most immigration benefits, fingerprints are requested automatically during the upfront processing of the immigration form. Domestically, individuals who must provide fingerprints receive appointment notices to appear at the appropriate USCIS ASC. Fingerprints taken at an ASC are submitted electronically through the NGI system (formerly known as IAFIS). USCIS links fingerprints to one or more of the receipts for which they are collected (e.g., a stand-alone I-539, a concurrently filed Form I-485 and I-131, etc.). However, if an individual submits multiple or stand-alone immigration filings, each with an associated biometrics requirement, a new biometric collection and updated criminal history background checks are required. USCIS requires that fingerprints be collected for each application, petition, or benefit request with an

DEF-00431657

National Background, Identity, and Security Check Operating Procedures

associated biometrics requirement, not only to initiate criminal history background checks but also for identity verification purposes.

There are two exceptions to the requirement to collect new biometrics:
- Military Naturalization: a biometric background check must be performed, but USCIS may use previously collected fingerprints from a different immigration filing or may use fingerprints collected as part of enlistment processing to perform the check.
- Notice to Appear (NTA) Issuance: USCIS permits the reuse of previously collected fingerprints because the NTA is not an application, petition, or benefit request submitted by an individual.[27]

USCIS receives electronic responses to ten-print fingerprint submissions [LE] The results are returned electronically in the Customer Profile Management System (CPMS).[28] Within days, the FBI Fingerprint Check results are made available in GLOBAL, CAMINO, and ELIS.

Individuals residing overseas who are applying for an immigration benefit may be fingerprinted, at the discretion of the FOD or DD, by USCIS officers overseas, a U.S. consular officer at a U.S. Embassy or consulate, or at a U.S. military installation abroad. For the majority of refugee applicants, authorized personnel collect their fingerprints at the time and location of the refugee interview.

---

[27] Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance, dated December 26, 2018. Departure-Related Systems Checks Requirement Preceding Notice to Appear (NTA) Issuance, dated December 26, 2018.

[28] CPMS has been identified as the data repository that directly receives fingerprint data from the ASC fingerprint capturing devices and then passes the fingerprint data on to other databases, include CPMS QUERY. Therefore, CPMS should be used as an authoritative source for determining whether an FBI response exists or whether someone has been fingerprinted at the ASC. If the FBI response is IDENT and within the last 15 months, IDHSs may be obtained directly from CPMS. CPMS should not be confused with the Biometrics Online Web Site, which connects to the same data repository, but displays only information related to the photograph right index print and signature image taken at the ASC.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431658

National Background, Identity, and Security Check Operating Procedures

CPMS Query -- FBI Fingerprint Check Criteria

CPMS Query - Search

LE

D. Types of Results from FBI Fingerprint Checks

CPMS Query Summary View

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431659

National Background, Identity, and Security Check Operating Procedures

Fingerprint checks are returned as one of three results:

Description of FBI Response	
FBI Response	**Description of FBI Response**

LE

155
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Description of FBI Response	
FBI Response	**Description of FBI Response**

LE

---

[29] See the International Operations Division Field Guidance on Application for Waiver of Grounds of Inadmissibility, Form I-601.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Description of FBI Response	
FBI Response	**Description of FBI Response**
LE	

E. IdHS Review

The IdHS (formerly known as the RAP Sheet), or Identity History Summary, is issued when an individual's fingerprints are identified in the FBI's database and describes arrests and subsequent dispositions attributable to that individual. For immigration, criminal history information is important to determine eligibility for the benefit sought. Review the IdHS carefully for additional A-numbers.

The IdHS is composed of two sections, the cover page and the arrest and court data. The cover page includes the FBI Universal Control Number (UCN), a unique control number assigned to every submission in NGI (formerly known as IAFIS). The use and dissemination restrictions and the descriptive information about the subject fingerprinted are also included in the cover page.

The arrest and court data consists of information submitted to the FBI from local, state, federal, and international criminal justice agencies. It can include arrest information, court information, supervision or custody, wanted information, and/or sexual offender registry information.

The arrest and court data section will also include the master name. This is the name associated with the first set of fingerprints submitted to the FBI for a subject. In most cases, this name and a unique identifying number will always be associated to the record. The FBI UCN is the unique number assigned by the FBI to a subject of a record.

The arrest record will appear from oldest to newest and include the date of arrest, a State Identification Number (SID), assigned to the individual by the state where the arrest occurred.

National Background, Identity, and Security Check Operating Procedures

The Originating Agency Identifier (ORI) is the number of the agency that submitted the information. The IdHS will list the charges at the time of the arrest, and when available court disposition or the date when the FBI last received information on this record.

When court information is submitted by the state to the FBI, it will include the charge, sentence, and the date of sentencing. Please note that the charge in the arrest might differ from the court information due to amended or reduced charges. Review this information thoroughly, as felony charges may have been reduced to a misdemeanor charge.

If an outstanding warrant for the individual exists, it will appear at the end of an IdHS with a notice and the wanted information. This will include Wanting/Originating Agency, NCIC Number, Wanted Name, which might differ from master name, charges, case number, date of warrant, and ORI with contact information. Follow local policy for contacting the law enforcement agency to confirm the warrant and for appropriate action.

F.   Validity of Results from FBI Fingerprint Checks
According to USCIS policy, a fingerprint result expires 15 months after the date of the FBI response. The FBI response date is displayed in CPMS Query as the PROCESS DATE and for asylum applications in GLOBAL, in the RESULT field. This may differ from the date printed on the IdHS.

USCIS requires that fingerprints must be collected for each application, petition, or benefit request with an associated biometrics requirement (e.g., I-485, N-400, I-539, I-589, I-821D, etc.).[30] Except in the case of military naturalization (as noted in FBI Fingerprint Check Procedures), fingerprints cannot be reused from one receipt or form type to another.

An IdHS is only valid for 15 months after the FBI response. In most cases, an updated IdHS is required for individuals whose fingerprint result is more than over 15 months old (see exceptions below).

An updated IdHS is also required when IDENT (Legacy US-VISIT IDENT) reveals new criminal information dated after the most recent FBI Fingerprint Check was completed. Please see "How to Obtain an Updated IdHS" for information on obtaining an updated IdHS.

In cases with an associated biometrics requirement, USCIS collects biometrics, initiates security checks, and obtains a fingerprint result. However, due to extended processing times or backlogs, a fingerprint result may expire prior to adjudication due to the passage of 15 months. USCIS

---

[30] Previously collected fingerprints may be reused for Military naturalization and NTA (I-862) issuance. However, only complete sets of fingerprints that previously yielded an IDENT or NON-IDENT response may be reused for NTA issuance.

DEF-00431663

<u>**National Background, Identity, and Security Check Operating Procedures**</u>

collected biometrics on the application, petition, or benefit request in question and verified the identity of the subject at the original ASC appointment. As such, USCIS may "refresh" the expired fingerprint result without requiring a second biometrics collection.

A fingerprint "refresh" is different from fingerprint "reuse." A fingerprint "<u>refresh</u>" is a resubmission of previously collected fingerprints to the FBI for an updated result *for the same receipt number*. A fingerprint "refresh" is sometimes referred to as a fingerprint "resubmit" (e.g., in CPMS). A fingerprint "refresh" or "resubmit" is <u>permissible</u> when the fingerprint result expires prior to adjudication because of extended processing times or backlogs.
- Example: Subject files an N-400 on January 1, 2020. Subject appears for biometrics collection on February 1, 2020 and the FBI result is dated that same day. Subject's N-400 is not adjudicated by May 1, 2021 due to processing delays, causing the fingerprint result to be expired and must be refreshed. This type of action is permitted.

If, for any reason, the fingerprint refresh does not generate an updated fingerprint result, then the subject must be scheduled for a second ASC appointment because of the prohibition on adjudicating with an expired FBI fingerprint check result.

A fingerprint "<u>reuse</u>" is using a fingerprint result/IdHS from one application or petition to satisfy the fingerprint requirement on a different application or petition (*including* a subsequent filing of the same form type). A fingerprint "reuse" may also mean resubmitting fingerprints collected for one receipt to obtain a current fingerprint result/IdHS on any other receipt (*including* a subsequent filing of the same form type). Both actions are <u>not permissible</u>. USCIS does not permit fingerprint reuse without first having biometric identity verification, except for military naturalization cases and NTA issuance. *See* Part C: FBI Fingerprint Check Procedures. Biometric identity verification typically occurs at an ASC appointment.
- Example: Subject files an I-485 on January 1, 2020. Subject appears for biometrics collection on February 1, 2020 and the FBI result is dated that same day. Subject files an I-131 on March 1, 2020. Subject fails to appear for Form I-131 biometrics collection on April 1, 2020. USCIS personnel must not use the FBI fingerprint result from the Form I-485 to satisfy the fingerprint check requirement for the Form I-131. There is no identity verification in this scenario which is why fingerprint "reuse" is not permitted.
- Example: Subject files an I-90 on January 1, 2020. Subject fails to appear for biometrics collection on February 1, 2020. While checking CPMS, the adjudicator notices the previous I-90 fingerprint result is on record. USCIS personnel must not use the FBI fingerprint result from a previous immigration filing—even the same form type—to satisfy the fingerprint check requirement for the pending I-90. USCIS requires that fingerprints must be collected for each application, petition, or benefit request with an associated biometrics requirement. There is no identity verification in this scenario which is why fingerprint "reuse" is not permitted.

National Background, Identity, and Security Check Operating Procedures

G.   Where to Place Results from FBI Fingerprint Checks

The IdHS (original from CJIS or system generated copy from CPMS) must be placed on the non-record (right) side of the file. The screen shot results of the FBI Fingerprint Check must also be placed on the non-record side of the file.

H.   Other Procedures Relating to FBI Fingerprint Checks

1.   How to Obtain an IdHS When Not in the File

If the IdHS is not located in the A or T file, USCIS personnel may:

- Query the individual's receipt number, A-number, social security number, or first and last name in the Customer Profile Management System (CPMS) Online Archive Web Site, available at https://cpms.uscis.dhs.gov/.[31] Ensure that the IdHSs obtained through CPMS are complete and accurate.
- If CPMS does not contain a record that corresponds with the IDENT result, and if the office has not received an IdHS, USCIS personnel may contact the Office of Fingerprint Liaison (OFL) to assist in troubleshooting the applicable transaction and corresponding results.
- The applicable USCIS office primary or alternate fingerprint coordinator designated to contact the OFL may send a request by completing an IdHS request form. See the spreadsheet example below.
- E-mail the IdHS request form to the USCIS, Office of Fingerprint Liaison at e-mail address "Fingerprint, Liaison (███████████@uscis.dhs.gov)." Status inquiries may be directed to the same e-mail address.

If the request pertains to an applicant whose fingerprint processing has been expedited, identify it as such in the subject line of the e-mail.

APPLICANT Name (LAST NAME, FIRST NAME)	A-NUMBER (If orphan, use S in front of number e.g. A0re45678)	DATE PRINTS LAST PROC. BY FBI	FBI No. (UCN)[32] (This is not an internal USCIS Control Number)	Applicant DOB (optional)
LE				

2.   How to Obtain an Updated IdHS

Fingerprint Resubmission Instructions for IDENT/NON-IDENT

---

[31] Note, consult the USCIS Service Desk if the link does not work.
[32] "FBI Universal control Number" [formerly known as the FBI Number (FNI)]

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431665

National Background, Identity, and Security Check Operating Procedures

The instructions below describe the standardized process for submitting IDENT and NON-IDENT Fingerprint Resubmission requests. (Refresh and resubmissions are synonymous - for the purpose of these instructions, resubmission will be the terminology used).

Step 1: File Preparation / Verification

- All A-numbers must include the preceding 'A' followed by the 9 numerical characters.
- The form type must be written with no spaces or hypens between the first and second characters. For example, I485, I765, etc.
- If the request is not submitted on the correct Resubmission Template, it will be returned to the sender for corrective action.
- Fingerprints may be resubmitted 12 months since the last (re)submission. Fingerprints that are submitted prior to the 12 months may be flagged as "Existing Fingerprints." If the requesting official has reason to believe the applicant's background status has changed, include "Requesting Priority Resubmission" in the body of the email request.
- All resubmissions must be submitted using the template found at the link below:

Resubmission Template

Step 2: Submitting Request

- It is recommended that the subject line of the email read "Fingerprint Resubmission for [submission date], [total number of records]". For example, "Fingerprint Resubmission for 2/26/15, 10 records". NOTE: This is a suggestion only. Please follow local procedures.
- Please email the resubmission request to ██████████@uscis.dhs.gov. Requests sent to other email boxes will not be honored.
- NOTE: Fingerprints originally submitted during the following time periods cannot be resubmitted and will need to be scheduled for an ASC appointment.
    - Prior to 2006
    - December 1, 2007 to March 31, 2008
    - September 1, 2008 to October 31, 2008

3.   How to Obtain a Complete IdHS when National Fingerprint File (NFF) state Criminal History Record Information (CHRI) is Missing
Upon receiving a civil applicant fingerprint check, FBI CJIS reaches out electronically to applicable NFF states in the event of an IDENT with an identity held in the Interstate Identification Index (III). Sometimes the NFF state response times-out and the FBI CJIS response to USCIS fails to include applicable NFF state CHRI. USCIS components may contact

161
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

the Office of Fingerprint Liaison to obtain a complete IdHS. This procedure only applies to incomplete NFF state responses.

NFF states include: Colorado, Florida, Georgia, Hawaii, Idaho, Iowa, Kansas, Maryland, Minnesota, Missouri, Montana, New Jersey, New York, North Carolina, Ohio, Oklahoma, Oregon, Tennessee, West Virginia and Wyoming.

Non-NFF states include: Alabama, Alaska, Arizona, Arkansas, California, Connecticut, Delaware, District of Columbia, Illinois, Indiana, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Mississippi, Nebraska, Nevada, New Hampshire, New Mexico, North Dakota, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Vermont, Virginia, Washington, and Wisconsin.

Incomplete responses from non-NFF (Purpose Code I) states may be resolved by the adjudication's component with the applicant.

Requests for a complete IdHS when the NFF state response is missing may be made by sending an email with a completed Excel spreadsheet/request form attached to the Office of Fingerprint Liaison a█████████████@uscis.dhs.gov, listed in Outlook as Fingerprint, Liaison.

Examples:
1.   All Records:

LE

162

National Background, Identity, and Security Check Operating Procedures

2.   Maryland

LE

163
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

3.   Montana

LE

164
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

VIII. Security Check: IDENT (Legacy US-VISIT IDENT)

A.   About IDENT

The Office of Biometric Identity Management (Legacy US-VISIT IDENT), under the Management Directorate of the Department of Homeland Security (DHS), provides biometric identification services that is part of a continuum of security measures that begins overseas and continues through a visitor's arrival in and departure from the United States. It incorporates eligibility determinations made by both DHS and DOS. The main repository for OBIM is IDENT, or the Automated Biometric Identification System. It is the largest biometric repository in the U.S. government.

In many cases, IDENT records begin overseas at, at locations such as the U.S. consulates issuing visas or refugee circuit ride locations, where prospective visitors' or immigrants' biometrics (digital finger scans and photographs) are collected and checked against a database of known criminals and suspected terrorists. When the visitor or prospective immigrant arrives at the port of entry, IDENT provides CBP officers with the ability to instantly check that the person is the same person who received the visa or was approved for immigration benefits. In other instances, IDENT records may begin domestically, when an individual is encountered by CBP or ICE as part of a finding of inadmissibility or an enforcement action.

IDENT encounter searches currently are mandatory for all asylum[33] and, refugee; applicants and dependents aged 14 to 79 as well as individuals being screened for credible fear or reasonable fear aged 14 or older. Due to processing times, IDENT screening may be initiated for these populations before they reach the age of 14. (Refer to component-specific guidance for additional details.)

1.   CPMS IVT (Legacy Secondary Inspections Tool – SIT)

The Secondary Inspections Tool (SIT) was established as part of the broader US-VISIT Program established under the Homeland Security Act of 2002. While some components still employ SIT, most have adopted to the Customer Profile Management System Identity Verification Tool (CPMS IVT), which is a Web-based application that interfaces with the Automated Biometric Identification System (IDENT) database. CPMS IVT includes the following features of interest to the USCIS user community:

-
-

LE

---

[33] Refer to the Affirmative Asylum Procedures Manual (AAPM).

DEF-00431670

National Background, Identity, and Security Check Operating Procedures

-
-

LE

Using CPMS IVT, the officer may verify that the person who appeared at the ASC is the same person who is appearing for the interview. USCIS District and Field Offices are required conduct IVT verification at the time of appearance for interview when fingerprint information is captured by an Application Support Center (ASC) and:

- The applicant/petitioner has filed one of the following form types: I-90, I-130 (in some cases*), I-131, I-539, I-485, I-600, I-600A, I-687, I-698, I-751, I-800, I-800A, I- 817, I-821, I-829, N-336, N-400
- An interview at a domestic USCIS District/Field Office is required as part of the adjudication process; or
- A customer appears at a domestic USCIS District/Field Office to obtain documentation of an immigration benefit (e.g. temporary I-551 or travel document).

*Note: The only U.S. citizen petitioners who would be subject to IVT would be petitioners filing orphan or adoption petitions (Forms I-600/600A or Forms I-800/800A) and U.S. citizen petitioners of family-based petitions required to appear at an ASC for biometric capture for purposes of complying with the Adam Walsh Act (AWA).

Also, prior to the adjudication (approval or denial) of any application, USCIS officers must use IVT for any applicant (with two exceptions for U.S. citizen petitioners) age 14 and over for naturalization cases and ages 14 to 79 for adjustment of status cases:

- Who is appearing at a domestic USCIS District/Field Office for a required interview in connection with an immigration or naturalization benefit, or to receive a document evidencing an immigration benefit (those cases where the interview is waived will not require IVT verification);
- Whose fingerprint information is required to support the immigration benefit sought (in order to perform a 1:1 comparison with an ASC encounter, the applicant must have appeared at the ASC and was required to do so as a prerequisite for the benefit being sought); and
- The applicant was required to appear at an ASC for biometric collection.

Refer to Volume 13, Chapter 8 of the Consolidated Handbook of Adjudication Procedures (CHAP) for additional guidance.

National Background, Identity, and Security Check Operating Procedures

Within RAIO, Asylum uses CPMS IVT to biometrically verify the identity of previously-fingerprinted I-589 applicants at the time of interview. IVT is also used, in some locations, when the applicant receives the final decision. Additionally, International and Refugee Affairs Division (IRAD) uses IVT in certain international locations as part of adjudicating I-131 applications for Refugee Travel Document based upon an underlying I-589 or I-590 application. (Refer to component-specific guidance for additional details.)

2.   ASC Processing

When an applicant/beneficiary appears at the ASC, ASC personnel digitally capture the following biometrics from the applicant/beneficiary:

- Photograph (all applicants)
- Signature (all applicants)
- Right index fingerprint (applicants requiring a card to be produced) and/or
- 10-prints (for applicants aged 14 and older requiring FBI Fingerprint Check and IDENT enrollment). Refer to component-specific guidance for additional details on biometrics collection for applicants below this age.

The photograph, signature, and right index fingerprint are stored in CPMS and may eventually be used by USCIS to create Form I-765, Employment Authorization Documents (EAD), if applicable. The 10-prints are electronically submitted to the FBI to search against the NGI (formerly known as IAFIS) system (FBI Fingerprint) database and certain RAIO forms (I-589, I-590, and certain I-730s) are submitted to the DoD Automated Biometric Information System (ABIS). In addition, the 10-prints and photograph are electronically submitted to and searched against the IDENT database. The responses from the FBI and DoD are stored in CPMS along with the IDENT status.

3.   Parameters of Encounter Data Contained in IDENT

The IDENT database currently contains biometric identifying information for the following individuals but is not all inclusive of the data found in IDENT:

-
-

LE

-

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

- LE

- Individuals who have been enrolled in frequent traveler programs by CBP (includes Free and Secure Trade (FAST), Northern Border Crossing System (NEXUS), and Secure Electronic Network for Travelers' Rapid Inspection (SENTRI)).

-

-

-

-

  LE

-

-

-

Individuals applying at ports of entry were added to the IDENT database according to the following table:

Date	Dataset	CBP/US-VISIT Deployment or Application
1/5/2004		
1/5/2004		
8/2004 (rolling basis)		LE
8/20/2004		
8/20/2004		

168

National Background, Identity, and Security Check Operating Procedures

9/2004 (rolling basis)	**LE**
9/30/2004	
11/15/2004 to 12/31/2004	
12/31/2005	

LE

LE Certain individuals and groups of travelers are exempt from IDENT's fingerprint processing during Entry and Exit, and **LE** These include:

- Visitors admitted on an A-1, A-2, C-3, G-1, G-2, G-3, G-4, NATO-1, NATO-2, NATO-3, NATO-4, NATO-5, or NATO-6 visa;
- **LE**
- Persons over the age of 79;
- Classes of visitors the secretary of state and the secretary of Homeland Security jointly determine shall be exempt;
- An individual visitor the secretary of state and the secretary of Homeland Security or the director of Central Intelligence Agency jointly determine shall be exempt;
- Taiwan officials who hold E-1 visas and members of their immediate families who hold E-1 visas;
- **LE** nd
- Canadian citizens not requiring an I-94.

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431674

<u>**National Background, Identity, and Security Check Operating Procedures**</u>

3.1: Watch List Dataset[34]

LE

LE

170
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

LE

171
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431676

National Background, Identity, and Security Check Operating Procedures

LE

B.   Who Requires CPMS-IVT/IDENT-based Checks

Applicants and beneficiaries aged 14 and older (see component-specific guidance regarding biometrics collection for applicants below this age) who appear at a USCIS District/Field Office or Asylum Office for interview have their identities verified through a 1:1 IDENT match using CPMS-IVT. If the individual appearing at the Field Office is not the same individual who appeared at the ASC (an "imposter"), the Field Office will follow applicable program and local procedures for referral of imposters.

There may be occasions where an applicant's identity cannot be verified biometrically on the day of or at the time of the interview due to system difficulties or, in rare circumstances, resource constraints. In these instances, field office personnel will attempt to verify the applicant's identity biometrically after the interview on the same date. In any case, applicants' identities must be verified prior to adjudication (approval or denial). And additional A-files identified during the verification process must be requested, consolidated, and any discrepancies resolved. Any hit information associated with the record must be considered prior to the issuance of any approval.

Form I-485

In addition, a Final IDENT check must be conducted on the day of final adjudication for all Form I-485 applicants, whether approved or denied. Note: Final IDENT checks are not required on:

- Withdrawals,
- The following denials executed at the NBC in the preprocessing of I-485s
  - Insufficient Filings – denied very early after contractor review for lack of initial evidence
  - Fingerprint Abandonment – denied after the applicant fails to show for fingerprint appointment

NOTE: Denials for the above stated reasons executed at any Field Office must run the Final IDENT Check prior to final adjudication.

DEF-00431677

National Background, Identity, and Security Check Operating Procedures

Form N-400

The Final IDENT check (also known as Oath IDENT Report) must be conducted within one business day of the naturalization Oath ceremony for all Form N-400 naturalization candidates. Note: Final IDENT checks are not required on:

- Withdrawals,
- The following denials executed at the NBC in the preprocessing of N-400s
  - Insufficient Filings – denied very early after contractor review for lack of initial evidence
  - Fingerprint Abandonment – denied after the applicant fails to show for fingerprint appointment

NOTE: Denials for the above stated reasons executed at any Field Office must run the Final IDENT Check within one business day of the final adjudication.

No Final IDENT checks are required on any I-485s or N-400s that are administratively closed.

Refer to Volume 13, Chapter 5 (Final IDENT Checks) and Chapter 8 (Customer Profile Management System–IDENTity Verification Tool (CPMS-IVT) of the CHAP or other component-specific procedural guidance for detailed information on triaging, referring, and resolving IDENT-based information.

C.   Types of Results from IDENT Checks

1.   National Security Indicators

Various government agencies, including DHS components (USCIS, CBP, and ICE), DOS, the FBI, and the National Ground Intelligence Center (NGIC), load biographic and biometric information into IDENT. The IDENT watch list includes, but is not limited to, biographic and/or biometric information for KSTs; fingerprints for military detainees held in Afghanistan, Pakistan, and Guantanamo; and individuals inadmissible or removable under sections 212(a)(3)(A), (B), or (F), or 237(a)(4)(A) or (B) of the Act.

2.   Criminal History Indicators

IDENT checks may reveal the FBI has criminal information related to an individual. An IDENT

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

                                                                    DEF-00431678

National Background, Identity, and Security Check Operating Procedures

D.   Validity of Results from IDENT Checks

IDENT checks do not expire. However, since new information may be added to the IDENT record at any time, the best practice is to perform a check prior to final adjudication, in accordance with local and component guidance.

E.   Where to Place Results from IDENT Check

All biometric matches discovered through the USVISIT-SIT or CPMS IVT should be printed and placed on the non-record (right) side of the file.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431679

National Background, Identity, and Security Check Operating Procedures

IX.   Resolution: National Security Concerns (CARRP)

A.   CARRP Policy and Operational Guidance

On July 26, 2011, USCIS issued an updated policy memorandum entitled "Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists," as well as associated Supplemental Guidance.

The policy memorandum and subsequently issued operational guidance for the following USCIS components apply to all applications and petitions that convey an immigrant or nonimmigrant status in which an officer identifies a National Security (NS) Concern.

April 24, 2008, operational guidance entitled "Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns."

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

February 6, 2009, policy memorandum "Additional Guidance on Issues Concerning the Vetting and Adjudication of Cases Involving National Security Concerns (Clarification Memorandum)," signed by Acting Deputy Director Michael Aytes.

March 26, 2009, policy memorandum entitled "Uniform Instructions for Standardized CARRP File Identification and Movement of CARRP Cases within USCIS (File Movement Memorandum)".

B.   Definition of NS Concern

At any stage of the screening or adjudicative processes, an officer may identify an indicator of an NS concern with respect to an individual or organization. An 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.

When deciding whether an NS concern exists:
- 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.
- Need not consider satisfying the legal standard used in determining admissibility or removability.

175

National Background, Identity, and Security Check Operating Procedures

- 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.

A NS concern can be either a Known or Suspected Terrorist (KST) or Non-KST NS Concern.

1.   Known or Suspected Terrorist (KST)

In accordance with CARRP policy, there are two types of NS concerns, Known or Suspected Terrorist (KST) and Non-KST. Each type requires specific handling which is outlined in the policy and in greater detail in the operational guidance.

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 NCIC, TECS, and/or CLASS, as used by DOS. For information on standalone **LE** records, refer to Chapter V, Section K, Step 4C within the NaBISCOP Handbook. A KST in NCIC has an **LE** number. However, if the record indicates that the individual is a gang member and there are no additional indicators that the individual is an NS concern, the hit should be resolved according to standard operating procedures for individuals who are a risk to public safety. A KST in TECS has a record number beginning with a **LE** or **LE** and should indicate that the individual is a " **LE** **LE**

TECS **LE** records with an exclusion code of **LE** are not KSTs, though they do require contact with the TSC to determine whether the KST NS concern relates to the individual and to record the encounter. Subjects with a TECS **LE** record with an exclusion code other than **LE** **LE** e., traditional TECS **LE** records) must be treated as KSTs under CARRP, per existing USCIS, directorate, and local guidance. Once officers have contacted TSC to report the encounter and confirm if the **LE** record is a positive match, **LE** hits confirmed to match to the current subject should be processed as Non-KST NS concerns under CARRP. For more information officer should consult the May 23, 2012, FDNS Policy Memorandum entitled, "Updated Instructions for Handling TECS **LE** Records".

Note: A KST NS record can be added or removed during any stage of the CARRP process. The FDNS-IO or designated officer must confirm that the subject is no longer a KST NS concern. Officers should consult the June 5, 2009, Domestic Operations memorandum entitled, "Clarification and Delineation of Vetting and Adjudication Responsibilities for Controlled Application Review and Resolution Program (CARRP) Cases in Domestic Field Office".

National Background, Identity, and Security Check Operating Procedures

2.   Non-KST NS Concern

A Non-KST NS concern includes all other NS concerns, regardless of source, including, but not limited to: associates of KST(s), un-indicted co-conspirators, terrorist organization members, persons involved with providing material support to terrorists or terrorist organizations, and agents of foreign governments.

Officers should refer to Guidance for Identifying National Security Concerns, as a tool for assistance in identifying NS indicators. Pay particular attention to the following sections:

- Statutory Indicators;
- Non-Statutory Indicators;
- Security Check Indicators;
- FBI Name Check;
- FBI Fingerprint or NCIC Criminal History Check | **LE** |
- IDENT; and
- TECS.

3.   Non National Security (NNS)

At any time during the adjudication process, a determination may be made that an NS concern no longer exists or that an NS indicator, after further research, does not meet the definition of an NS concern in accordance with CARRP. Once a determination has been made that an NS concern no longer exists, the case no longer falls under CARRP processing and must be returned to routine work flow not withstanding any other issues such as EPS or fraud and following supervisory approval.

C.   Four Step Approach to Cases with National Security Concerns

The CARRP process provides a disciplined approach to identify, record, and adjudicate applications and petitions where a National Security (NS) concern is identified, and applies to all applications and petitions that convey an immigrant or nonimmigrant status. Officers should refer to relevant guidance for instructions on adjudication of applications and petitions that do not convey an immigrant and nonimmigrant status but have a NS or egregious public safety concern.

This CARRP process is applied **by officers designated within each operational component** and involves four (4) distinct, yet not mutually exclusive, processing steps:

1. *Identifying an NS Concern:* The process of identifying and confirming whether the indicator relates to the applicant, petitioner, beneficiary or derivative (hereafter,

DEF-00431682

National Background, Identity, and Security Check Operating Procedures

"individual"[36]), and whether there is an articulable link between the individual and activities, individuals or organization described in section 212(a)(3)(A), (B) or (F) or 237(a)(4) (A) or (B) of the Act (related to national security).

2. *Internal Vetting and Assessing Eligibility in Cases with NS Concerns:* If it is determined that an NS concern exists, the case is forwarded to a designated officer for a thorough review of the record associated with the application/petition to determine if the individual is eligible for the benefit sought.

3. *External Vetting of NS Concerns:* If after completion of the eligibility assessment and internal vetting, the individual appears eligible for the benefit sought, or if field management determines further processing is necessary to strengthen or support a decision, the application/petition proceeds to the External Vetting stage. The field is responsible for external vetting of all KST and Non-KST NS concerns.
    See the memo entitled "Revision of Responsibilities for CARRP Cases Involving Known or Suspected Terrorists."

4. *Adjudication of NS Cases:* The focus of this stage is to evaluate any additional information obtained during the vetting process to determine if the NS concern has been resolved or confirmed, whether the application/petition should be approved or denied, and when appropriate, to proceed with removal, rescission, termination, or revocation.

If, after completing the vetting and deconfliction processes 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 counsel and HQ counsel when appropriate.

Note: The field is NOT authorized to approve CARRP cases involving KSTs unless guidance and written approval is received from USCIS Headquarters.
Pursuant to each component's CARRP operational guidance, information on the vetting and adjudication of the NS concern is entered into the Fraud Detection and National Security Data System (FDNS-DS).

Deconfliction is of utmost importance throughout the CARRP process. Designated USCIS officers must conduct deconfliction with the appropriate law enforcement agency or record owner to ensure that any USCIS action does not adversely impact any investigative or other interest.

---

[36] For purposes of this memorandum, the term "individual" may include a petitioning company.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431683

National Background, Identity, and Security Check Operating Procedures

D.   Employment and Travel Authorization Applications with NS concerns

If an individual with an NS concern files Form I-765 and/or Form I-131, the application will be released for adjudication, even if vetting is not complete within sixty (60) days of the date that the application was received.

For stand-alone I-765 and I-131 applications, the officer should determine if the NS concern supports removal, revocation, rescission, or termination of the underlying status.

Prior to action on the application, designated officers must deconflict with the record owner(s) and/or law enforcement agency.

E.   Form I-90 with NS Concerns

A permanent resident holds lawful status and is entitled to evidence of that status until it is removed through rescission or removal proceedings. The CARRP process does not apply to I-90 applications. Officers should refer to the February 9, 2009, policy memorandum entitled "Revised Guidance Pertaining to the Adjudication of Form I-90, Application to Replace Permanent Resident Card" for instructions on adjudication of I-90 applications. This policy memorandum revised the guidelines for adjudicating the I-90 application established in Policy Memorandum 110 (PM 110).

The revised policy establishes that Form I-90 and Form N-565 will be adjudicated when the following conditions have been met:

- The applicant has established his or her identity;
- It has been established that the applicant is a lawful permanent resident; and
- Security checks are completed and valid at the time of adjudication.

Any derogatory information received as a result of the security checks will be resolved **only after** the adjudication of the I-90 application. The issuance of the Form I-551, Permanent Resident Card, Certificate of Citizenship, or Certificate of Naturalization must not be delayed due to any pending resolutions. The adjudication of such cases will no longer be suspended as provided in PM 110.

F.   Santillan (EOIR Grants) with NS Concerns

Santillan class members are those who have been granted permanent resident status by the Executive Office of Immigration Review (EOIR) and who have not been issued evidence of their

179

National Background, Identity, and Security Check Operating Procedures

status. These individuals are currently covered by the terms of the injunction order issued on December 22, 2005 (published at 2005 WL 3542661).[37] The injunction mandates that USCIS issue documentation of permanent resident status to class members within a specific time frame from the date of the class member's InfoPass appointment with USCIS after he or she receives the EOIR grant. Generally, the documentation must be issued within 30 days, if the status was granted on or after April 1, 2005, or 60 days, if the status was granted before April 1, 2005. USCIS is bound by the terms of the injunction regardless of NS concerns and must follow the procedures outlined in the December 29, 2005 memorandum on interim guidance. If NS concerns remain after issuance of the Permanent Resident Card, the case should be referred to the local FDNS component.

G.   Request for Assistance to HQFDNS National Security Immigration Vetting Division (IVD), National Security and Vetting Branch (NSVB)

The field may contact HQFDNS for assistance during the processing of an application/petition with an NS concern. Prior to requesting assistance from HQ FDNS-NSVB, the Designated Officer must:

- Complete all internal vetting and the initial eligibility assessment
- Obtain local management approval prior to sending a RFA request
- Make sure the system generated BCAA is complete
- Create an NSVB RFA (HQ RFA) record after the required management approval

Refer to the current FDNS-DS User Guide regarding how to complete a RFA request via the Special Actions Sub Tab in FDNS-DS.

---

[37] This memorandum complements the guidance contained in the December 29, 2005 memorandum entitled "Interim Guidance for Processing of Status Documentation for EOIR-adjusted Lawful Permanent Residents Pursuant to the Permanent Injunction in Santillan," et al. No. C-04-2686 (N.D. CA Dec. 22, 2005), as well as the March 31, 2005 memorandum entitled Executive Office for Immigration Review (EOIR) Processing, and the April 8, 2005, memorandum entitled "Clarification of Memorandum Executive Officer for Immigration Review (EOIR) Processing."

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431685

National Background, Identity, and Security Check Operating Procedures

X.   Resolution: Egregious Public Safety Concerns & Other Criminal Cases

A.   Egregious Public Safety (EPS) Policy and Guidance

In 2011, USCIS signed a Memorandum of Agreement between USCIS and United States Immigration and Customs Enforcement (ICE) on the issuance of Notices to Appear to aliens encountered during an adjudication. The accompanying policy memorandum, entitled "Revised Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Removable Aliens" dated November 7, 2011, has been referred to as the New NTA Policy Memorandum. However, this memo has since been superseded by two (2) companion policy memorandums: PM-602-0050.1, entitled "Updated Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Deportable Aliens," dated June 28, 2018, and (for DACA cases) PM-602-0161, entitled "Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) When Processing a Case Involving Information Submitted by a Deferred Action for Childhood Arrivals (DACA) Requestor in Connection With a DACA Request or a DACA-Related Benefit Request (Past or Pending) or Pursuing Termination of DACA," dated June 28, 2018.

The NaBISCOP adopts the procedures outlined in PM-602-0050.1 and PM-602-0161. Refer to component-specific guidance for additional information. General procedural information related to the background check process for NTAs will be added to the NaBISCOP upon completion.

B.   EPS Case Definition

An EPS case is defined as any case where information indicates the alien is under investigation for, has been arrested for (without disposition), or has been convicted of any of the following:
- Murder, rape, or sexual abuse of a minor as defined in 101(a)(43)(A) INA;
- Illicit trafficking in firearms or destructive devices as defined in 101(a)(43)(C) INA;
- Offenses relating to explosive materials or firearms as defined in 101(a)(43)(E) INA;
- Crimes of violence for which the term of imprisonment imposed or where the penalty for a pending case is at least one year as defined in 101(a)(43)(F) INA;
- An offense relating to the demand for or receipt of ransom as defined in 101(a)(43)(H) INA;
- An offense relating to child pornography as defined in 101(a)(43)(I) INA;
- An offense relating to peonage, slavery, involuntary servitude, or trafficking in persons as defined in 101(a)(43)(K)(iii) INA;
- An offense relating to alien smuggling as described in 101(a)(43)(N) INA;
- Human Rights Violators, known or suspected street gang members, or INTERPOL hits; or
- Re-entry after an order of exclusion, deportation, or removal subsequent to conviction for a felony where a Form I-212, Application for Permission to Reapply for Admission into the U.S. after Deportation or Removal, has not been approved.

181

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP––in whole or in part––unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Arrests without Disposition for above Offenses

The MOA between USCIS and ICE indicates that, even without a conviction, an alien may be an EPS case if there has been an arrest "without disposition." This applies specifically to an arrest where charges are still **pending**. If the alien was arrested but the charges were dropped or the alien was acquitted, the case will not be referred under this provision of the MOA. Also, if an arrest was for an offense described above, but the conviction was ultimately for an offense not defined as an EPS case, the case will not be referred under this provision of the MOA.

C.   EPS Adam Walsh Act

The Adam Walsh Act (AWA) prohibits U.S. citizens and LPRs who have been convicted of certain "specified offenses against a minor" from filing a family based immigration petition on behalf of any beneficiary. Besides guidance in this SOP, vetting officers should also follow procedures in the February 8, 2007, memorandum entitled "Guidance for Adjudication of Family-Based Petitions and I-129F Petition for Alien Fiancé(e) under the Adam Walsh Child Protection and Safety Act of 2006," and the SOP for the adjudication of family-based petitions under the Adam Walsh Act signed by Acting Associate Director Donald Neufeld on September 24, 2008.

D.   International Marriage Broker Regulation Act

If certain criminal convictions are revealed during the adjudication of a K nonimmigrant visa for an alien fiancé(e) (K-1) or alien spouse (K-3), adjudicators should follow the guidance in the July 21, 2006, memorandum entitled "International Marriage Broker Regulation Act Implementation Guidance".

E.   Referral to ICE (RTI) for EPS Case

EPS cases must be referred to ICE for possible removal proceedings prior to adjudication, subject to the following procedures:

- Suspend adjudication for 60 days, or until ICE provides notification of its action on the case, whichever is earlier.[38]
- Refer case immediately to the appropriate officer or unit for creation of a RTI.
  - Service Centers and the NBC: Route immediately to appropriate BCU/FDNS- OPS.
  - Field Offices: Route immediately to the FDNS-IO or other authorized officer in accordance with local policy.

The appropriate officer or unit conducts the following:

---

[38] 8 CFR 103.2(b)(18)

National Background, Identity, and Security Check Operating Procedures

1. Prepare RTI.
   o The RTI should include any relevant attachments that USCIS has at the time, such as a copy of the IdHS (formerly known as RAP sheet), arrest disposition, a copy of the application.
   o If certified conviction records are available in the file, include those records, but do not hold an RTI to obtain them.
2. Update FDNS-DS as appropriate.
3. Forward a copy of the RTI to appropriate ICE office.
   o Service centers and the NBC forward a copy to the ICE Benefit Fraud Unit (BFU).
   o Field offices forward a copy to the local ICE Special Agent in Charge (SAC).
4. Place a hard copy of the RTI in the A-file or Receipt file.
5. Update appropriate systems as required by local guidance (CLAIMS).
6. Retain the file unless ICE requests it or 60 days expire from the time the referral is received by ICE.

IF	THEN
ICE does not respond within 60 days,	Resume adjudication, taking into account the basis for the RTI.
ICE declines the RTI,	Resume adjudication, taking into account the basis for the RTI.
ICE accepts case,	Deconflict prior to adjudication and provide assistance to ICE where appropriate.

1. USCIS retains discretion to formally place the case in abeyance for ICE to conduct further investigation.
2. Complete resolution memorandum referencing the content of the RTI and response (if any) from ICE prior to any local adjudicative action.
3. Update appropriate systems as required by local guidance (CLAIMS).

F.   Referral to ICE for Other Criminal Cases

In all cases in which it appears that the alien is inadmissible or removable for a criminal offense not included in the EPS case list, USCIS will complete the adjudication prior to referring the case to ICE. ICE will decide whether and how it will institute proceedings and whether or not they will detain the alien.

Once adjudication is completed immediately refer the case to the appropriate officer or unit for creation of a RTI.
- Service Centers and the NBC: Route immediately to appropriate BCU.
- Field Offices: Route immediately to the FDNS-IO or other authorized personnel in accordance with local policy.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

The appropriate officer or unit conducts the following:
1. Prepare RTI.
   - The RTI should include any relevant attachments that USCIS has at the time, such as a copy of the IdHS (formerly known as RAP sheet), arrest disposition, a copy of the application.
   - Where USCIS obtains certified conviction records through normal processing of the application, include those records but do not hold an RTI on a completed case to obtain those records.
2. Update FDNS-DS as appropriate.
3. Forward a copy of the RTI and the accompanying file, if in the possession of the office or center issuing the RTI, directly to the appropriate ICE field operations director (FOD) or designated POC.
4. Concurrently transmit a copy of the RTI to ICE HQDRO Criminal Alien Division at ██████████████████████ @ice.dhs.gov for statistical monitoring purposes.

G.   Exceptions to EPS RTI Criteria

A case that otherwise meets the referral criteria should not be referred to ICE, but should be resolved by the BCU, FDNS-IO, or designated officer, when the subject:
   - Was removed/excluded and there is no reason to believe he or she has reentered the United States.
   - Was granted relief or proceedings were terminated by an Immigration Judge (IJ), and no new qualifying crimes (which qualify for EPS vetting) have been reported since relief was granted/proceedings were terminated.
   - Has a pending case with the Executive Office for Immigration Review (EOIR) and no new qualifying crime which require mandatory detention.
   - Is currently in custody with an ICE detainer.
   - Is currently under an Immigration Order of Supervision, is reporting as required, and no new qualifying crime which require mandatory detention.
   - Is under final order of removal, but has not been removed.

H.   Employment and Travel Authorization Applications with EPS Concerns

If an individual with an EPS concern files Form I-765 or Form I-131, the officer will suspend adjudication for no more than sixty (60) days from the date the file is received by ICE, or until ICE provides notification of its intended action(s), whichever date is earlier.

I.   Form I-90 with EPS Concerns

An applicant who is a Lawful Permanent Resident (LPR) holds such status unless it is:

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431689

National Background, Identity, and Security Check Operating Procedures

1. Abandoned by the applicant,
2. Revoked through rescission and/or removal proceedings, or
3. Superseded by naturalization.

Otherwise, the applicant is entitled to evidence of his or her status. All I-90 applications will be adjudicated when all of the filing requirements and the following conditions have been met:

1. The applicant has established his or her identity; and
2. It has been established that the applicant is a lawful permanent resident.

Please note that officers must ensure that fingerprint checks and TECS checks have been initiated, completed, and are valid at the time of adjudication of the I-90; however, any derogatory information received as a result of these checks are to be resolved only after the adjudication of the I-90.

Similarly, I-90 applications with associated EPS concerns are to be adjudicated pursuant to the above-mentioned instructions before an ICE referral is made. The I-90 adjudication must not be suspended due to any EPS concerns. An I-90 that meets the definition of an EPS case will be referred to ICE pursuant to established procedures only after the adjudication of the I-90 has been completed.

For further information, please see the February 9, 2009, policy memorandum signed by Donald Neufeld revising the guidelines for the adjudication of I-90 application for further information. The memo may be accessed by clicking the following link, "Revised Guidance Pertaining to the Adjudication of Form I-90, Application to Replace Permanent Resident Card". (This policy memorandum revised the guidelines for adjudicating the I-90 application established in Policy Memorandum 110 (PM 110).

J.   Santillan (EOIR Grants) with EPS Concerns

Santillan class members are those who have been granted permanent resident status by the Executive Office of Immigration Review (EOIR) and who have not been issued evidence of their status. These individuals are currently covered by the terms of the injunction order issued on December 22, 2005 (published at 2005 WL 3542661).[39] The injunction mandates that USCIS issue documentation of permanent resident status to class members within a specific time frame from the date of the class member's InfoPass appointment with USCIS after he or she receives the EOIR grant. Generally, the documentation must be issued within 30 days, if the status was granted on or after April 1, 2005, or 60 days, if the status was granted before April 1, 2005.

---

[39] This memorandum complements the guidance contained in the December 29, 2005 memorandum entitled, Interim Guidance for Processing of Status Documentation for EOIR-adjusted Lawful Permanent Residents Pursuant to the Permanent Injunction in Santillan, et al. No. C-04-2686 (N.D. CA Dec. 22, 2005), as well as the March 31, 2005 memorandum entitles Executive Office for Immigration Review (EOIR) Processing, and April 8, 2005 memorandum entitled Clarification of Memorandum Executive Officer for Immigration Review (EOIR) Processing.

185

National Background, Identity, and Security Check Operating Procedures

USCIS is bound by the terms of the injunction regardless of EPS concerns and must follow the procedures outlined in the December 29, 2005, memorandum on interim guidance. If EPS concerns remain after issuance of the Permanent Resident Card, the case should be referred to the local FDNS component.

186
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

XI.   Resolution: Immigration Fraud

A.   Immigration Benefit Fraud Policy and Guidance

USCIS has signed a Memorandum of Agreement between USCIS and United States Immigration and Customs Enforcement (ICE) on the Investigation of Immigration Benefit Fraud in September 2008. Officers should refer to the Fraud Detection Standard Operating Procedures dated December 6, 2019 for explanations of commonly encountered immigration fraud and for an in-depth understanding of the referral process to FDNS and to ICE which can be found under the FDNS ECN Page.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431692

<u>National Background, Identity, and Security Check Operating Procedures</u>

XII.   Security Checks Required for Issuance of Form I-862 — Notice to Appear and Form I-863 — Notice of Referral to an Immigration Judge

A. Form I-862 - Notice to Appear (NTA) and Form I-863 — Notice of Referral to an Immigration Judge

Form I-862, *Notice to Appear* (NTA), is filed with the Executive Office of Immigration Review (EOIR) in order to commence removal proceedings under section 240 of the INA. USCIS was delegated the authority by the Secretary of the U.S. Department of Homeland Security (DHS) to issue Form I-862, *Notice to Appear* in order to initiate removal proceedings. See *Delegation by the Secretary of the Department of Homeland Security to the Bureau of Citizenship and Immigration Services, Delegation Number 0150.1; Paragraph II(N)*. This delegation did not extend to International District Directors and officers, who are not authorized to issue NTAs. U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP) also have legal authority to issue NTAs. As such, USCIS must ensure that issuance of NTAs fits within and supports the Department's overall removal priorities – promoting national security and the integrity of the immigration system.

On January 25, 2017, the President issued Executive Order (EO) 13768 *Enhancing Public Safety in the Interior of the United States*. EO 13768 sets forth the President's immigration policies for enhancing public safety and articulates the priorities for removal of aliens from the United States. Additionally, EO 13768 instructs that the government will no longer exempt classes or categories of removable aliens from potential enforcement.

On February 20, 2017, the DHS Secretary issued an implementation memorandum related to the President's immigration enforcement priorities entitled, *Enforcement of the Immigration Laws to Serve the National Interest*. The memorandum sets forth guidance for all DHS personnel regarding the enforcement priorities.

On June 28, 2018, the USCIS Director issued *PM-602-0050.1, Updated Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Deportable Aliens*. PM 602-0050.1 provides updates to USCIS guidelines for referring cases to ICE and issuing NTAs. PM 602-0050.1 supersedes the November 7, 2011, PM-602-0050, *Revised Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Removable Aliens*.[40]

---

[40] With the noted exception relating to Deferred Action for Childhood Arrivals (DACA) cases. When adjudicating or taking adverse action in a DACA case, officers must continue applying the November 7, 2011 PM 602-0050. See

188

National Background, Identity, and Security Check Operating Procedures

On December 26, 2018, the Director issued the Memoranda *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance* and *Departure-Related Systems Checks Requirement Preceding Notice to Appear (NTA) Issuance* in order to clarify security checks and systems checks requirements for officers when reviewing for potential NTA issuance. The Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance,* expressly rescinded and superseded the previous security check requirements guidance *Security Check Requirements Proceedings Notice to Appear Issuance*, dated March 2, 2004.

Law enforcement and criminal history background checks (collectively referred to here as "security checks") routinely identify a significant number of national security threats, public safety risks, aliens not lawfully present in the United States, aliens who have engaged in fraud or willful misrepresentation in connection with any official matter or application before a governmental agency, and aliens subject to other grounds of removal. Completion of security checks during the course of adjudications provides an early opportunity for USCIS to determine eligibility, identify potential national security and public safety risks, and discover any relevant and potential grounds for removal prior to initiating removal proceedings. USCIS initiates security checks immediately prior to NTA issuance in order to assess any changes in security check results that may impact or inform the issuance of an NTA, provide up-to-date records, and help ensure that the EOIR and ICE are fully informed regarding both an alien's immigration history and any criminal background. USCIS conducts departure-related systems checks immediately prior to NTA issuance to determine whether an alien departed the United States, thereby supporting the Department's overall removal priorities while simultaneously supporting the ability of EOIR to control its dockets and prioritize cases for removal.

USCIS officers must either initiate or complete, as described below and subject to the current age restrictions, the following checks: FBI Fingerprint Checks, TECS/NCIC checks, FBI Name Checks, and any departure-related systems check intended to determine whether an alien departed the United States (i.e., Arrival and Departure Information System (ADIS) checks or Unified Passenger (UPAX) system checks). These security checks and systems checks required for NTA issuance are the baseline requirements for screening and vetting immediately prior to NTA issuance. Local policies and procedures may require additional security checks pursuant to local OCC, SOPs, adjudication guides, or agreements with ICE. Furthermore, the security checks

---

PM 602-0161 *Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) When Processing a Case Involving Information Submitted by a Deferred Action for Childhood Arrivals (DACA) Requestor in Connection With a DACA Request or a DACA-Related Benefit Request (Past or Pending) or Pursuing Termination of DACA*, dated June 28, 2018.

189

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

required for NTA issuance are *in addition* to any security checks that may be required by USCIS for adjudication of an application, petition, or benefit request. Nothing in the NaBISCOP is intended to supersede, negate, or replace any particular local guidance. If there is a contradiction or a perceived contradiction between NaBISCOP security checks and a local policy regarding NTA issuance, officers should raise that to their chain of command and/or local OCC.

USCIS officers working in Refugee, Asylum, and International Affairs (RAIO) Directorate, should consult with OCC or RAIO leadership to determine which security checks and systems checks contained in this section of NaBISCOP must be completed, or merely initiated, prior to NTA issuance for aliens who are in custody (detained). These cases proceed on a different path to EOIR than NTAs issued by other directorates, such as Field Office Directorate (FOD) or Service Center Operations (SCOPS).

B. FBI Fingerprint Check Requirement

The Federal Bureau of Investigation (FBI) Fingerprint check results provide summary information of an individual's administrative or criminal record within the United States. FBI Fingerprint checks will often include immigration enforcement information as well. FBI Fingerprint check results are currently returned in the form of an Identity History Summary (IdHS), formerly known as a Record of Arrest and Prosecution (RAP Sheet). The IdHS describes arrests and, when available, subsequent dispositions attributable to that individual. For USCIS, criminal history record information (CHRI) is important to determine both eligibility for any underlying immigration benefit request as well as all appropriate charges to be listed in the Notice to Appear (NTA). For detailed information on FBI Fingerprint Checks see NaBISCOP Section VII. Security Check: FBI Fingerprint Check.

As a general rule, USCIS must have a *valid* FBI Fingerprint result *prior* to NTA issuance, subject to the guidance below. *See* Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018. Pursuant to Section VII of this NaBISCOP, a particular "fingerprint result expires 15 months after the date of the FBI response." *See* NaBISCOP Section VII. Security Check: FBI Fingerprint Check, Part F.

NOTE: Regarding the biometrics services fee, USCIS has the authority to collect a biometrics services fee under 8 CFR 103.17 for any biometric collection pertaining to "requests for benefits." However, Form I-862 and I-863 are not requests for benefits. Consequently, USCIS is *not* authorized to collect the biometric services fee when scheduling an alien for biometrics collection associated with Form I-862.

National Background, Identity, and Security Check Operating Procedures

1. Age-related Exemptions

Presently, USCIS is limited in the collection of biometrics or fingerprints to certain age groups by regulation, depending on the particular application or petition filed.[41] Further, even in cases where USCIS is permitted to collect fingerprints for individuals under 14, the FBI may not return CHRI pertaining to juvenile adjudications. Finally, the current language of 8 CFR 236.5 appears to limit fingerprint collection associated with commencing removal proceedings to aliens "14 years of age or older."[42] For these reasons, depending on the underlying application or petition filed with USCIS and the age of the alien, USCIS may not have the authority to require an alien to submit biometrics or fingerprints *solely* in order to issue an NTA.

If USCIS already has the biometrics of an alien under the age of 14 due to a previously filed application or petition, officers must resubmit or "refresh" those fingerprints to the FBI prior to NTA issuance in order to obtain an updated IdHS for the alien and satisfy the required NTA security checks.

If USCIS never previously collected the biometrics of an alien under the age of 14, USCIS may not have the legal authority to request biometrics solely to issue the NTA. In these cases, officers should request guidance through their chain of command and/or local OCC prior to issuing an ASC notice for Form I-862.

2. Validity of Results from FBI Fingerprint Checks

Fingerprints are one of many biometric modalities collected by USCIS. Fingerprints themselves never expire. FBI Fingerprint *results,* also referred to as an IdHS, do expire. Presently, IdHS are only valid for 15 months from the date of the FBI response. See NaBISCOP Section VII, Part F, Validity of Results from FBI Fingerprint Checks. NaBISCOP contains a general prohibition against reusing fingerprint results from one form type to another. See NaBISCOP Section VII, Part F, Validity of Results from FBI Fingerprint Checks. NaBISCOP clearly states that "Fingerprints must be obtained for each application filed that requires the biometrics be captured…" See NaBISCOP Section VII, Part F, Validity of Results from FBI Fingerprint Checks.

However, this general prohibition against reusing fingerprint results from one application or form type to another does not apply to NTAs since Form I-862 and I-863 are not benefit requests submitted by an alien. Fingerprints previously collected by USCIS for an application, petition, or

---

[41] See 8 CFR §235.1(f)(1)(iv)(A) requirement to provide biometric identifiers does not apply to "aliens younger than 14 or older than 79 on date of admission"; 8 CFR §264.2(d) requiring that after filing an application, each applicant 14 years of age or older shall be fingerprinted as prescribed in 8 CFR 103.16; 8 CFR §264.5(b)(8) requiring permanent residents to file for a replacement Permanent Resident Card when they reach the age of 14 years ensuring the child is fingerprinted as required under INA 262; 8 CFR 245a.4(b)(5) requiring fingerprint card for applicants 14 years and older; and 8 CFR 210.2(c)(2)(i) requiring submission of fingerprints for special agricultural workers age 14 and older.

[42] See 8 CFR 236.5 "Every alien 14 years of age or older against whom proceedings based on deportability under section 237 of the Act are commenced under this part by service of a notice to appear shall be fingerprinted and photographed."

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431696

National Background, Identity, and Security Check Operating Procedures

benefit request may be re-submitted to the FBI or "refreshed" in order to comply with security check requirements for NTA issuance. As a matter of course, only complete sets of fingerprints that previously yielded an IDENT or Non-IDENT response may be re-used for NTA issuance. Solely in the context of NTA issuance, these fingerprints are re-submitted to the FBI, at no cost to the alien, in order for USCIS to obtain an updated fingerprint result/IdHS in order to satisfy the security check requirements for NTA issuance.

The validity period for FBI fingerprint results is calculated from the date of the FBI fingerprint response on the IdHS to the date of potential NTA issuance—*not* the time of final adjudication of the underlying application, petition, or benefit request. In other words, FBI fingerprint results may have been valid at the time of final adjudication and expired in the period prior to NTA issuance. If an IdHS was valid at the time of the denial, but expired by the time an officer is reviewing for potential NTA issuance, the fingerprints must be refreshed to obtain a valid result.

There are several scenarios for FBI fingerprint checks that an officer may encounter when conducting security checks prior to NTA issuance. Where the alien's previous fingerprint result/IdHS:

- Is less than 15 months old. The officer will use the last fingerprint result/IdHS from the underlying application, petition, or benefit request to satisfy the security check requirements for NTA issuance. There is no need to refresh these fingerprint results.
- Is 15 months old or older. The officer will resubmit or "refresh" the last valid fingerprints in order to generate an updated fingerprint result/IdHS to satisfy the security check requirements for NTA issuance. The officer must follow the standard procedures for submitting a request to resubmit or "refresh" the expired fingerprint results, just as the officer would for fingerprint results that expire prior to the adjudication of an open application or petition. The officer is not limited to only "refreshing" the fingerprints from the underlying or "last" application, petition, or benefit request, rather the officer can request a "refresh" of any fingerprints collected by USCIS that previously yielded an IDENT or Non-IDENT response from the FBI. When refreshing fingerprints for NTA issuance, officers must change the "form type" in the dropdown list in CPMS from whatever the underlying form type was, to select Form I-862, *Notice to Appear*. This will simplify data and tracking of fingerprint refreshes conducted in order to issue an NTA.
- Was never generated. In some cases, USCIS never collected an alien's fingerprints in the past or only collected a single press-print due to the particular biometrics requirement of a previous application, petition, or benefit request. Consequently, there will be no valid set of fingerprints for the officer to resubmit or "refresh" with the FBI. In these cases, the officer must issue an ASC appointment notice and schedule the alien for biometrics collection at the next available date and time. Relevant facts to note:

192

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP—in whole or in part—unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431697

National Background, Identity, and Security Check Operating Procedures

- USCIS considers issuance of an ASC appointment notice as satisfying the requirement at 8 CFR 1003.47(e) that USCIS "initiate" relevant security checks prior to NTA issuance.
- The ASC appointment notice must reflect that biometrics are requested for Form I-862 – *Notice to Appear*. This will simplify data and tracking of ASC appointments scheduled in order to issue an NTA.
- The officer will not delay NTA issuance in order to ascertain if the alien appeared for biometrics collection at the scheduled ASC appointment.
- Requests to reschedule ASC appointments issued for Form I-862 are not favored.
- USCIS is *not* authorized to collect the biometric services fee when scheduling an alien for biometrics collection associated with Form I-862.

Questions or concerns about whether or not an officer can or should refresh a particular alien's previous fingerprint results or schedule an alien for biometrics collection at an ASC in order to satisfy security checks prior to NTA issuance, should be raised through the chain of command and/or local OCC.

C. TECS/NCIC Checks Requirement

TECS (formerly known as the Treasury Enforcement Communications System) is an automated enforcement and inspection lookout system maintained by CBP. The National Crime Information Center (NCIC) is a database maintained by the FBI. NCIC contains lookout information posted by federal, state, and local governmental agencies. Security checks have been expanded to include TECS on individuals seeking immigration benefits and travel documents. USCIS personnel regularly use TECS/NCIC checks to: identify individuals who may pose a risk to national security and/or public safety, identify aliens who may be present in the United States without lawful immigration status, identify aliens who are subjects of current criminal investigations, prevent ineligible aliens from obtaining immigration benefits, screen for active arrest warrants, and identify registered sex offenders in accordance with the Adam Walsh Act. For detailed information on TECS/NCIC checks, including individuals who must be queried, name and date of birth variation requirements, and properly documenting queries.

Subject to the guidance below, USCIS officers[43] must conduct TECS/NCIC security checks an alien immediately *prior* to NTA issuance. *See* Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018. Different directorates generate, process, and issue NTAs differently.

---

[43] For credible fear cases interviewed by RAIO's Asylum Division, the aliens are detained prior to NTA issuance. ICE runs TECS/NCIC checks on these aliens prior to any release. Therefore, this requirement does not apply to aliens in the credible fear context.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

- For RAIO's Asylum Division, the TECS/NCIC security check must be conducted and the results reviewed either at the time the NTA is generated by the Asylum Officer or at the time the NTA is served on the alien. Asylum Offices may choose to conduct and review the TECS/NCIC security check at both points in time but are not required to do so.
- For all other divisions and directorates, the phrase "immediately prior to NTA issuance" means the TECS/NCIC check must be conducted and the results reviewed on the same day as serving the NTA. Offices may choose to also conduct the TECS/NCIC check when the file is initially reviewed for possible NTA issuance or at the time the NTA is generated where that date is different than the date the NTA is served, but this guidance only requires the TECS/NCIC check on the same day as serving the NTA.

Different applications, petitions, or benefit requests may require additional individuals to be queried in TECS/NCIC prior to an adjudication (i.e., a spousal petitioner, derivatives, adult household members, etc.), for purposes of conducting security checks prior to NTA issuance only the alien who will receive the NTA needs to be queried. However, this necessarily includes all appropriate name and date of birth variations for that alien. The standard requirements for documenting TECS/NCIC queries, hits, and resolutions still apply to TECS/NCIC security checks conducted prior to NTA issuance.

1. Age-related Exemptions

Pursuant to NaBISCOP Section V, Part D TECS Person Query Procedures, TECS and NCIC security checks will be run on subjects "age 14 and over" prior to NTA issuance. TECS queries are not required on subjects under age 14 when conducting security checks prior to NTA issuance.

When calculating whether an alien is "age 14 and over" for purposes of security checks prior to NTA issuance, officers should calculate the alien's age at the time of possible NTA issuance, *not* the alien's age at the time of the denial of the underlying application, petition, or benefit request. Consequently, an alien may "age in" to TECS and NCIC security checks due to the passage of time between the issuance of a denial and review for potential NTA issuance.

2. Validity of Results from TECS/NCIC Checks

The validity period for a TECS/NCIC query is 180 calendar days, as stated in the memorandum entitled "Extension of the Interagency Border Inspection System (IBIS) Record Check Validity Period" dated April 26, 2006 ("2006 IBIS memorandum) and this NaBISCOP. *See* NaBISCOP Section-V, Part I - Validity of Results from TECS Queries. Notably, this interoffice memorandum expressly superseded the March 1, 2006 IBIS SOP policy which previously established the TECS/NCIC query validity period of 90 days. Further, the Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA)*

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Issuance, dated December 26, 2018, rescinded the previous guidance on this issue which memorialized that TECS/NCIC checks were valid for 90 days when conducting security checks prior to NTA issuance. *See* Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018. Because the 2006 IBIS memorandum remains valid and the 2004 NTA Security Checks memorandum was rescinded by the Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018, the validity period for TECS and NCIC security checks is now uniformly established at 180 days.

Officers must query an alien specifically for the purpose of conducting security checks prior to NTA issuance and *not* simply rely on TECS/NCIC results conducted at the time the underlying application, petition, or benefit request was denied—even where those previous TECS/NCIC queries are less than 180 days old. Consistent with other TECS/NCIC queries, they are run at distinct times and documentation is retained in the A-file/receipt file. NaBISCOP requires that TECS/NCIC checks be run at the time of NTA issuance. *See* NaBISCOP, Section V, Part I – Validity of Results from TECS Queries. Furthermore, the 2018 Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, clearly mandates that USCIS officers "must conduct" TECS/NCIC security checks expressly for the purpose of NTA issuance.

According to the 2018 Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, officers must re-query a subject in the interests of obtaining up-to-date derogatory information solely for the purpose of issuing an NTA. If new derogatory information is discovered, then it must be resolved prior to NTA issuance and according to existing guidance. However, if no new derogatory information is discovered, officers are not required to re-resolve TECS/NCIC hits if the previous resolution is otherwise valid. Consequently, depending on the outcome of the TECS/NCIC checks, officers may only need to resolve new or subsequent derogatory information for purposes of NTA issuance. Further, while officers are required to re-query the name and date of birth combinations on the ROIT for NTA issuance, if no subsequent derogatory information is discovered, there is no prohibition against revalidating or recertifying the TECS/NCIC resolutions from the time of denial pursuant to local policies and procedures.

Questions or concerns about whether or not an officer must re-query names and dates of birth or may revalidate a previous TECS/NCIC resolution in order to satisfy security checks prior to NTA issuance, should be raised through the chain of command and/or local OCC.

D. FBI Name Check Requirement

The FBI's National Name Check Program (NNCP) researches and disseminates, in accordance with applicable laws and policies, information contained in FBI files in response to Name Check

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

requests.

LE

LE

LE   In most instances where
a positive response exists, it is returned to USCIS in the form of a Letterhead Memorandum
(LHM). Similar to a TECS/NCIC hit, a positive FBI Name Check result must be resolved by
USCIS prior to adjudication of the application/petition. For detailed information on FBI Name
Checks, including required form types and individuals who require them, see NaBISCOP Section
VI. Security Check: FBI Name Check.

FBI Name Checks must be completed or initiated, based on the underlying benefit request, prior
to NTA issuance subject to the guidance below.

1. Age-related Exemptions

FBI Name Checks are required for several forms filed with USCIS.[44] For all underlying
adjudications that require FBI Name Checks, the requirement applies for each applicant age 14
and older at the time of adjudication, without any upper-age limit,[45] who submits their
application from inside the United States. *See FBI Name Checks and Process Clarification for
Domestic Operations*, dated December 21, 2006.
While no express authority exists with respect to applicants who "age in" to FBI Name Checks
for purposes of NTA issuance, officers will be required to manually request FBI Name Checks
for this population of aliens. Without regard to NTA issuance, guidance states that, "if an
applicant is less than 14 years of age at the time of filing, but turns 14 years old while the
application is pending, then a name check is required." See *FBI Name Checks and Process
Clarification for Domestic Operations*, dated December 21, 2006. If an applicant can "age in" to
FBI Name Checks for purposes of an adjudication, then it logically follows that applicants can
"age in" to FBI Name Checks for purposes of NTA issuance. As such, in cases where an
applicant turns 14 years of age *subsequent* to their underlying denial but *prior* to possible NTA
issuance, officers must manually request an FBI Name Check for that alien in order to satisfy the
security checks for NTA issuance.

2. Validity of Results from FBI Name Checks

---

[44] Presently there is a discrepancy in resources listing the forms that require FBI Name Checks security vetting for
underlying applications. *FBI Name Checks and Process Clarification for Domestic Operations* dated December 21,
2006, lists seven forms, while NaBISCOP lists 11, and CLAIMS3 is automatically sending data on two additional
forms to the FBI. The NaBISCOP Advisory Panel is working to resolve this issue.
[45] On noted exception is Form I-485 – *Application to Register Permanent Residence or Adjust Status*, which has an
upper-age limit of 80 years old. See *FBI Name Checks and Process Clarification for Domestic Operations*, dated
December 21, 2006.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

"A completed name check or an initiated name check is required ***prior*** to issuance of a Notice to Appear." *See FBI Name Checks and Process Clarification for Domestic Operations*, dated December 21, 2006 and Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018. Officers will be confronted with two scenarios with respect to FBI Name Checks for NTA issuance: 1) cases where the underlying benefit request required an FBI Name Check result as part of that adjudication; and 2) cases where the underlying benefit request did not require an FBI Name Check as part of that adjudication.

For those underlying applications and petitions where an FBI Name Check was already completed as part of that adjudication,[46] a new name check is not required before issuing a Form I-862 or Form I-863. *See* Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018.

However, most of the applications, petitions, and benefit requests filed with USCIS do not require FBI Name Checks as a security check. In these cases, where the underlying adjudication did not require an FBI Name Check as a security check, officers must manually request an FBI Name Check in order to satisfy security checks prior to NTA issuance. *See* Memorandum *Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018.

Questions or concerns about whether or not an officer may rely on a previous FBI Name Check result or whether they must manually request a new FBI Name Check in order to satisfy security checks prior to NTA issuance, should be raised through the chain of command and/or local OCC.

E. Confirmation of an Alien's Departure Prior to NTA Issuance Requirement

Arrival and Departure Information System (ADIS)

The Visa Waiver Permanent Program Act (VWPPA) enacted on October 30, 2000, required the Attorney General to develop and implement a fully automated entry and exit control system that collected a record of arrival and departure for every alien who arrived in and departed from the United States by sea or air at a port of entry (POE). The Arrival and Departure Information System (ADIS), was initially maintained by the US-VISIT Program to achieve this end. ADIS supported the goal of matching arrival and departure records so that the Office of the Attorney General could calculate, for each country, the portion of nationals of that country that arrived but for whom no record of departure existed (unconfirmed overstays), as well as those nationals for whom there were records of departure but who stayed in the United States beyond the CBP Admit Until Date (AUD) (confirmed overstays). ADIS expanded to serve as a repository for storing, reconciling, and reporting of non-U.S. citizen (USC) air and sea traveler information.

On October 1, 2002, ADIS began receiving arrival and departure data from the Advance

---

[46]*See* NaBISCOP, Section VI.

DEF-00431702

National Background, Identity, and Security Check Operating Procedures

Passenger Information System (APIS). Information received from APIS includes data from arrival and departure passenger manifests. In December 2003, ADIS began collecting adjustments to status information from the Computer-Linked Application Information Management System 3 (CLAIMS3) and the Student and Exchange Visitor Information System (SEVIS). More recently, ADIS was adapted to incorporate additional data elements and transactions associated with the Automated Biometric Identification System (IDENT) and other related immigration systems in order to maintain consistent alien travel histories. Today, ADIS maintains real-time travel histories and current immigration status on 270 million alien traveler identities. It matches departure records with arrivals to determine alien overstays, creates and stores arrival and departure records, and provides a wide range of ad hoc queries and reporting capabilities on these data.

ADIS has many functions, including: determining a traveler's immigration status, ascertaining whether an alien is an in country overstay, determining whether an alien is an out of country overstay, etc.

Unified Passenger (UPAX)

CBP's Automated Targeting System – Passenger (ATS-P) is another system containing certain departure information. ATS-P is one of a suite of Targeting and Analysis Systems Program Division (TASPD) applications that provide users with targeting, situational awareness, and decision support.

LE

LE

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431703

National Background, Identity, and Security Check Operating Procedures

<div style="border:1px solid">

LE

</div>

USCIS has the authority to issue NTAs under the immigration laws, but as a matter of policy determined that NTAs will generally not be issued against aliens who depart the United States after receiving a denial on an application, petition, or benefit request.

In the context of NTA issuance, USCIS officers[47] are required to conduct system checks in ADIS, UPAX, or any successor system in order to ascertain whether or not an alien departed the United States. *See* Memorandum *Departure-Related Systems Checks Requirement Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018. All the standard requirements for documenting ADIS and UPAX system checks and queries still apply to ADIS and UPAX checks conducted immediately prior to NTA issuance.

1. Age-related Exemptions

There are no age restrictions related to the information stored in ADIS or UPAX for alien travelers. While one of the DHS systems that feeds data elements to ADIS and UPAX is IDENT, and IDENT contains biographic information that is subject to certain regulatory age restrictions, those age restrictions do not apply directly to ADIS and UPAX. Furthermore, the specific purpose for USCIS running system checks in ADIS and UPAX is to ascertain whether an alien departed the United States prior to NTA issuance, given that particular information would be stored in ADIS or UPAX regardless of the alien's age, there are no age restrictions for conducting departure-related systems checks in ADIS and UPAX prior to NTA issuance. In other words, officers should conduct ADIS and UPAX systems checks on every alien, regardless of age, in order to determine if they departed the United States prior to issuing an NTA. *See* Memorandum *Departure-Related Systems Checks Requirement Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018.

2. Validity of Results from ADIS and UPAX System Checks

There is no express policy guidance pertaining to the validity period of queries or results from ADIS or UPAX systems checks. According to NaBISCOP, "IDENT checks do not expire. However, the best practice is to perform a check prior to final adjudication, in accordance with local and component guidance." NaBISCOP Section VIII Security Check: IDENT, Part D. ADIS is no longer part of the US-VISIT Program.

While Section VIII of NaBISCOP does not expressly include ADIS or UPAX, for purposes of conducting systems checks prior to NTA issuance, officers are required to conduct departure-

---

[47] This requirement does not apply to NTAs issued by the Asylum Division of RAIO.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

related systems checks immediately prior to NTA issuance in order to determine if the alien departed the United States subsequent to the underlying denial. This means the departure-related systems checks must be conducted and the results reviewed on the same day as serving the NTA. Offices may choose to also conduct the departure-related systems checks when the file is initially reviewed for possible NTA issuance or at the time the NTA is generated where that date is different than the date the NTA is served, but this guidance only requires the departure-related systems checks on the same day as serving the NTA. *See* Memorandum *Departure-Related Systems Checks Requirement Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018.

Any ADIS and UPAX systems checks conducted at the time the underlying denial was issued, do *not* satisfy the systems checks requirement for NTA issuance. Officers are required to conduct new ADIS and UPAX checks, subsequent to the issuance of any denial and prior to NTA issuance, in order to determine if the alien departed the United States. *See* Memorandum *Departure-Related Systems Checks Requirement Preceding Notice to Appear (NTA) Issuance*, dated December 26, 2018. Further, ADIS and UPAX systems checks conducted subsequent to the underlying denial, but for a different application, petition, or benefit request, do *not* satisfy the ADIS and UPAX systems checks requirement for NTA issuance.

Questions or concerns about when an officer must conduct ADIS and UPAX systems checks prior to NTA issuance, should be raised through the chain of command and/or local OCC.

National Background, Identity, and Security Check Operating Procedures

Appendix A: Security Check Requirements by Form Type & Quick Reference

The following table shows, by form type, on which individuals USCIS personnel MUST conduct the following security checks: TECS (T), FBI Name Check (N), and FBI Fingerprint Check (F).

Form	Individual Requiring Security Check T: TECS F: FBI Fingerprint Check N: FBI Name Check						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
BONDS			T				
EOIR-29	T		T	T	T	T	Query those subjects required on the underlying petition/application type. HH members 18 years of age and older.
I-90	T, F						Derogatory information from security checks to be resolved after adjudication.
I-94	T						
I-95	T						
I-102	T						
I-129			T	T			Business entities which are employment- based petitioners do not need to be queried, including sole proprietorship operated under a business name. But sole proprietorships operated under the owner's personal name must be queried and may require an RFE or additional system checks (e.g. CLEAR/Accurint) to obtain the biographical data needed for a TECS check.
I-129F			T, F	T			Fingerprints may be required per Adam Walsh Act SOP of September 24, 2008.
I-129R Religious			T	T			Petitioner query to include any names and addresses found in the file,

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Form	Individual Requiring Security Check T: TECS F: FBI Fingerprint Check N: FBI Name Check						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
Worker							belonging to the petitioning organization.
I-129S			T	T			
I-130			T, F	T[48]	T[49]		Fingerprints may be required per Adam Walsh Act SOP of September 24, 2008.
I-131	T, F						T: Both petitioners and beneficiaries of HRIFA applications must be queried. Form is multi-purpose. Biometrics are required for applicants for a re-entry permit and refugee travel documents. An FBI Fingerprint check might be required for applicants for humanitarian parole.
I-131A	T						Officers should consult the September 29, 2016 Standard Operation Procedure for issuing Carrier Documentation. USCIS International Operations ceased issuing "Boarding Letters" with the implementation of Form I-131A.

[48] In the case of individuals residing outside the United States, depending upon the application or petition type, security checks may be performed multiple times prior to their arrival into the United States by USCIS during the adjudication and travel document issuance process: **LE**

LE

process.

[49] TECS check to be completed on the derivative spouse in the event of death of the petition beneficiary, where petition reinstatement has been requested. This does not apply to USCIS International Operations, which only adjudicates I-130 Petitions filed on behalf of immediate relatives (spouse, child, parent), who may not claim derivatives.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Form	Individual Requiring Security Check T: TECS F: FBI Fingerprint Check N: FBI Name Check						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-140			T	T	T		Business entities which are employment-based petitioners do not need to be queried, including sole proprietorship operated under a business name. But sole proprietorships operated under the owner's personal name must be queried and <u>may</u> require an RFE <u>or</u> additional system checks (e.g. CLEAR / Accurint) to obtain the biographical data needed for a TECS check.
I-191	T						
I-192	T,N,F						
I-212	T						DOS will [LE] **LE** See Section IV, Part C for more information on applications filed overseas.
I-290B	T		T	T	T	T	Query those subjects required on the underlying petition/application type.
I-360			T	T			T: Except for religious worker petitions, business entities to include sole proprietorships which are employment- based petitioners do not need to be queried. Individual persons are not considered business entities

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

| Form | Individual Requiring Security Check

T: TECS
F: FBI Fingerprint Check
N: FBI Name Check | | | | | | Special Instructions |
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
							and require a TECS Person Query (Modernized SQ11).
I-360 Religious Worker			T	T			Petitioner query to include any names and addresses found in the file, belonging to the petitioning organization.
I-485	T, N, F –		T *				- A TECS JIT check must be run on the applicant's primary name and DOB on the date of final adjudication of the form. Note: Administratively closed cases are not final adjudications and do not require a TECS JIT check. *TECS should be run on the petitioner of the family-based immigrant petition at the time of adjudication in support of the Adam Walsh Act. N: FBI Name Check not required on an individual who is more than 80 years and one day old.
I-485 Suppl. J	T						T: TECS should be run upon Supplement J submission (front end run from CLAIMS3) and again at the time of final I-485 adjudication.
I-526			T	T			
I-539	T, F				T, F		Exceptions are the following: certain A, G, and NATO nonimmigrants are not required to pay a fee, and attend a biometric appointment.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431709

National Background, Identity, and Security Check Operating Procedures

Form	Individual Requiring Security Check T: TECS F: FBI Fingerprint Check N: FBI Name Check						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
I-589	T, N, F				T, N, F		IDENT check also required.
I-590	N, F				N, F	N, F	T: DOS **LE** **LE** **LE** IRAD conducts TECS checks of U.S. based anchor and qualified family members during RAVU processing of P-3, family reunification cases. CBP conducts **LE** F: For certain refugee applicants **LE** **LE** If an I-590 Request for Reconsideration is approved, these checks must be re-run, if expired.
I-600			T,F	T,F		T,F	HH members 18 years of age and older; Beneficiaries between 14-16 years old.
I-600A	T, F					T, F	HH members 18 years of age and older.
I-601	T, N, F						Query those subjects required on the underlying petition/application type.

DEF-00431710

National Background, Identity, and Security Check Operating Procedures

Form	Individual Requiring Security Check T: TECS F: FBI Fingerprint Check N: FBI Name Check						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
							See Section IV, Part C for more information on applications filed overseas.
I-601A	T, N, F						DOS **LE** See Section IV, Part C for more information on applications filed overseas.
I-602	T						
I-612	T						
I-687	T, N, F						
I-690	T						
I-694	T						
I-698	T, N, F						
I-700	T						
I-730			T	T,N, F			T: See Section IV, Part C for more information on applications filed overseas. N: When the beneficiary is in the U.S.
I-751			T	T,F	T,F		T: Query spouse/step-parent through whom conditional residence was gained. F: * Fingerprints are required for the Conditional Permanent Resident (CPR) only (not for the USC/LPR

DEF-00431711

National Background, Identity, and Security Check Operating Procedures

Form	Individual Requiring Security Check T: TECS F: FBI Fingerprint Check N: FBI Name Check						Special Instructions
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
							through whom the CPR status acquired)[50]
I-765	T						
I-800			T,F	T,F		T,F	HH members 18 years of age and older; Beneficiaries between 14-16 years old.
I-800A	T,F					T,F	HH members 18 years of age and older.
I-817	T,F					T,F	T: Also query the legalized alien.
I-821	T,F						
I-821D		T, F					
I-824	T		T	T	T		T: Follow TECS querying procedures required by the underlying petition/application.
I-829	T,F				T,F		
I-881	T, N, F						IDENT check also required.
I-914	T, F						
I-914A	T						
I-918			T, F		T		
I-924	T*						*TECS is required on the applicant and the principals of the regional center, as well as on the address of the principal, and the name and address of the regional center.
I-924A	T*						*TECS is required on the applicant and the principals of the regional center, as well as on the address of the principal, and the name and

---

[50] Refer to the SCOPS I-751 Adjudication SOP.

207

National Background, Identity, and Security Check Operating Procedures

| Form | Individual Requiring Security Check

T: TECS
F: FBI Fingerprint Check
N: FBI Name Check | | | | | | Special Instructions |
	Applicant	Requestor	Petitioner	Beneficiary	Derivatives	Household (HH) Members	
							address of the regional center, and the name and address of any affiliated Commercial Enterprises.
N-300	T						
N-336	T						
N-400	T, N, F				T		T: Query applicant's foreign born children between the ages of 14-18. If an applicant requests a name change, query the new name also. All required TECS checks for the applicant and children (i.e., all AKAs and name variants for the applicant, primary name, and DOB for children) must be valid (no more than 180 days old) on the date of approval of the Form N-400 and on the date of the Naturalization Oath ceremony. Notwithstanding the above TECS checks, a TECS JIT check must be run on the applicant's primary name and, DOB no earlier than (2) business days prior to the date of the applicant's Naturalization Oath ceremony.
N-470	T				T		
N-565	T*						*Derogatory information from security checks to be resolved after adjudication.
N-644	T						T: Query the decedent.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

TECS Requirements by Form Type and Individual			
Form	Individual Requiring Security Check T: TECS F: FBI Fingerprint Check N: FBI Name Check		Special Instructions
	Applicant	Child	
N-600	T	T	Query the applicant as well as the parent through which U.S. citizenship is derived or acquired. If the parent or legal guardian is the applicant filing on behalf of a minor child, then query the applicant as well as the child (if over 14) who will derive or acquire citizenship.
N-600K	T	T	T: Query the applicant as well as the child (if over 14) who will naturalize. For the purpose of this form *only*, the applicant is the parent, grandparent, or legal guardian who signs/files the form on behalf of the child.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431714

National Background, Identity, and Security Check Operating Procedures

Appendix B: Description of Form Numbers

Form Number	Form Name
EOIR-29	Notice of Appeal to the Board of Immigration Appeals from a Decision of a USCIS officer
I-90	Application to Replace Permanent Resident Card
I-94	Arrival/Departure Record
I-95	Crewman's Landing Permit
I-102	Application for Replacement/Initial Nonimmigrant Arrival-Departure Document
I-129	Petition for a Nonimmigrant Worker
I-129F	Petition for Alien Fiance(e)
I-129S	Nonimmigrant Petition Based on Blanket L Petition
I-130	Petition for Alien Relative
I-131	Application for Travel Document
I-140	Immigrant Petition for Alien Worker
I-192	Application for Advance Permission to Enter as a Nonimmigrant
I-212	Application for Permission to Reapply for Admission into the United States After Deportation or Removal
I-290B	Notice of Appeal or Motion
I-360	Petition for Amerasian, Widow(er), or Special Immigrant
I-485	Application to Register Permanent Residence or Adjust Status
I-526	Immigrant Petition by Alien Entrepreneur
I-539	Application To Extend/Change Nonimmigrant Status
I-589	Application for Asylum and Withholding of Removal
I-590	Registration for Classification as Refugee
I-600	Petition to Classify Orphan as an Immediate Relative
I-600A	Application for Advance Processing of Orphan Petition
I-601	Application for Waiver of Ground of Inadmissibility
I-601A	Application for A Provisional Unlawful Presence Waiver
I-602	Application By Refugee For Waiver of Grounds of Excludability
I-612	Application for Waiver of the Foreign Residence Requirement (under Section 212(e) of the Immigration and Nationality Act, as Amended)
I-687	Application for Status as a Temporary Resident Under Section 245A of the Immigration and Nationality Act
I-690	Application for Waiver of Grounds of Inadmissibility Under Sections 245A or 210 of the Immigration and Nationality Act
I-694	Notice of Appeal of Decision Under Sections 245A or 210 of the Immigration and Nationality Act

DEF-00431715

National Background, Identity, and Security Check Operating Procedures

Form Number	Form Name
I-698	Application to Adjust Status from Temporary to Permanent Resident (Under Section 245A of Public Law 99-603)
I-700	Application for Temporary Resident Status as a Special Agricultural Worker
I-730	Refugee/Asylee Relative Petition
I-751	Petition to Remove the Conditions of Residence
I-765	Application for Employment Authorization
I-800	Petition to Classify Convention Adoptee as an Immediate Relative
I-800A	Application for Determination of Suitability to Adopt a Child from a Convention Country
I-817	Application for Family Unity Benefits
I-821	Application for Temporary Protected Status
I-823	Application - Inspections Facilitation Program
I-824	Application for Action on an Approved Application or Petition
I-829	Petition by Entrepreneur to Remove Conditions
I-881	Application for Suspension of Deportation or Special Rule Cancellation of Removal (Pursuant to Section 203 of Public Law 105-100 (NACARA))
I-914	Application for T Nonimmigrant Status
I-914A	Application for Immediate Family Member of T-1 Recipient
I-918	Petition for U Nonimmigrant Status
I-924	Application For Regional Center Under the Immigrant Investor Pilot Program
I-924A	Supplement to Form I-924
N-300	Application to File Declaration of Intention

National Background, Identity, and Security Check Operating Procedures

Form Number	Form Name
N-336	Request for a Hearing on a Decision in Naturalization Proceedings (Under Section 336 of the INA)
N-400	Application for Naturalization
N-470	Application to Preserve Residence for Naturalization Purposes
N-565	Application for Replacement Naturalization/Citizenship Document
N-600	Application for Certificate of Citizenship
N-600K	Application for Citizenship and Issuance of Certificate under Section 322
N-644	Application for Posthumous Citizenship
N-648	Medical Certification for Disability Exceptions

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Appendix C: TECS Terms Indicating Possible NS Concerns

The following tables contain certain common terms and acronyms related to TECS. The terms and acronyms in the table below may (or may not) be indicators of an NS concern, depending on the circumstances of the case. Further inquiry by the officer is needed. This list is not all inclusive.

The terms and acronyms in the tables below are additional terms and acronyms commonly encountered in TECS.

Table 1 - Common Terms and Acronyms Related to TECS

LE

213

DEF-00431718

<u>**National Background, Identity, and Security Check Operating Procedures**</u>

Table 1 - Common Terms and Acronyms Related to TECS

LE

214
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Table 1 - Common Terms and Acronyms Related to TECS

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431720

National Background, Identity, and Security Check Operating Procedures

LE

Table 2 - Additional Terms and Acronyms commonly Encountered in TECS

LE

216
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

LE

Table 3 - Other Common TECS Subject Status Codes

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Table 4 - Non-NS/PS Offenses
Although at the time of adjudication an officer may deem some or all of the offenses/violations listed below pertinent to his/her work, these offenses/violations have been deemed not to rise to the level of a threat to National Security or Public Safety (NS/PS) under current guidance. These cases should be resolved using current resolution procedures. Non-NS/PS crimes include but are not limited to:

LE

218
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Appendix D: List of Acronyms

Acronym	Description
A#	Alien Registration Number
AAO	Administrative Appeals Office
ABIS	Automated Biometric Identification System
ACD	Assistant Center Director
ACS	FBI's Automated Case System
ADIT Stamp	Alien Documentation Identification Technology Stamp
APIS	Advance Passenger Information System
APSS	Asylum Pre-Screening System
ARD	Associate Regional Director
ASCM	Application Support Center Manager
ASC	USCIS Application Support Center
ASC-ISO	Application Support Center Immigration Services Officer
ASU	Adjudication Support Unit
AUSA	Assistant United States Attorney
AWA	Adam Walsh Act
BCA	Background Check Assessment
BCAA	Background Check and Adjudicative Assessment
BCC	Border Crossing Card
BCU	Background Check Unit
BIA	Board of Immigration Appeals
BOP	Bureau of Prison
CA	Consular Affairs
CARRP	Controlled Application Review and Resolution Program
CFR	Code of Federal Regulations
CBP	U.S. Customs and Border Protection
CCD	DOS's Consular Consolidated Database
CFDO	Center Fraud Detection Operations
CIDN	Customer Identification Number
CIDR	Citizenship and Immigration Data Repository
CIS	Central Index System
CJIS	Criminal Justice Information Services
CLAIMS	Computer-Linked Applications Information Management System
CLASS	Consular Lookout and Support System (DOS)
COB	Country of Birth
COC	Country of Citizenship
CPMS	Customer Profile Management System
CRR	Case Resolution Record
DEA	Drug Enforcement Administration

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Acronym	Description
DHS	Department of Homeland Security
DNR	Does Not Relate
DOB	Date of Birth
DOS	Department of State
DRO	Detention and Removal Operations
EAD	Employment Authorization Document
EARM	ENFORCE Alien Removal Module
EDMS	Enterprise Document Management System
EOIR	Executive Office for Immigration Review
EPIC	El Paso Intelligence Center
EPS	Egregious Public Safety
ESB	Enterprise Service Bus
FBI	Federal Bureau of Investigation
FCO	File Control Office
FDNS	Office of Fraud Detection and National Security
FDNS-DS	Fraud Detection and National Security Data System
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
FPM	Fraud Prevention Manager (DOS)
FPS	Federal Protective Service
FTO	Foreign Terrorist Organization
GAO	Government Accountability Office
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
HSDN	Homeland Security Data Network
HPD	Humanitarian Parole Database
HQ	Headquarters
HSTC	Human Smuggling and Trafficking Center
IAFIS	Integrated Automated Fingerprint Identification System (FBI) [now called the Next Generation Identification (NGI)
IBIS	Formerly the Interagency Border Inspection System and is now TECS
IBIS SOP	Interagency Border Inspection System Standard Operating Procedures
ICE	Immigration and Customs Enforcement
IDENT	Automated Biometrics Identification System
IJ	Immigration Judge
IO	Immigration Officer
IRAD	International and Refugee Affairs Division
IRS	Intelligence Research Specialist
ISRS	Image Storage Retrieval System
KCC	Kentucky Consular Center (DOS)

220

National Background, Identity, and Security Check Operating Procedures

Acronym	Description
KST	Known or Suspected Terrorist
LEA	Law Enforcement Agency
LES	Law Enforcement Sensitive
LESO	Law Enforcement Support Operations
LHM	Letterhead Memorandum
LPR	Lawful Permanent Resident
MFAS	Marriage Fraud Amendment System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NACI	National Agency Check with Inquiries
NAILS	National Automated Immigration Lookout System
NBC	National Benefits Center
NaBISCOP	National Background Identity and Security Checks Operating Procedures
NCIC	FBI National Crime Information Center
NCIC III	National Crime Information Center Interstate Identification Index
NFTS	National File Tracking System
NGI	Next Generation Identification (formerly known as IAFIS)
NIIS	Nonimmigrant Information System
NLETS	National Law Enforcement Telecommunications System
NQP	Naturalization Quality Procedures
NNCP	National Name Check Program
NS	National Security
NSAU	National Security Adjudication Unit
NSB	National Security Branch
NSEERS	National Security Entry Exit Registration System
NSN	National Security Notification
NSR	National Security Record
NSRV	National Security and Records Verification Directorate
NSTP	National Security Threat Protection Unit
NSU	National Security Unit
NTA	Notice to Appear
NTC	National Targeting Center
NVC	National Visa Center (DOS)
OFL	Office of Fingerprint Liaison
OGA	Other Government Agency
OPE	Overseas Processing Entity
ORI	Originating Agency Identifier
OSI	Office of Security and Integrity
PCQS	Person-Centered Query System
PICS	Password Issuance and Control System

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Acronym	Description
POC	Point-of-Contact
RAFACS	Receipt and Alien File Accountability and Control System
RAIO	Refugee, Asylum and International Operations
RAP	Record of Arrest and Prosecution
RAPS	Refugees, Asylum and Parole System
RCMP	Royal Canadian Mounted Police
RFE	Request for Evidence
RNACS	Re-engineered Naturalization Application Casework System
ROIT	Record of Inquiry – TECS
ROIQ	Record of IBIS Query
ROP	Record of Proceeding
RPM	Records Policy Manual
RSO	Regional Security Offices
RTI	Referral to ICE
SAO	Security Advisory Opinion
SAW	Seasonal Agricultural Worker
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SCO	Security Control Officer
SCOPS	Service Center Operations
SEVIS	Student and Exchange Visitor Information System
SIMS	Secure Information Management System
SIR	Significant Incident Report
SIT	Secondary Inspection Tool
SOF	Statement of Findings
SOP	Standard Operating Procedures
SORN	Systems of Record Notices
SPII	Sensitive Personally Identifiable Information
SSN	Social Security Number
STE	Secure Telephone Equipment
STU III	Secure Telephone Unit – Third Generation
TECS	Treasury Enforcement Communications System (former full name)
TIDE	Terrorist Identities Datamart Environment
TPS	Temporary Protected Status
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
TSOU	Terrorist Screening Operations Unit
UNI	FBI's Universal Index
USC	United States Citizen

222

National Background, Identity, and Security Check Operating Procedures

Acronym	Description
U.S.C.	United States Code
USCG	United States Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	United States Secret Service
US-VISIT	United States-Visitor and Immigrant Status Indicator Technology
VAWA	Violence Against Women Act
VGTOF	Violent Gang and Terrorist Organization File
WMD	Weapons of Mass Destruction
WRAPS	DOS's Worldwide Refugee Admissions Processing System

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431728

National Background, Identity, and Security Check Operating Procedures

Appendix E: Glossary of Terms

Term	Description
Absconder	An alien who failed to surrender after receiving a final order of deportation or removal.
Action Code	The computer codes used to update a CLAIMS History File. Each code indicates the completion of a different action during the adjudicative process.
Aggravated Felon	Any alien who has been convicted of a criminal offense within the definition of 101(a)(43) of the Act.
Alias	An additional (e.g., nicknames, maiden names or other married names) or assumed name.
Ancillary Application	Applications for travel, employment authorization, or applications which do not convey an immigrant or nonimmigrant status, and are filed in connection with a primary or underlying application or petition.
Applicant	The individual listed on an application as the recipient of the immigration benefit sought. (Note: On the Form N-600K or, in some cases, the Form N-600, the adult who signs/files the application is treated as the applicant, although the child listed on the form receives the benefit.)
ASU	Adjudication Support Unit. Division within the National Security Branch at HQ FDNS which provides adjudicative assistance to the field such as the development, coordination, and implementation of case resolution strategies for cases with national security concerns. ASU also coordinates with Intelligence and Law Enforcement Agencies to declassify or to obtain permission to use classified information for such cases when appropriate.
Back End Checks	Security and systems checks performed immediately before the adjudication of an application or petition.
Batch Processing	The process by which a list of search criteria is electronically compared with database such as TECS. The list of search criteria can be generated either by extracting information from a separate database, such as CLAIMS, or through another spreadsheet or database.
BCAU	Background Check Analysis Unit. Division within the National Security Branch at HQ FDNS responsible for external vetting of KST cases and providing advice and technical assistance to the field for vetting cases with national security concerns.
BCU	Background Check Unit. Division found at service centers and the National Benefit Center. This division is responsible for reviewing and resolving TECS hits and other concerns as designated by local office policy.
Beneficiary	The individual listed on a petition as the recipient of the immigration benefit sought.

224

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP——in whole or in part——unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Term	Description
Carrier ID	A six-digit identifier used to distinguish batches. The first three digits will always be "CIS," followed by the first letter of the center (C, M, N, T, or V) conducting the batch query. The last two digits are used to identify a specific batch for a particular day within a center.
Center	Service center and/or National Benefits Center
CFDO	Center Fraud Detection Operations. A unit within FDNS located at each service center and the National Benefit Center responsible for referral of suspected fraud and public safety cases to ICE.
Component	Refers to the following divisions within USCIS: Office of Field Operations Service Center Operations Refugee Affairs Division Asylum Division International Operations
CRR	Case Resolution Record. Title of the form used for NS referrals to HQ FDNS prior to the National Security Record (NSR). Use was discontinued in May 2006.
Derivative	An individual who receives benefits from an application/petition without filing an application/petition on his or her own behalf.
Derivative of N-400	Child of N-400 applicant who meets all of the following criteria: 1) under 18 years of age, 2) lawful permanent resident, 3) resides in the United States in the legal and physical custody of the N-400 applicant parent (320 INA).
Director	District director and/or center director, asylum office directors, field office directors, and international operations district directors.
eCISCOR	The Enterprise Citizenship and Immigrations Services Centralized Operational Repository, eCISCOR, serves as an intermediary repository for immigration and naturalization information derived from several USCIS systems and will replace the Citizenship and Immigration Services Centralized Oracle Repository (CISCOR). eCISCOR is being built to interface with the Standard Management Analysis Reporting Tool (SMART) and PCQS. The CISCOR database consolidates data from USCIS's five Computer-Linked Application Information Management System 3.0 (CLAIMS 3) service center local area networks (LANs) to support CLAIMS 3 adjudications, workflow management, performance measurement, and ad hoc queries. eCISCOR is modelled on CISCOR, but utilizes replication technology to immediately capture data changes in the source system to prevent data discrepancies. eCISCOR is being developed and implemented in an effort to streamline access to information by

225

National Background, Identity, and Security Check Operating Procedures

Term	Description
	consolidating immigration and naturalization information from several USCIS systems into a centralized repository. eCISCOR will replicate and load read-only records from the following systems: Claims 3 (C3), CLAIMS 4 (C4), CIS2, GLOBAL, AR11, RAILS, RNACS, MFAS, and the Enterprise Service Bus (ESB) Background Vetting Service (BVS), which is used to determine whether a specified offense against a minor is included in an individual's criminal history record originally derived from the Federal Bureau of Investigation (FBI) Integrated Automated Fingerprint Identification System (IAFIS).
Egregious Public Safety Concern	Any case where information indicates the alien is under investigation for, has been arrested for (without disposition), or has been convicted of any of a list of criminal concerns, including but not limited to murder, rape, sexual abuse of a minor, trafficking in firearms or explosives, or other crimes listed in the MOA with ICE, Policy Memorandum 110, and section X, above.
ENFORCE	Enforcement Case Tracking System, ENFORCE is an event-based case management system that integrates and supports functions including subject processing, biometric identification, allegations and charges, preparation and printing of appropriate forms, data repository, and interface with the national database of enforcement events.
Field	Field refers to field offices, service centers, the National Benefits Center, and equivalent offices within the Refugee, Asylum, and International Operations Directorate (RAIO).
Final Decision (aka: Final Adjudicative Action(s))	Any decision of approval, denial, abandonment denial, revocation (excluding automatic revocation), rescission, reaffirmation, referral to immigration judge, or withdrawal of a benefit application/petition. Final decisions (final adjudicative action(s)) do NOT include: Administrative closures of any kind.
Final IDENT check (aka: OBIM-IDENT Check or Oath Ceremony IDENT Report)	Final IDENT check (also known as the OBIM-IDENT check and the Oath Ceremony IDENT Report) is conducted immediately prior to the grant of Lawful Permanent Residence or U.S. Citizenship. The primary purpose is to verify that no new derogatory information has been posted. For all Forms I-485, Application to Register Permanent Residence or Adjust Status, Final IDENT checks must be conducted on the day of final decision (aka: final adjudicative action) (Approval or denial. See instructions for list of exact final adjudicative actions, *including exemptions for specific I-485 denials executed at the NBC*, which require the Final IDENT Check to be performed).

226

National Background, Identity, and Security Check Operating Procedures

Term	Description
	For all Forms N-400, Application for Naturalization, Final IDENT checks must be conducted no more than one (1) business day prior to the Oath ceremony. Final IDENT checks may be run using one of the four (4) identifiers: A Number, Encounter Identity (EID) number, Fingerprint Identification Number (FIN), or Receipt Number. Final IDENT checks should **NOT** be run on any I-485 or N-400 cases that have been *administratively closed.*
Front End Check	Security and systems checks performed at the receipt of an application or petition to screen for NS, EPS, fraud, or other criminal concerns.
FTO	Foreign Terrorist Organization. Foreign organizations are designated by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended.
GLOBAL	GLOBAL is the Refugee, Asylum and International Operations (RAIO) case management system that assists the RAIO Directorate in the adjudication process for applicants. The case management system supports RAIO and USCIS in the screening of individuals in the credible fear, reasonable fear, affirmative (I-589), defensive, and NACARA (I-881) processes. It provides the means for tracking of asylum cases as they progress from application filing through final determination/decision or referral to the U.S. Immigration Courts.
LE	
Household Member	An individual 18 years of age or older living at the residence of an I-600 or I-800 petitioner or an I-600A or I-800A applicant.
HQ FDNS	Headquarters Office of Fraud Detection and National Security. Office within the National Security and Records Verification Directorate of USCIS.
Hit	A record returned by a security or background check system in response to a query, the subject of which may or may not relate to the subject being queried.
INTERPOL	International Criminal Police Organization, the world's largest international police organization. This organization facilitates cross-border police co-operation and supports and assists all organizations, authorities, and services whose mission is to prevent or combat international crime.
Just In Time (JIT) Check	Just In Time (JIT) TECS checks for Forms I-485 and N-400 are limited to the primary name and date of birth listed on the application (no alias).

227

National Background, Identity, and Security Check Operating Procedures

Term	Description
	JIT checks conducted immediately prior to the grant of Lawful Permanent Residence or U.S. Citizenship, the primary purposes of which is to ensure that no new Terrorism Information (TI), also referred to as Known or Suspected Terrorist (KST) lookouts, have posted since the last check was completed. A secondary purpose of JIT check is to ensure no potentially disqualifying information has been posted in TECS since the last query, such as information indicating a possible Adam Walsh Act (AWA) concern regarding a family-based I-130 petitioner at the time of the beneficiary's adjustment of status. For all Form I-485, Application to Register Permanent Residence or Adjust Status, JIT checks must be conducted on the day of final decision (aka: final adjudicative action) (approval or denial, see Appendix E: Glossary for exact list of final decisions). Note: No JIT check is required for any administratively closed I-485. For all Form N-400, Application for Naturalization, JIT checks must be conducted within no more than (2) business days prior to the date of the applicant's Naturalization Oath ceremony. JIT checks should NOT be run on either I-485 or N-400 applications that have been administratively closed.
JTTF	Joint Terrorism Task Force. Run by the FBI, JTTF are small cells of highly trained, locally based members from U.S. law enforcement and intelligence agencies. JTTF is responsible for all domestic and international terrorism matters.
KST	Known or Suspected Terrorist 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, and/or CLASS, as used by DOS. A KST in TECS has a record number beginning with a [LE] and ending in a [LE] and should indicate that the individual is a " [LE] [LE]
LHM	Letterhead Memorandum. A written summary of derogatory and/or pertinent information on an individual, prepared by the FBI, as a result of a positive response to the FBI Name Check request. The LHM may be classified or unclassified, or may contain a reference to a third agency (Third Agency Referral).
MMT	The Manifest Message Transmission is a CBP service typically used for batch TECS / NCIC queries. MMT provides all API data transmissions, including carrier, arrival and departure date and location, all directions and all modes of travel.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP—in whole or in part—unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431733

National Background, Identity, and Security Check Operating Procedures

Term	Description
LE	
NCIC Certification Test	The online test that must be successfully completed by each TECS user in order to obtain access to NCIC information. Certification remains valid for two years, after which re-certification is required.
NCTC	National Counterterrorism Center. In August 2004, the President established NCTC to serve as the primary organization in the United States Government for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism (CT) and to conduct strategic operational planning by integrating all instruments of national power. It is a multi-agency organization.
LE	
No Match	This annotation is used on the ROIQ if a TECS query results in no TECS hit.
Non-KST	A Non-KST NS concern includes all other NS concerns, regardless of source, including but not limited to: associates of KST(s), unindicted co-conspirators, terrorist organization members, persons involved with providing material support to terrorists or terrorist organizations, and agents of foreign governments.
NSR	National Security Record. Document used to record national security referrals from the field to HQ FDNS and to transmit the results of background check resolution activities from HQ FDNS to the originating office. Use was discontinued in May 2008.
NSRV	National Security and Records Verification Directorate. Directorate within USCIS.
NSTP	National Security Threat Protection unit. A component of ICE that assumed national security TECS resolution activity from the INS National Security Unit.
NSU	National Security Unit. Division within Immigration and Customs Enforcement (ICE).
OSI	Office of Security and Integrity

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431734

National Background, Identity, and Security Check Operating Procedures

Term	Description
Record Owner	The person who created or owns a given record, or the agency for whom that person works.
Petitioner	The individual, business, school, or other organization listed on the petition as the entity seeking an immigration benefit on behalf of a beneficiary.
PICS Officer	The officer within a USCIS office who is responsible for granting access to certain systems for USCIS personnel and maintaining relevant documentation.
Primary Name and DOB	The name and date of birth provided by the applicant or petitioner as his or her given name and date of birth. This is generally listed in the first part of the application/petition.
Query	A search in a security or background check system for relevant information through the data entry of search criteria relating to the subject. This query may be conducted through manual data entry or an electronic batch process.
Relates	This annotation is used on the ROIQ if a TECS query results in a hit that closely corresponds to the subject queried.
Resolution	A determination of the effect or relevance of the available information on the eligibility of the applicant, petitioner, beneficiary, or derivative for the benefit sought.
ROIQ	Record of IBIS Query. This form was formerly used to record the search criteria queried and the results of those queries.
ROIT	Record of Inquiry - TECS. This form is currently used to record the search criteria queried and the results of those queries.
SCO	The local USCIS officer who is responsible for implementing USCIS policy for TECS use and coordinating the designation and assignment of the TECS access for all applicable USCIS personnel. This officer serves as the local point of contact within USCIS for general TECS access issues.
Search Criteria	The search criteria for an SQ11 query include last name, first name and date of birth of a subject. The search criteria for an LE query are comprised of the name of the business or school.
Security Check	Specific checks or combination of checks required for each application or petition type, pursuant to each component's procedures.
Shortened Name Query	Notation on the ROIT where first names and last names exceeds 29 characters and NCIC query returns with an error due to length. USCIS personnel are instructed to adjust the name fields for a maximum of 29 characters for both name fields, rerun the query for NCIC results, and notate under the name with 'shortened name query' on the ROIT.
Shorter String Match Search	Refers to the first name field in TECS in which results of a TECS query may match all or only a portion of the queried first name. In the case of a subject with multiple variations of a first name or compound first name, USCIS personnel may query the portion of the first name that is

230

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Term	Description
	common to all variations. If the shorter string match search was used, USCIS personnel are required to notate "shorter string" on the ROIT.
Supporting Documentation	Documentation provided by the applicant, petitioner, or their designee in conjunction with an application/petition. This documentation includes all USCIS required forms and documents that establish relationship or identity. Examples of accepted documents include: passports, visas, Border Crossing Cards, Form I-94, Birth Certificates, Marriage Certificates, Divorce Decrees, diplomas/academic transcripts, student identification cards, military identification cards, driver's licenses, Social Security Cards.
System Match	A record returned by TECS in response to a query, the subject of which may or may not relate to the subject being queried. Same as TECS Hit.
TECS	Formerly known as the Treasury Enforcement Communications System/Interagency Border Inspection System. This is a computer system containing lookout and wants and warrants from various law enforcement and intelligence agencies. The system is maintained by CBP.
TECS by ELIS (TbE)	TECS by ELIS (TbE) is an electronic application that provides results of automated TECS/NCIC background checks via ATLAS for queries systematically run in systems such as CLAIMS 3 (C3) cases.
TECS Certification Test	The online test that must be successfully completed by each user in order to obtain access to TECS. Certification remains valid for two years, after which re-certification is required.
TECS Record	A uniquely numbered and identifiable entry into TECS or NCIC made by a contributing agency.
TECS Resolution Memo	Formal documentation of the reconciliation of a relating hit. The completion of this documentation is mandatory and must be completed before rendering a final decision.
TEL	Terrorist Exclusion List. Section 411 of the USA PATRIOT ACT of 2001 (8 U.S.C. § 1182) authorized the Secretary of State, in consultation with or upon the request of the Attorney General, to designate terrorist organizations for immigration purposes. This authority is known as the "Terrorist Exclusion Lis (TEL)" authority. A TEL designation bolsters homeland security efforts by facilitating the USG's ability to exclude aliens associated with entities on the TEL from entering the United States.
Terrorist Activity	Defined in 212(a)(3)(B)(iii) of the Act.
LE	
TIDE	Terrorist Identities Datamart Environment. This database contains all source highly classified information provided by members of the Intelligence Community such as CIA, DIA, FBI, NSA. From this classified database, an unclassified extract is provided to the TSC. That information, in turn, is used in compiling various watch lists such as the

National Background, Identity, and Security Check Operating Procedures

Term	Description
	TSA's No-Fly list, State Department's Visa and Passport Database, Homeland Security's Boarder System, and FBI's NCIC for state and local law enforcement.
TIPOFF	Program at DOS which managed the most comprehensive terrorist database. The TIPOFF database was enhanced and became the National Counterterrorism's primary terrorist identities database which is now known as the Terrorist Identities Datamart Environment (TIDE).
TSC	Terrorist Screening Center. Created in September 2003 to consolidate terrorist watch lists and provide 24/7 operational support for thousands of Federal screeners across the country and around the world. Administered by the FBI.
TSDB	Terrorist Screening Database. Houses the consolidated terrorist watch list which is maintained by the TSC. The information is extracted from the classified database, TIDE.
TSOU	Terrorist Screening Operations Unit. If there is a positive match for a subject on the terrorist watch list, the TSC notifies the TSOU. TSOU coordinates with the case agent/originating agency which nominated the individual to be placed on the watch list.
USCIS Officer	The following officers, including senior and supervisory officers: immigration analyst, intelligence research specialist, immigration information officer, immigration officer, field office director, immigration services officer, asylum officer or refugee officer).
USCIS Personnel	A person employed by USCIS or a company or agency that entered into a contract with USCIS to perform specified functions.
Valid TECS Query	A query completed within the previous 180 days, *unless* a JIT check is required. A final adjudicative decision cannot be made if all required TECS queries have not been conducted within the prescribed timeframe for the form type.
VGTOF	Violent Gang and Terrorist Organization File. The file has been designed to provide identifying information about violent criminal gangs and terrorist organizations and members of those gangs and organizations to law enforcement personnel. This information serves to warn law enforcement officers of the potential danger posed by violent individuals and to promote the exchange of information about these organizations and members to facilitate criminal investigations. USCIS has access to VGTOF through NCIC.
Work Folder	An unofficial file created at a local office for working purposes.

National Background, Identity, and Security Check Operating Procedures

Appendix F: Records Maintenance (Modernized MS92)

The Record Maintenance (Modernized MS92) function is specifically utilized to create TECS lookout records and sub-records as well as edit/update and delete records as needed Aircraft, Person, and Thing are the only record types currently available for this function. Others will be added as TECS modernization continues.

Why Enter a Record into TECS?

The 2013 TECS Record Creation SOP provides the most complete guidance on best practices for TECS record creation and maintenance. The information provided below is a snapshot of what is contained in the SOP. Most questions regarding specific requirements/recommendations for TECS record entry and maintenance may be answered by reviewing the aforementioned SOP. All other questions should be referred, through the chain of command, to the component-specific TECS SCO.

USCIS creates TECS records to alert TECS users to immigration and benefit related issues such as the following:

1. Pre-Adjudication – suspected fraud
2. Pre-Adjudication – confirmed fraud
3. Post-Adjudication – suspected fraud, denial notice issued
4. Post-Adjudication – suspected or confirmed fraud, benefit granted
5. Inadmissibility findings in accordance with the Immigration and Nationality Act (INA) § 212(a)
6. Involvement in or suspected involvement in immigration benefit fraud.
7. Impostors/Identity Compromise: Impostors may use someone else's document and genuine documents may be obtained by persons who are not entitled to them through identity fraud. Such fraud is common with the Permanent Resident Card, Form I-551. Often, the true bearer of a document is complicit in the act of fraud, by either giving their genuine document to a look-alike (impostor) or allowing another person to obtain a genuine card in the true bearer's name, but with the other person's photograph. TECS records must be created that will alert USCIS and law enforcement entities when such fraud has been committed.
8. Alert for Lost/Stolen Documents such as Permanent Resident Cards and/or Employment Authorization Documents (EADs).
9. Threats to Officer or Public Safety: As we want to safeguard our borders, so do we want to safeguard all personnel who may encounter persons posing a potential threat to public safety.
10. Non-Known of Suspected Terrorist (Non-KST) concerns with no prior TECS record.
11. Issuance of an NTA/Referral to Immigration Judge.[51]

---

[51] Refer to component-specific guidance for NTA processing.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431738

National Background, Identity, and Security Check Operating Procedures

Who Enters a Record into TECS?

FDNS immigration officers, Background Check Unit (BCU) staff and other USCIS officers as designated by local policy, may be required to enter records into TECS. No classified information may be entered into TECS. Certain fields are automatically system-generated and require no input from the user. Those who enter TECS records are responsible for maintaining the records as needed, ensuring the records contain complete and current information. Those unable to maintain TECS records they have created due to change of role or relocation should coordinate the transfer of these records to the appropriate POC(s) as determined by local policy.

The tables below outline the steps for creating and modifying TECS records.

LE

How to Enter a TECS Record		
Step	**Action Required**	**Notes**
1	Log in to TECS.	
2		
3	LE	
4		
5		

234

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

How to Enter a TECS Record		
Step	**Action Required**	**Notes**
6		
7		
8		
9		

LE

235
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431740

National Background, Identity, and Security Check Operating Procedures

How to Enter a TECS Record		
Step	**Action Required**	**Notes**
10		
11	**LE**	
12		
13		
14		

236
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

How to Enter a TECS Record		
Step	Action Required	Notes
15		
16		
17		
18		
20		

LE

237

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

How to Enter a TECS Record		
Step	Action Required	Notes
21		
22		
23		
24		
25		
26		
27		

LE

238
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

How to Enter a TECS Record		
Step	**Action Required**	**Notes**
28		
29		
30		
31		
32		
33		
34		

LE

239
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

How to Enter a TECS Record		
Step	**Action Required**	**Notes**
35	LE	
36		

How to Link Existing TECS Records		
Step	**Action Required**	**Notes**
1	LE	
2		

240

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP—in whole or in part—unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

How to Link Existing TECS Records		
Step	**Action Required**	**Notes**
3		
4		
5		
6		
7		
8		
9		

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431746

National Background, Identity, and Security Check Operating Procedures

How to Create Sub-Records		
Step	**Action Required**	**Notes**
1		
2	**LE**	
3		
4		

How to Edit/Delete Subject Records in TECS[52]		
Step	**Action**	**Notes**
1		
2	**LE**	
3		

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

How to Edit/Delete Subject Records in TECS[52]		
Step	**Action**	**Notes**
4		
5		

LE

243
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431748

National Background, Identity, and Security Check Operating Procedures

Appendix G: List of References

1. "Accessing National Crime Information Center Interstate Identification Index (NCIC III) Data" dated June 3, 2005, and signed by William R. Yates and Joseph Cuddihy.
2. "Additional Guidance: Processing Fingerprint Checks Prior to the Filing of Form I-600 Abroad" dated May 13, 2003, and signed by William R. Yates.
3. Asylum Division issued on May 14, 2008: "Issuance of Revised Section of the Identity and Security Checks Procedures Manual Regarding Vetting and Adjudicating Cases with National Security Concerns" signed by Joseph Langlois.
4. Attachment: "Enhanced Processing Instructions"
5. Attachment: "IBIS National Security Case Resolution Record,"
6. Attachment: "IBIS National Security Case Notification,"
7. Attachment: "IBIS National Security Case Resolution Request,"
8. Attachment: "IBIS | LE | User Agreement"
9. Attachment One: "Fingerprint Waiver Policy for All Applicants for Benefits under the Immigration and Naturalization Act and Procedures for Applicants Whose Fingerprint Responses Expire after the Age Range during which Fingerprints are Required"
10. Attachment Two - Beginning on page 6: "National Quality Procedures, Part III, Fingerprint Check Integrity"
11. "Benefits-Related Fingerprint Clearance Policy" dated April 2, 1997, and signed by Paul W. Virtue HQPGM.
12. "Clarification and Modification of New Resolution Process for IBIS National Security/Terrorism-Related Positive Results" dated March 29, 2005, and signed by William R. Yates.
13. "Clarification of February 14, 2003 Memorandum Concerning Fingerprint Check Integrity When Adjudicating Orphan Petitions" dated May 15, 2003, and signed by William R. Yates and Janis Sposato.
14. "Closing of Cases with Pending Law Enforcement Checks" dated April 5, 2004, and signed by William R. Yates and Janis Sposato.
15. "Completion of Interagency Border Inspection System (IBIS) Lookout Checks on Applications/Petitions for Immigration Benefits" dated September 5, 2001, and signed by Michael A. Pearson.
16. Cornell University Law School, Legal Information Institute U.S. Code Collection § 552a. Records Maintained on Individuals, (2009).
17. Department of Homeland Security, Locate Ports of Entry, (December 28, 2017)
18. Department of Homeland Security Management Directive System, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, January 6, 2005 (MD Number: 11042.1).
19. "Discontinuation of IBIS Alias Name Checks for Petitions and Applications When the Beneficiary and Dependents are not Physically Present in the United States," dated March 23, 2005, and signed by William R. Yates.

244

National Background, Identity, and Security Check Operating Procedures

20. Domestic Operations issued on April 24, 2008: "Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns."
21. Memorandum from Don Neufeld, Acting Associate Director, Domestic Operations, to Regional Directors, District Directors, Field Office Directors, Service Center Directors, Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns, April 24, 2008 (HQ 70/28.1).
22. Domestic Operations Division issued on June 5, 2009: "Clarification and Delineation of Vetting and Adjudication Responsibilities for Controlled Application Review and Resolution Program (CARRP) Cases in Domestic Field Offices," signed by Donald Neufeld
23. Donald Hawkins, Privacy Officer, Office of Security and Integrity, Chapter 8: Classified National Security Information (NSI), September 10, 2009.
24. Donald Hawkins, Privacy Officer, Office of Security and Integrity, Personally Identifiable Information (PII), September 3, 2009.
25. Donald Hawkins, Privacy Officer, Office of Security and Integrity, Safeguarding Classified and Sensitive Unclassified Information, May 2013.
26. Donald Hawkins, Privacy Officer, Office of Security and Integrity, Significant Incident Reports (SIRs), September 3, 2009.
27. "Expeditious Processing of Civil Fingerprint Cards, Forms FD-258" dated May 18, 2000, and signed by William R. Yates.
28. "Facilitated Process for Conducting FBI Checks for Diversity Visa and Age Out Adjustment of Status Applications (FBI-G-325 Name Checks --Expedites)" dated August 14, 2001, and signed by William R. Yates and Joseph Cuddihy.
29. "FBI Name Check Procedures" dated September 30, 2004, and signed by Joseph E. Langlois.
30. "FBI Name Check Procedures (Part II)" dated March 16, 2005, and signed by Joseph E. Langlois.
31. "FDNS Processing of Positive FBI Responses to G-325 Name Checks" dated October 21, 2004, and signed by Don Crocetti.
32. "Fingerprint Waiver Policy for Naturalization Applicants who are Unable to be Fingerprinted (NQP Policy Memorandum No. 60" dated November 15, 1999, and signed by William R. Yates.
33. "Fingerprint Check Integrity When Adjudicating Orphan Petitions" dated February 14, 2003, and signed by Johnny N. Williams.
34. "Fingerprint Waiver Policy for All Applicants for Benefits under the Immigration and Naturalization Act and Procedures for Applicants Whose Fingerprint Responses Expire after the Age Range during which Fingerprints are Required," dated July 20, 2001, and signed by Michael Pearson.
35. "Guidance on the Acceptance and Handling of FD-258 Fingerprint Cards (NQP Policy Memorandum No. 32" dated March 27, 1998, and signed by James S. Angus.
36. "Handling of all Pending Significant Incident Reports (SIRs)" dated May 27, 2005, and

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

    signed by William R. Yates.

37. "IBIS Naming Conventions" dated December 30, 2005, and signed by Michael Aytes.

38. "Increased Vigilance and Heightened Awareness: Increasing Intensity of Inspections at Land Border Ports-of-Entry: Operations Plans for IBIS Name Queries of Drivers and Passengers" dated October 31, 2002, and signed by Johnny N. Williams.

39. "INS Policy on the Usage of the Interagency Border Inspection System" dated July 31, 2001, and signed by Michael D. Cronin.

40. "Interagency Border Inspection System Records Check," dated July 2, 2002, and signed by Johnny N. Williams and Thomas Schiltgen.

41. "Instructions on Conducting IBIS Checks for Employment-Based Immigrant and Nonimmigrant Petitions and Employment-Based Applications for Adjustment of Status," dated April 29, 2004, and signed by William R. Yates.

42. "Interagency Border Inspection System Processing Completed at the National Benefits Center" dated December 7, 2005, and signed by Michael Aytes.

43. "Interagency Border Inspection System Records Check Requirements" dated January 20, 2004, and signed by William R. Yates.

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

45. INTERPOL, INTERPOL Notices, September 3, 2009.

46. Johnny Williams memorandum entitled "Enhanced Processing Instructions" dated March, 18, 2002, and William Yates memorandum entitled "Revised Enhanced Processing Instructions" dated April 5, 2005.

47. Memorandum from Donald K. Hawkins, Chief Privacy Officer, to all USCIS employees and contractors, USCIS Policy Regarding Personally Identifiable Information, July 8, 2008.

48. Memorandum from Donald Neufeld, Acting Associate Director, Office of Domestic Operations, to Field Leadership, Access to the Department of State's Consular Consolidated Database (CCD): Use of CCD Visa Data Safeguards Regarding Disclosure of Visa Data in Immigration Adjudications, June 17, 2008 (DOMO 70/2.2).

49. Memorandum from Donald Neufeld, Acting Associate Director, Office of Domestic Operations, to Field Leadership, Transmittal of SOP for Adjudication of Family-Based Petitions under the Adam Walsh Child Protection and Safety Act of 2006, September 24, 2008 (HQ 70/1-P).

50. Memorandum from Donald Neufeld, Acting Associate Director, Office of Domestic Operations, to Field Leadership, National Security Adjudication and Reporting Requirements- Update, February 9, 2009 (HQ 70/23 & 70/28.1).

51. Memorandum from Joseph E. Langlois, Chief, Asylum Division, to Asylum Office Directors and Deputy Directors, Supervisory Asylum Officers, Quality Assurance/Training Officers, and Asylum Officers, Production and Distribution of New

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

National Background, Identity, and Security Check Operating Procedures

Watch List Hit Reports by the Asylum Division, December 14, 2006 (HQRAIO 120/9.3a).

52. Memorandum from Joseph E. Langlois, Chief, Asylum Division, to all Asylum Office Personnel, Issuance of Updated IBIS and US-VISIT Procedures and Security Checklist, January 26, 2007 (HQRAIO 120/9.3a)

53. Memorandum from Joseph E. Langlois, Chief, Asylum Division, to Asylum Office Directors and Deputy Directors, Disclosure of Consular Affairs Visa Data in Asylum Adjudications, January 24, 2008 (HQRAIO 50/18.5.9).

54. Memorandum from Louis D. Crocetti, Jr., Director, Office of Fraud Detection and National Security, to Asylum Directors, Center Directors, Regional Directors, and District Directors, Criteria for Referring Benefit Fraud Cases, December 14, 2004 (HQ FDNS 70/2.1).

55. Memorandum from L. Francis Cissna, Director, USCIS, Departure-Related Systems Checks Requirement Preceding NTA Issuance, December 26, 2018.

56. Memorandum from L. Francis Cissna, Director, USCIS, Updated Guidance for Security Check Requirements Preceding Notice to Appear (NTA) Issuance and Departure-Related Systems Checks, December 26, 2018.

57. Memorandum from Michael Aytes, Associate Director, Domestic Operations, to all Service Center Directors, Regional Directors, District Directors, and Officers-in-Charge, Interim Guidance for Processing Status Documentation for EOIR-adjusted Permanent Residents pursuant to the Permanent Injunction in Santillan et al v. Gonzales, No. C 04-02686 (N.D. CA Dec. 22, 2005), December 29, 2005.

58. Memorandum from Michael Aytes, Associate Director, Domestic Operations, to all Service Center Directors, Regional Directors, District Directors, and Officers in Charge, International Marriage Broker Regulation Act Implementation Guidance, July 21, 2006 (HQOPRD 70/6.2.11).

59. Memorandum from Michael Aytes, Associate Director, Domestic Operations, to Regional Directors, Service Center Directors, District Directors (except foreign), Officers in Charge (except foreign), and National Benefit Center Director, FBI Name Checks Policy and Process Clarification for Domestic Operations, December 21, 2006.

60. Memorandum from Michael Aytes, Associate Director, Domestic Operations, to Regional Directors, District Directors, including Overseas District Directors, Service Center Directors, National Benefits Center Director, Associate Director of National Security and Records Verification, Guidance for Adjudication of Family-Based Petitions and I-129F Petition for Alien Fiancé(e) under the Adam Walsh Child Protection and Safety Act of 2006, (February 8, 2007) (HQDOMO 70/1-P).

61. Memorandum from Michael Aytes, Associate Director, Domestic Operations, to Associate Director of National Security and Records Verification, Regional Directors, District Directors, Director of National Benefits Center, Service Center Directors, Chief of Service Center Operations, Chief of Field Operations, Revised Guidance for the

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Removable Aliens," dated November 7, 2011, and also referred to as the New NTA Policy Memorandum, November 7, 2011 (Subject Code: PM-602-0050).

62. Updated Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) in Cases Involving Inadmissible and Deportable Aliens, dated June 28, 2018 (Subject Code: PM-602- 0050.1).

63. Guidance for the Referral of Cases and Issuance of Notices to Appear (NTAs) When Processing a Case Involving Information Submitted by a Deferred Action for Childhood Arrivals (DACA) Requestor in Connection With a DACA Request or a DACA-Related Benefit Request (Past or Pending) or Pursuing Termination of DACA, date June 28, 2018 (PM-602-0161).

64. Memorandum from Michael Aytes, Associate Director, Domestic Operations, and Louis D. Crocetti, Jr., Division Chief, Office of Fraud Detection and National Security, to Fraud Detection Unit Chiefs, Regional Directors, District Directors, National Benefits Center Director, Service Center Directors, Standard Operating Procedures for Religious Worker Petition Anti-Fraud Enhancements, July 5, 2006 (HQFDNS 180/8.1-P).

65. Memorandum from Michael Aytes, Associate Director, Domestic Operations, Janis Sposato, Associate Director, Immigration, Integrity, and Information, and Tracy Renaud, Acting Director, Officer of Refugee, Asylum, and International Operations, to Regional Directors, District Directors, Asylum Directors, National Benefits Center Director, Service Center Directors, and Fraud Detection Unit Chiefs, Extension of the Interagency Border Inspection System (IBIS) Record Check Validity Period, April 26, 2006 (HQFDNS 180/10.2-P).

66. Memorandum from Paul A. Schneider, Under Secretary for Management, and Hugo Teufel III, Chief Privacy Officer, Review of Safeguarding Policies and Procedures for Personnel- Related Data, June 13, 2007.

67. Memorandum from William R. Yates, Acting Associate Director for Operations, to Regional Directors, Service Center Directors, and District Directors, Adjudication of Benefit Applications Involving NSEERS Registrants, April 2, 2004 (HQOPRD 70/6.22/04) .

68. Memorandum from William R. Yates, Associate Director of Operations, U.S. Citizenship and Immigration Services, to Regional Directors, Service Center Directors, District Directors, and National Benefit Center Director, Discontinuation of IBIS Alias Name Checks for Petitions and Applications When the Beneficiary and Dependents are not Physically Present in the United States, March 23, 2005.

69. Memorandum from William R. Yates, Associate Director of Domestic Operations, and Joseph Cuddihy, Associate Director, Office of Refugee, Asylum and International Operations, to Asylum Directors, Regional Directors, District Directors, National Benefits Center Director, Service Center Directors, Accessing National Crime

DEF-00431753

National Background, Identity, and Security Check Operating Procedures

Information Center Interstate Identification Index (NCIC III) Data, June 3, 2005(HQFDNS 70/2.1-P).

70. "National Security Adjudication and Reporting Requirements Update" dated February 9, 2009, and signed by Donald Neufeld.

71. "National Security Unit Case Closures" dated February 19, 2004, and signed by William R. Yates.

72. "New Resolution Process for IBIS National Security/Terrorism-Related Positive Results," dated November 29, 2004, and signed by William R. Yates.

73. "Non-U.S. Citizens Prohibited from Access to DOJ Information Technology (IT) Systems," dated March 4, 2002, and signed by Robert F. Diegelman.

74. "Operational Guidance for Conducting and Documenting NCIC III Checks"

75. "Policy for Requesting Updated Rap Sheets for Expired Fingerprint Results", dated December 27, 2001, and signed by William R. Yates.

76. Policy Memorandum, Adjudication of applications that are submitted by individuals subject to the registration and reporting requirements of the National Security Entry Exit Registration System ("NSEERS" or "Special Registration"); Addition of Adjudicator's Field Manual (AFM) Chapter 10.23 (AFM Update AD12-08) , June 20, 2012.

77. "New National Security-Related IBIS Procedures," dated May 21, 2004, and signed by William R. Yates.

78. Privacy Policy Guidance Memorandum from Hugo Teufel III, Chief Privacy Officer, to DHS Directorate and Component Leadership, Use of Social Security Numbers at the Department of Homeland Security, June 4, 2007 (2007-2).

79. "Processing Fingerprint checks Prior to the Filing of Form I-600 Abroad" dated April 7, 2003, and signed by William R. Yates and Janis Sposato.

80. "Production and Distribution of New Watch List Hit Reports by the Asylum Division" dated December 14, 2006, and signed by Joseph E. Langlois,

81. Refugee Affairs Division, "National Security Concerns in Refugee Cases Standard Operating Procedure (RAD CARRP SOP)" March 2018.

82. "Request for Duplicate Rap Sheets and Inquiries", dated February 22, 2001, and signed by William R. Yates.

83. "Responsibilities of Adjudicators" dated November 13, 2002, and signed by Johnny N. Williams.

84. "Revised Enhanced Processing Instructions" dated April 5, 2005, and signed by William R. Yates.

85. "Revised Guidance for Accessing National Crime Information Center – Interstate Identification Index (NCIC III) Data" dated March 18, 2012

86. "Revised Guidance Pertaining to the Adjudication of Form I-90, Application to Replace Permanent Resident Card" dated February 6, 2009, and signed by Donald Neufeld.

87. "Revised National Security Adjudication and Reporting Requirements" dated February 4, 2008, and signed by Michael Aytes.

88. "Revision of the SQ11 IBIS Background Check Policy Guidance for pending I-360 and I-129 Religious Worker Petitions" dated September 18, 2006, and signed by Michael Aytes

National Background, Identity, and Security Check Operating Procedures

and Janis Sposato.

89. "Securing Compliance with Fingerprinting Requirements Prior to the Asylum Interview and Amending Procedures for Issuance of Recommended Approvals – Revised" dated October 4, 2006, and signed by Joseph E. Langlois.

90. "Transition and Revised Processing Procedures for FBI Biographic Name Check (G-325 or G-325A) Hit (NQP Policy Memorandum No. 68)" dated July 25, 2000, and signed by William R. Yates, LIMITED OFFICIAL USE ONLY - NOT FOR PUBLIC USE.

91. United States Citizenship and Immigration Services, Asylum Division, Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants, June 3, 2005.

92. United States Citizenship and Immigration Services, Domestic Operations, Standard Operating Procedure Form I-862, Notice to Appear, September 8, 2006.

93. United States Citizenship and Immigration Services, Form G-639, Freedom of Information Act/Privacy Act Request, September 1, 2009.

94. United States Citizenship and Immigration Services, Office of Fraud Detection and National Security, CARRP, Policy for Vetting and Adjudicating Cases with National Security Concerns, April 11, 2008.

95. United States Citizenship and Immigration Services, Office of Fraud Detection and National Security, Fraud Detection Standard Operating Procedures, December 6, 2019.

96. United States Citizenship and Immigration Services, Office of Fraud Detection and National Security, IBIS Standard Operating Procedure, March 1, 2006.

97. United States Citizenship and Immigration Services, Office of Fraud Detection and National Security, Attachment A – Guidance for Identifying National Security Concerns, April 11, 2008.

98. United States District Court, Northern District of California, San Francisco Division, Maria Santillan, et al., vs. Alberto R. Gonzales, Attorney General of the United States; Michael Chertoff, Secretary of Homeland Security, The United States Citizenship and Immigration Services; Emilio Gonzalez, USCIS Director; David Still, USCIS San Francisco District Director, (Case No. C 04-2686-MHP).

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Appendix H: USCIS - Fraud Detection and National Security (FDNS) Liaisons to Law Enforcement (LE)/ Intelligence Community (IC) Partner Agencies

USCIS has designated officers assigned to assist in information sharing with the following agencies:

Terrorist Screening Center (TSC)

FBI National Name Check Program (NNCP)

National Joint Terrorism Task Force (NJTTF)

Homeland Security Investigations-Forensic Laboratory (HSI-FL)

CBP National Targeting Center (NTC)

Human Smuggling Trafficking Center

INTERPOL United States National Central Bureau (USNCB)

National Counterterrorism Center (NCTC)

For contact information and guidance on submitting requests to these agencies refer to the USCIS-FDNS Liaison Branch page on the FDNS ECN site.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431756

National Background, Identity, and Security Check Operating Procedures

Appendix I: Quick Reference

TECS: Person Subject Query SQ11 & NCIC "Hot Files"		
IF	**THEN**	**Evidence in File (Non-record Side)**
No match found,	Annotate ROIT in the "No Match" box. Proceed to adjudication.	ROIT
Hit does not relate,	Annotate ROIT in the "DNR" box. Proceed to adjudication.[53]	ROIT
Hit relates and is NS,	Annotate ROIT in the "Relates" box. Cannot proceed to adjudication. Refer for CARRP processing in accordance with the April 11, 2008, memorandum entitled "Policy for Vetting and Adjudicating Cases with National Security Concerns".[54]	ROIT, Relevant TECS screen prints
Hit relates and is EPS,	Annotate ROIT in the "Relates" box. Cannot proceed to adjudication. Refer for EPS processing per Policy Memorandum 110. (Asylum and TPS cases not included)	ROIT, Relevant TECS screen prints
Hit relates and is other concern,	Annotate ROIT in the "Relates" box. Cannot proceed to adjudication. Follow local resolution processing.	ROIT, Relevant TECS screen prints

Validity of TECS Query? 180 calendar days.

FBI Fingerprint Check	
IF	**THEN**
LE	

---

[53] NS hits excluded.
[54] If contact with the Terrorist Screening Center is required to determine that a hit does not relate, a designated officer must contact the TSC.

252

National Background, Identity, and Security Check Operating Procedures

FBI Fingerprint Check	
IF	THEN

LE

253
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431758

National Background, Identity, and Security Check Operating Procedures

FBI Fingerprint Check	
IF	**THEN**
	LE

Validity of FBI Fingerprint Check - 15 months from FBI process date.

FBI Name Check			
FBI Code	**CPMS QUERY/ GLOBAL Code**	**USCIS Action**	**Evidence in File**
LE			

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431759

National Background, Identity, and Security Check Operating Procedures

LE

255

National Background, Identity, and Security Check Operating Procedures

LE

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain
electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely
necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to
the NaBISCOP ECN for the most recent procedural guidance.

LE

Validity of FBI Name Check Query - Indefinitely for the application for which it was requested. If used for another application, it must be within 15 months of the FBI Processed date. Only one definitive response is necessary for each name and DOB variation submitted.

257

DEF-00431762

National Background, Identity, and Security Check Operating Procedures

Appendix J Recommended Systems List
The following table shows systems, databases, and queries USCIS personnel use in the course of conducting security and background checks. Links to access forms are provided in the table below. To see more detail about each system, click on the link in the System Name column.

NOTE:
Some systems are not available to all USCIS personnel. Please check with your supervisor if you have questions about which of the following systems you can or should use.

- If you have questions on what background checks are mandatory please see Background Check Process.
- If you have questions on when other system checks are required, please consult local management and/or immediate supervisor.

*Printer-Friendly version of the Recommended Systems List available here.

Recommended Systems List		
System Name	**Common Searches**	**System Information**
Accurint - LexisNexis Enterprise Solution (*Non-U.S. Government System*)	•Name/DOB •SSN	Accurint/LexisNexis is a data fusion system for law enforcement that increases efficiency and investigative effectiveness. Accurint is not to be cited in USCIS notices or decisions; rather, information obtained through Accurint must be independently verified through the original source (i.e., via the applicable Judicial Branch, DMV, or State Corporation Commission website). **Access/Further Info: Field OPS** - see Regional Accurint/CLEAR systems administrator. **SCOPS and RAIO** - see HQ Component systems administrator. URL: https://▮▮▮▮▮▮▮▮▮
Arrival Departure Information System (ADIS)	• Ad-hoc Name/DOB query • Passport Number • Naturalization date • I-94	ADIS is a CBP system which aggregates travel and border crossing records, including arrivals and departures from the U.S. of LPRs, Refugees, and Asylees. This database provides more complete arrival and departure records than ⌐ **LE** ¬ **Access/Further Info:** HASH ID and temporary

258

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		password are issued by local SCO (list of local SCOs available at: http://████████████ ████████████)Once access is granted, use ████████████to open the web-based system.
Analytic Framework for Intelligence (AFI)	• Name/DOB • A-Number	AFI is a single sign-on (SSO) system which allows a federated search across law enforcement and intelligence systems, which enhance DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk. This aids in the enforcement of customs, immigration, and other laws enforced by CBP, ICE, and others. Access to information from over 60 data sources with a single sign-on: APIS, [LE]EID, NSEERS, IOIL, [LE]ICE Intel Products, IIRs, SEVIS, CCD, CEE, Visa data, ROIs[LE] LETC,[LE] TECS Intel (MOIRs), Primary Name and Vehicle, and many more. Also allows: **LE**

259

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		LE
Alien Change of Address Query Request (AR-11)	•Name, by country of Citizenship (COC) and/or DOB •A-number •Fingerprint Identification Number (FIN) •Admission Number (I-94)	AR-11 is a Change of Address (COA) system (Since December 2018, a sub-system of CIS2) dedicated to housing address change information submitted by nonimmigrants and lawful permanent residents (all of whom are required, by regulation, to report all temporary or permanent changes of address within ten days).
Case and Activity Management for International Operations (CAMINO)	•Name/DOB •A-Number •SSN •Consulate •Case Number •Email Address WRAPS Request/Person ID	CAMINO is a web-based, centralized case management system used worldwide by USCIS International Operations to adjudicate pending applications. **Access/Further Info:** Limited to authorized personnel of International Operations.
CBP Vetting	•Name/DOB •A-Number •SSN •Consulate •Case Number •Email Address WRAPS Request/Person	CBP Vetting is an application that provides for the vetting of subject and other information by government agencies. Processes vetting requests against TECS and National Crime Information Center (NCIC) databases and produce response files for viewing or downloading. Participation in CBP Enforcement Vetting gives

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431765

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
	ID Name/DOB •Name/DOB •Passport Number •Visa Control Number Foil Number	users the ability to submit vetting requests via onscreen entry or by uploading vetting request files that conform to specific formatting requirements. Users can then view or download the vetted response file that is created as a result of the vetting request submission. **Access/Further Info:** CBP controls user ID/password issuance. CBP vetting data may be available through other systems. URL: https:/ ▮▮▮▮▮▮▮▮▮▮
Consular Consolidated Database (CCDI/CCD)		The CCD is the database in the Washington, D.C. area that holds all of the current and archived data from all of the Consular Affairs post databases around the world. This includes the data from the ACS, CST, DV, IV (Immigrant Visa), NIV (Nonimmigrant visa), eClass, and IDENT applications (Note: Often contains photos of applicants, scanned copies of visa applications, and biographic information; May have lookout information and reasons for visa refusal.) The American Citizen Record Query (ACRQ) feature provides U.S. Citizen passport information. **LE**

DEF-00431766

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		LE
		Access/Further Info: DOS controls User ID and password issuance. If you have not yet created an account that can be enabled in the DHS/USCIS/OFO User Location, please do so at https█████████████ Then, create a ticket online at "My IT" at https:/████████████████████ and be sure to attach the form and Rules of Behavior. Thereafter, the best way to contact the current USCIS CCD Certifying Authorities (non-IVAMS), whether you need your password reset, your e-mail address affirmed, or general inquiries, is to create a ticket on USCIS myIT at

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		https:/ ████████████████ Please click on **System Access Request** followed by **Other System Access** and enter the information listed below in the **Additional information about my need** field and click on the "**Order Now**" button.
		Additional Information about my need: System: **CCD** Existing User ID (if applicable): *[Your CCD User Location and User ID]* Access Requested: **password reset, your e-mail address** Additional Information:
		Once access is granted, use the web-based system via https:/ ████████████████
Citizenship and Immigration Data Repository (CIDR)	•Name/DOB •A-number	CIDR stores and houses USCIS unclassified data sets (currently CLAIMS 3, and ultimately, CLAIMS 4) on the DHS classified network at the Secret (HSDN) and, in the near future, Top Secret (C-LAN) level. CIDR allows FDNS Immigration Officers to perform federated searches of data as well as comprehensive data analysis of large data sets using a suite of Commercial Off the Shelf (COTS) analytical tools. Stores classified FBI LHMs on the HSDN, enabling users to retrieve and review information efficiently. **Access/Further Info:** Limited to authorized personnel with "Secret" clearance. For additional details, go to http:// ████████████████████████████ ████████████████████████████
Central Index System 2 (CIS2)	•Name, by COC and/or DOB • A-Number •9101 Search by A-Number	The Central Index System (CIS) is a repository of electronic data used to maintain alien biographic, and current and historical immigration status information. CIS maintains information on lawful permanent residents, naturalized citizens, U.S.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431768

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	Common Searches	System Information
	•9102/9103 Search by Name/DOB •9504 Review A-file location •9106	border crossers, apprehended aliens, legalized aliens, aliens who have been issued employment authorization and other individuals of interest to the DHS. Information contained within CIS is used for immigration benefit determination and for immigration law enforcement operations by U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP). Information contained within CIS is also used by federal, state and local benefit granting programs, and by federal, state and local law enforcement entities. Central Index System 2 (CIS2) replaced the mainframe application with a web-based application. All CIS mainframe functionality are available in CIS2. The CIS2 screens mirror the CIS mainframe screens with only slight differences as CIS2 is Section 508 compliant, whereas CIS mainframe was not. All current CIS mainframe interfaces continue to exist in CIS2. CIS runs the following search queries: • 9101 (ID # search/display) • 9102 ('sounds like' search) • 9103 (exact name search) • 9106 ('sounds like' w/DOB search) • 9222 (ARC/BCC card display) • AR-11 (alien change of address query) • PF7 (card history) **Access/Further Info:** PICS ID and password are used to obtain access through "MyIT" icon on desktop, or at https▮▮▮▮▮▮▮▮▮▮▮ ▮▮▮▮▮▮▮▮▮▮ (Select "Business System Access" button and follow the prompts). Once access is

DEF-00431769

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	Common Searches	System Information
		granted, use "National" icon on desktop to open the system.
Computer-Linked Application Information Management System-3 (CLAIMS-3/C3)	•Name/DOB of beneficiary or petitioner •Receipt Number •A-Number	CLAIMS-3 (C3) is a database for all petitions or applications that are processed by the Service Centers. It allows USCIS users to view, update and track applications and petitions, from receipting fees to final adjudication through motions and appeals. It is accessed by a password, and level of access differs depending on user need. Users can view biographic data, case status and history for many types of forms. **Access/Further Info:** PICS ID and password are used to obtain access through "MyIT" icon on desktop (Select "Business System Access" button and follow the prompts). Once access is granted, use "National" icon on desktop to open the system. *Note: C3MF was placed in read-only mode on January 7, 2018. C3LAN will continue to be used for case updates. Users need to ensure that they have the eCISCOR-C3LAN PCQS user role to access case information.*
Computer-Linked Application Management System-4 CLAIMS 4/C4 - Legacy)	•Name/DOB •A-Number • SSN •Attorney •Address	Legacy CLAIMS-4 (C4) is a LAN-based software application called Switchboard. CLAIMS 4 offers USCIS a means of tracking immigrant status from initial status through work authorization, legal permanent residence, and citizenship. This national database was initially implemented for Form N-400 (Application for Naturalization) and interfaces with CIS, RAFACS, and FBI systems. While most N-400s are now processed either through web-based CLAIMS 4 or through ELIS, Legacy CLAIMS 4 remains the system of record for receipting and adjudicating the following forms: N-600, Application for Certificate of Citizenship; N-600K, Application for Citizenship and Issuance of Certificate Under Section 322, and N-565, Application for Replacement

DEF-00431770

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		Naturalization/Citizenship Document. It offers automated support for the variety of tasks associated with processing and adjudicating immigration benefits, including inputting application information, automated scheduling of examinations and adjudication, scheduling of oath ceremonies, generating notices, and enforcing standardized processes and work flow for each application type. **Access/Further Info:** PICS ID and password are used to obtain access through "MyIT" icon on desktop or at https:/███████████████ ██████████ Select "Other System Access," and specify Legacy C4. The local C4 administrator will need to give final approval. Once access is granted, use "Switchboard" icon on desktop to open the system.) *Note: Current plans are to decommission C4 (both web and legacy) in September 2019.*
Computer-Linked Application Management System-4 (CLAIMS 4/C4 – Web-Based)	• Name/DOB • A-Number • SSN • Attorney • Address	Web-based CLAIMS 4 (C4) stems from a LAN-based software application called Switchboard. CLAIMS 4 offers USCIS a means of tracking immigrant status from initial status through work authorization, legal permanent residence, and citizenship. This national database was initially implemented for Form N-400 (Application for Naturalization) and interfaces with CIS, RAFACS, and FBI systems. It offers automated support for the variety of tasks associated with processing and adjudicating immigration benefits, including inputting application information, automated scheduling of examinations and adjudication, scheduling of oath ceremonies, generating notices, and enforcing standardized processes and work flow for each application type.

DEF-00431771

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	Common Searches	System Information
		Access/Further Info: PICS ID and password are used to obtain access through "MyIT" icon on desktop or at https:/██████████ ████████████ Select "Other System Access," and specify Web-based C4. Once access is granted, use https:██████████/to open the web-based system.) *Note: Current plans are to decommission C4 (both web and legacy) in September 2019.*
Consular Lookout and Support System (CLASS)	N/A	CLASS contains records from numerous USG entities. Information includes visa refusals, lost and stolen passports, immigration violations, criminal history, terrorism concerns, and other derogatory information. **Access/Further Info:** CLASS is generally not accessed directly by USCIS officers. However, **LE**
CLEAR (*Non-U.S. Government System*)	•Name/DOB •SSN	CLEAR is a commercial investigative platform. CLEAR aggregates public and commerical records such as property records. **Access/Further Info:** Field OPS - see Regional Accurint/CLEAR systems administrator. SCOPS and RAIO - see HQ Component systems administrator. *Note: CLEAR is not to be cited in USCIS notices or decisions; rather, information obtained through Accurint must be independently verified through the original source (i.e., via the applicable Judicial Branch, DMV, or State Corporation Commission website).*
Customer Profile Management System (CPMS)	•Name/DOB •A-Number •FIN	CPMS is the repository of biometric and biographic identity, background check, and benefit card data for USCIS. CPMS stores the identity information collected at the Application support Centers (ASC) and the results of biometric background checks from

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431772

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		the Federal Bureau of Investigations (FBI) Next Generation Identification (NGI), biometric background checks from the Federal Bureau of Investigations (FBI) Next Generation Identification (NGI), Department of Defense (DOD) Automated Biometric Identification System (ABIS), and provides real-time link to the DHS Office of Biometric Identity Management (OBIM) IDENT. CPMS stores benefit card, extension sticker, and travel document information once they have been produced by the Enterprise Print Management Service (EPMS), Integrated Card Production System (ICPS)/ National Production System (NPS) or Application for Travel Document (Form I-131)/ Travel Document System Information Production System (TDPS). **Access/Further Info:** PICS ID and password are used to obtain access through "MyIT" icon on desktop (Select "Business System Access" button and follow the prompts). Once access is granted, use https:███████████ open the web-based system. *Note: Most locations now use CPMS IVT feature for Legacy US-VISIT SIT queries.*
Dun & Bradstreet (D&B) (*Non-U.S. Government System*)	•Company Name •Registered Agent Name •Location (City/State) •Telephone Number •Business Address •Federal Employer Identification Number (FEIN)	Dun & Bradstreet (D&B) is a web-based tool that allows USCIS users to access commercially available information from Dun & Bradstreet in order to validate information submitted by companies and organizations petitioning to employ foreign workers; vet key business information and critical data elements in support of the USCIS Mission; and identify any existing inconsistencies and/or identify potential fraud within domestic or international entities. **Access/Further Info:**

268

National Background, Identity, and Security Check Operating Procedures

System Name	Common Searches	System Information
		Field OPS personnel should see the Field OPS POC. SCOPS personnel should see the SCOPS POC.
Enforcement Alien Removals Module (EARM)	•A-Number •FIN •Event ID •FBI Number	EARM is a DHS/ICE system containing records of individuals encountered by ICE Office of Detention and Removal and/or individuals scheduled for immigration court proceedings. **Access/Further Info:** Access for USCIS users obtained through IMM (ICE version). Prospective users *and* authorizing supervisors need to register at the site and confirm their information (users may currently Select ▮▮▮▮▮▮▮▮ as supervisor, for request purposes). Secondary approvals also required. Once access is granted, use https▮▮▮▮▮▮▮ to open the web-based system.
EDMS/ EDMS Receipts	•A-Number •Receipt Number	EDMS contains scanned electronic copies of all digitalized A-files. EDMS Receipts, a companion module, contains scanned electronic copies of all digitized receipt files (i.e., I-131s, I-129s, I-539s, etc.). Copies of some scanned N-400 and N-336 filings also are retrievable through the ELIS Contingency Repository. U.S. Citizenship and Immigration Services (USCIS), Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP) personnel requiring access to A-file or Digitized Receipt Files information can access the electronic file directly through the EDMS. **Access/Further Info:** Request via ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮

269

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	Common Searches	System Information
		▓▓▓▓▓▓▓▓▓▓ open the web-based system.
Electronic Immigration System (ELIS)	•Name/DOB (exact *or* Name/DOB range) •A-Number •Receipt Number	ELIS is the online account-based system that allows customers to view their applications, petitions or requests, receive electronic notification of decisions, and receive real-time case status updates. Uses web-based technology to: • Integrate information used for adjudication and analysis • Improve data integrity • Reinforce consistency in decision-making • Help keep the immigration system secure ELIS' paperless processes revolve around the customer rather than forms and incorporate: • Case management, analytics, and decision support technology • An end-to-end adjudicative process based on benefits • Established electronic interfaces with other agencies • More standard ways for customers to communicate directly with USCIS USCIS ELIS enables customers and their representatives to submit requests for benefits electronically. USCIS ELIS also allows internal users (such as adjudicators, supervisors, and clerks) to efficiently process customers' applications.
Electronic Verification of Vital Events (EVVE) (*Non-U.S. Government System*)	•Name/DOB	EVVE Provides customers with the ability to quickly, reliably, and securely verify and certify birth and death information. Electronic inquiries from authorized users can be matched against over 250 million birth and death records from state and jurisdiction owned vital record databases nationwide. An electronic response from the state or jurisdiction either verifies or denies a match within matter of seconds. No other system on the market provides access to a more complete set of state and jurisdiction owned vital records than EVVE.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DEF-00431775

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		Access/Further Info: Maintained by the National Association for Public Health Statistics and Information Systems (NAPHSIS). Access generally limited to authorized FDNS personnel. Obtain EVVE Agency Query User form by emailing ▮▮▮▮▮▮▮@uscis.dhs.gov. After access is granted, use https:▮▮▮▮▮▮▮▮▮▮▮▮
Fraud Detection and National Security - Data System (FDNS-DS)	•Subject •Name/DOB •A-number •Receipt Number •CME Number (RFA/Lead/Case) •Address •Organization	FDNS-DS is a web-based application/database that is used to monitor the development of fraud leads and national security cases by immigration analysts. This tool is primarily used by Fraud Detection Units (FDU), Service Center Field Operations' Center Fraud Units (CFDO), and Background Check Units (BCU). Other components also use FDNS-DS to initiate FDNS referrals. **Access/Further Info:** Limited to authorized USCIS personnel. Requires approved FDNS-DS training prior to requesting access. Once access is granted, use https://▮▮▮▮▮▮▮▮▮▮▮▮ to access the web-based system.
Financial Crimes Enforcement Network (FinCEN) Portal	N/A	FinCEN contains information and analysis from Dept. of Treasury about financial transactions and Significant Activity Reports (SARs). SARs are self-reported to Treasury by banks and other financial institutions. **Access/Further Info:** Queries using the FinCEN portal may be requested through the HQ FDNS National Security and Public Safety Division (NSPSD). *Note: The Bank Secrecy Act (BSA) strictly prohibits disclosure of most information found in FinCEN.*
GLOBAL	•Name/DOB	The new Asylum Pre-Screening Process (APSO) was deployed in March 2018, replacing APSS. GLOBAL contains applicant data for all Forms I-

271

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		881, Application for Suspension of Deportation or Special Rule Cancellation of Removal (Pursuant to Section 203 of Public Law 105-100 (NACARA) and Forms I-589, Application for Asylum and Withholding of Removal (*Affirmative Asylum applications with USCIS*). **Access/Further Info:** Global is temporarily available to non-RAIO users via MyAccess (Business System Access Request: Checkers-DID(it) Checkers) until information is available in PCQS. Non-RAIO users and RAIO FDNS users should select the "read-only" role. All requestors must complete the Confidentiality form that is available via MyAccess: https:▓▓▓▓▓▓▓▓▓▓▓▓
Homeland Secure Information Network (HSIN)	•Name •Various intel reports	HSIN is a trusted network for sharing Sensitive But Unclassified (SBU) information across the homeland enterprise, including with state and local partners. **Access/Further Info:** USCIS Helpdesk cannot assist with granting access. Within HSIN, access to particular communities may be further restricted by officer role. URL▓▓▓▓▓▓▓
Interim Case Management Solution (ICMS)	•A-Number •Receipt number	ICMS is a web-based front-end to the CLAIMS 3 Local Area Network (LAN) system at the National Benefits Center (NBC). ICMS can be used to review, modify, and adjudicate the following Forms: • I-90 - Application to Replace Permanent Resident Card • I-130 - Petition for Alien Relative • I-212 - Application for permission to Reapply for Admission into the U.S. After Deportation or Removal • I-290B - Notice of Appeal or Motion • I-360 - Petition for Amerasian, Widow(er), or Special Immigrant • I-485 - Application to Register Permanent

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

DEF-00431777

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		Residence or to Adjust Status • I-601 - Application for Waiver of Grounds of Excludability • I-612 - Application for Waiver of the Foreign Residence Requirement • I-730 - Refugee/Asylee Relative Petition • I-765 - Application for Employment Authorization • I-821D - Consideration of Deferred Action for Childhood Arrivals The system contains information on persons lawfully admitted for permanent residency, Asylees and Parolees lawfully admitted for employment authorization (although, Asylees and Parolees are not initially covered under the Privacy Act, these individuals often change their status to lawful permanent residents and at that time will be covered by the Privacy Act), Commuters and other persons authorized for frequent border crossing, and Naturalized United States Citizens. **Access/Further Info:** PICS ID and password are used to obtain access through "MyIT" icon on desktop or at https:/███████████ ████████ (Select "System Access Request" button, then "Request Access Role" button to enter "MyAccess," and follow the prompts). Once access is granted, use https:/████████████████████████████ to open the web-based system.
INTELINK-U	•Name	DNI-U is the network infrastructure portion of the system formerly known as the Open Source Information System (OSIS). The new Intelink-U database houses open source information obtained from the Intelligence community. **Access/Further Info:** DNI-CIO controls User ID and password issuance. Once access is granted,

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		use https://[REDACTED] the web-based system.
Law Enforcement Enterprise Portal (LEEP)	N/A	Maintained by the FBI, LEEP is a gateway providing law enforcement agencies, intelligence groups, and criminal justice entities access to beneficial resources. Users can strengthen case development with investigative tools available, collaborate with internal and external agencies, and securely share sensitive documents. Examples of available resources include: Virtual command centers, nationwide criminal justice records, global cyber-complaint data, counterterrorism threat tracking, and intelligence centers. **Access/Further Info:** FBI controls User ID and password issuance. URL: https://www.[REDACTED]
National Appointment Scheduling System (NASS)	•Name/DOB •A-Number	NASS is used to request biometrics appointment scheduling for applicants seeking a benefit • Cancel appointments (may cause rescheduling) • Search for applicant scheduling data/history, appointment notices, etc. • Create applicant record for scheduling biometrics appointments Request fingerprint refresh if applicant's fingerprint result expired, request biometrics cloning from one Service Center to another, and report on scheduling data, backlog, manifest, etc. • Users access NASS on USCIS network using single sign on (PIV card). Users may request new or different access levels via ICAM. • After a supervisor's electronic approval, users should receive access within 24 hours. • Users will be notified of access expiration after 1 year. Recertification is necessary. • NASS Roles include: System Information o Admin (zip codes, allocations, bulk cancel,

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		etc.) – BD HQ users o Power (cancel/expedite) - Service Centers/NBC, Rescheduling Unit (APBU), ASCs, Call Centers o User (create/upload) - Most other users o Query (read only) - CMS users **Access/Further Info:** Request via https://███████████████████████ Once access is granted, use https://████████████████████ to open the web-based system.
Public Access to Court Electronic Records (PACER)	N/A	PACER is an electronic public access service that allows users to obtain case and docket information online from federal appellate, district, and bankruptcy courts, and the PACER Case Locator. PACER is provided by the Federal Judiciary in keeping with its commitment to providing public access to court information via a centralized service. This database may be used to confirm open-source information obtained from JUSTIA and other open sources. **Access/Further Info:** Access to PACER generally is limited to a select few Intel Officers and Agency Counsel. Master accounts may be available in some locations. URL: www.pacer.gov
Person Centric Query Service (PCQS -ESB)	• Name/DOB • A-Number • SSN	PCQS (CIS Super Query) allows users to submit a single query to return a consolidated record of an immigrant's interactions with the U.S. immigration system. PCQS is a composite service that allows a system or a person to submit a single query for all transactions involving an immigrant across a number of USCIS and DOS systems. PCQS returns a consolidated and correlated view of the immigrant's past interactions with the government as he or she passed through the U.S. immigration system. **Access/Further Info:** Complete the USCIS ESB and USCIS Rules and Behavior forms. The ESB

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		form must be signed by supervisor and faxed or emailed to the USCIS Help Desk. Once access is granted, use https:/██████████████████████ o to open the web-based system.
RAILS	•A-Number •Receipt Number	RAILS (formerly NFTS Modernization) is a joint effort between IRIS and the Office of Information Technology (OIT). RAILS is the current system of record for tracking of millions of immigrant and receipt files. RAILS interfaces with other case management systems (CIS, ELIS, GLOBAL, etc.) to support file tracking and transactions nationally as well as tracking by USCIS agents worldwide via the USCIS Intranet. Contains exact information regarding the location of all A-files, T-files, or S-files. Access is required to order or work with A-files. If you are working with an A-file, you must transfer the file to your Responsible Party Code (RPC) in RAILS. Once you are finished with an A-file, you should re-assign it to a colleague or charge out to Records. Scanned documents from files at the NRC may be requested by calling 816-350-████ r emailing ████████████@uscis.dhs.gov **Access/Further Info:** PICS ID used to obtain access through "MyIT" icon on desktop or at https://██████████████████████ (Select "System Access Request" button, then "Request Access Role" button to enter "MyAccess," and follow the prompts).

DEF-00431781

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	Common Searches	System Information
Service Center CLAIMS (SCCLAIMS)	•Name/DOB •SSN •FEIN •Preparer •A-Number •Remitter •Representative •Address	FDNS-SIB is actively working to transition all identified SCCLAIMS user needs to SMART and SAS. In order to ensure that these alternative systems can be used in lieu of SCCLAIMS, we have setup an ECN to assist with capturing user provided descriptions of queries, reports, and any other mission need that is currently being filled by SCCLAIMS. SIB will collect this information on an ongoing basis via the SCCLAIMS Transition Project ECN site.
Student & Exchange Visitor Information System (SEVIS)	•Name/DOB •SEVIS ID •School or program •Student status	SEVIS tracks and monitors nonimmigrant students and exchange visitors. If accepted by a Student and Exchange Visitor Program (SEVP)-certified school, foreign students may be admitted to the United States with the appropriate F or M nonimmigrant status. If accepted for participation in a Department of State-verified exchange visitor program, exchange visitors may be admitted to the United States with J nonimmigrant status. Records of these nonimmigrant admissions and continued participation in these educational programs are maintained in SEVIS. Further, SEVIS enables SEVP to assure proper reporting and record keeping by schools and exchange visitor programs, thereby ensuring data currency and integrity. SEVIS also provides a mechanism for student and exchange visitor status violators to be identified so that appropriate enforcement is taken (i.e., denial of admission, denial of benefits or removal from the United States). Also contains information on the schools and programs being attended. Other information in SEVIS includes: Biographical data; Admission number, Citizenship; Current school code; Current student status; All I-20s and DS-2019s issued for each student and exchange visitor; School and exchange visitor program data, including school status, school code, designated school officers, and school/program violations;

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	Common Searches	System Information
		Education and employment data; Dependents (F2s and J2s). ICE uses the information in SEVIS to identify potential security problems with individual students and the schools they attend. ICE actively pursues investigations of these security violations. If subject has filed I-485 after the date of termination, the subject may have failed to comply with the conditions of nonimmigrant admission. This might make an alien ineligible for adjustment status (INA 245(c) (2), 8 USC 1255 (c) (2). **Access/Further Info:** A SEVIS request requires the following, in PDF format: █████████████████████████████████████ Once access is granted, use █████████████████████████████████████ *Note: Limited SEVIS information also available in CCD.*
TECS / National	•Name/DOB •TECS Record ID	TECS is a multi-agency database of lookout information and is used to improve border

DEF-00431783

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
<u>Crime Information Center</u> / National Law Enforcement Telecommunications System (TECS/NCIC-NLETS - Modernized)		enforcement and facilitate inspection of individuals applying for admission to the United States at ports-of-entry and pre-inspection facilities. **Access/Further Info:** HASH ID and temporary password are issued by local SCO (list of local SCOs and other useful information about TECS available on the <u>TECS/NCIC</u> website via the following link: ▮▮▮▮▮▮▮▮▮▮▮▮ Prospective users must complete the TPA Privacy Awareness course before you can access the system. Once access is granted, access the web-based system via ▮▮▮▮▮▮▮▮▮▮ •Discretionary queries available for address, business, etc. **LE** NIV) •SQ11 searches require a name/DOB; to include **LE** •SQ94 - Entry/Departure travel history
TECS by ELIS (TbE)	• Name/DOB • Receipt number	TECS by ELIS (TbE) is an electronic application that provides results of automated TECS/NCIC background checks via ATLAS for queries

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

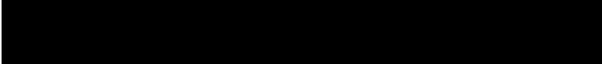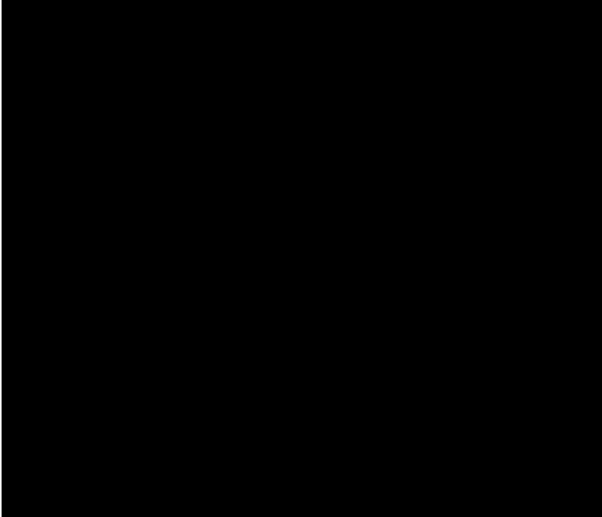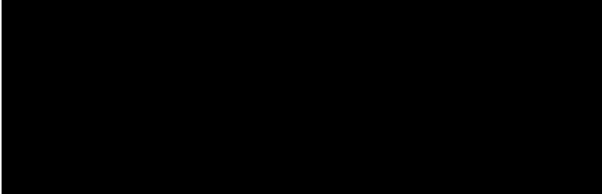## National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
	• A-number • Import from eCiscor	systematically run in systems such as CLAIMS 3 (C3) cases. TbE stores digital versions of the ROIT (Record of Inquiry – TECS), Resolution Memos and uploaded supporting documentation. A case in TbE can be searched by using the receipt number, A number, or the first and last name and date of birth. Manual Name Harvesting can be completed in TbE. TbE will run an automatic check via ATLAS after a user saves and submits a name. User also have the ability to import cases from eCISCOR. **Access/Further Info:** Request via https://███████████████████Once access is granted, use URL: https:/██████████████████with the Chrome browser.
UPAX	N/A	UPAX is a DHS/CBP with multiple inputs and capabilities, including functions previously accessible to USCIS personnel only through ATS-p. UPAX has replaced ATS-p as the module used at all U.S. airports and seaports receiving international flights and voyages to evaluate passengers and crewmembers prior to arrival or departure. It assists the CBP officer's decision-making process about whether a passenger or crewmember should receive additional screening prior to entry into or departure from the country because the traveler may pose a greater risk for violation of U.S. law. The system analyzes the Advance Passenger Information System (APIS) data from TECS, Passenger Name Record (PNR) data from the airlines, TECS crossing data, TECS seizure data, and watched entities. ATS-P processes available information from these databases to develop a risk assessment for each traveler.

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		Access/Further Info: CBP controls ID and password issuance to individuals who complete the following process: Requests for UPAX access <u>must be initiated and submitted by the appropriate supervisor</u> and the requesting employee must have a current favorably adjudicated Full-Field background investigation. To obtain authorization to use the Automated Targeting System – Unified Passenger programs the following steps need to be taken: 1. 2. 3. 4. **UPAX+Passenger Name Records (PNR)**. PNR access is not automatically granted –detailed justification for the need.

281

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	**Common Searches**	**System Information**
		1. Each USCIS FDNS requestor should provide a short but specific justification why they need the ATS-P + PNR access requests. 2. In the Spreadsheet column with the justification for the request (or in separate statement in the body of the email), the requestor also need to include answers to these 3 questions: • Why do you need PNR access, how is this access going to support your daily duties (specify duties)? • Before such access, how were you able to perform your daily responsibilities? • In the event that you lose this access, how will your work be affected? ███████ Further guidance regarding background information may be obtained by contacting the USCIS OSI Customer Service mailbox at ████████ CustomerServ@dhs.gov. ***Step-by-step instructions to encrypt messages go to the OSI Portal at** http://████████
Validation Instrument for Business Enterprises (VIBE)	• Receipt number	VIBE is a tool designed to enhance USCIS's adjudications of certain employment-based immigration petitions. Uses commercially available data from an independent information provider (IIP) to validate basic information about companies or organizations filing petitions to employ alien workers. VIBE also is used to electronically refer cases with criminal, national security, intelligence, and fraud concerns to the Center Fraud Detection Operations (CFDO). In current use by CBP, DOS, and in a pilot program with DOL. The VIBE Status Report (VSR) within VIBE includes information that indicates the viability of a petitioner and a VIBE score that can also be

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
<u>Please Note</u>: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.

National Background, Identity, and Security Check Operating Procedures

Recommended Systems List		
System Name	Common Searches	System Information
		overridden to notify Officers: If a petitioning organization is currently a subject of an administrative investigation, Is suspended from filing with USCIS, Is the subject of an ongoing criminal investigation, Has associated individuals charged with committing fraud/convicted for fraud. The "VIBE Pre-defined Company Score"(Comment) section on the VSR provides additional information about a petitioning entity that is pertinent to its validity/eligibility, or a brief description of why a business entity's score has been overridden. **Access/Further Info:** Request via https://███████████████████████ Once access is granted, use https://████████████████/VIBE/█████ to open the web-based system. *Note: Users with PCQS access automatically have access to VIBE, as well.*
Worldwide Refugee Admissions Processing System (WRAPS)	•Name/DOB •A-number •Case Number	WRAPS is a DOS Case management system for refugee applications and U.S. resettlement processing. Contains scanned copies of the I-590, Assessment, and other interview docs. May also contain family tree, persecution story, and RSC case notes. **Access/Further Info:** Complete WRAPS Access Form (available in Systems Folder) and turn in to a supervisor, who must email form to the RPC Help Desk. Once access is granted, use the following URL to open the web-based system: https://███████████████████████████ ██████████████████████████████

Other Commercial and Open Source Databases:

283

National Background, Identity, and Security Check Operating Procedures

Note: Refer to component-specific guidance as to when discretionary checks of open source information may be appropriate.

1. American Medical Association Doctor Finder (OPEN SOURCE) - Searchable database of nationwide AMA certified medical doctors. https://apps.ama-assn.org/doctorfinder/

2. Black Book Online - A free public records search of federal, state, and county public records. http://www.blackbookonline.info/

3. CAMPAIGN CONTRIBUTION DATABASES (OPEN SOURCE) - These finance databases are important because they often uncover discrepancies in SUBJECTS' finances (aka TAX FRAUD). For example, when a SUBJECT claims a very low/moderate level of income and is concurrently maxing out campaign contributions to multiple campaigns then most likely SUBJECTS' income is being misrepresented/not accounted for in tax payments. Lines of questioning can be established to uncover discrepancies between SUBJECTS' actual income vs. reported income. These databases are especially important in cases involving a nexus to terrorism because many terrorist fundraisers seek to establish strong connections with Congressional members in order to further their charities influence as well as to influence/expedite immigration decisions. http://www.opensecrets.org & http://www.followthemoney.org

4. CYBERCOP (NC4- SITUATIONAL READINESS NETWORK) - ID/password selected and access authorized by Cybercop; Intelligence data and postings from across the law enforcement community. https://cybercop.esportals.com/index.cfm

5. Department of State (DOS) U.S. Visa: Reciprocity and Civil Document by Country (reciprocity page) - Nonimmigrant visa applicants from certain countries*/areas of authority may be required to pay a visa issuance fee after their application is approved. These fees are based on the principle of reciprocity: when a foreign government imposes fees on U.S. citizens for certain types of visas, the United States will impose a reciprocal fee on citizens of that country*/area of authority for similar types of visas.

   https://travel.state.gov/content/visas/en/fees/reciprocity-by-country.html/
6. Global Security and Jane's - Both can be used to research organizations or countries of interest. http://www.globalsecurity.org/ https://janes.ihs.com/

7. GUIDESTAR (OPEN SOURCE) - Contains tax and board member information for non-profit entities. http://www.guidestar.org

National Background, Identity, and Security Check Operating Procedures

8. <u>ICE Pattern Analysis and Information Collection System (ICEPIC)</u> - ID/password assigned by ICEPIC; ICEPIC (Tool) is a toolset that assists in analyzing suspect identities and discovering possible non-obvious relationships among individuals/organizations. Modular set of information analysis tools that allow disparate sources of information to be analyzed to find previously unknown relationship data about individuals who are the subject of ongoing and valid investigations.

9. <u>JUSTIA (OPEN SOURCE)</u> - This database allows user to search Federal District Court Filings & Dockets to find federal litigation (including MANDAMUS suits) pertaining to SUBJECT. Search under Cases Filed In: All Federal District Courts & All Lawsuit Types. The PACER database can confirm findings. http://dockets.justia.com/

10. <u>LAW ENFORCEMENT GUIDE TO TERRORIST GROUPS & EMBLEMS</u> - https://www.usadojo.com/wp-content/uploads/2010/09/terrorist-emblems.pdf

11. U.S. Department of Treasury OFAC's Specially Designated Nationals (SDN) and Blocked Persons List - Published list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. The list also includes individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country- specific.

A search of the Treasury Department's **OFAC** list by name and organization is absolutely essential in all cases in which a nexus to terrorism might exist. The OFAC list is important because it provides USCIS with **open source** derogatory information, which can immediately be used to formulate a denial upon very strong grounds. The open source designation of the list allows us to open up lines of questioning without the limitations that classified materials provide.

Executive Order 13224 designated 29 foreign individuals and entities as Specially Designated Global Terrorists (SDGTs). The Order also authorizes the Secretary of the Treasury, Attorney General and Secretary of State to consult with one another to form and update regularly a public list of SDGTs. This list is released in the Federal Register and also on the OFAC website. Under the Order, finances of all entities/individuals on the list are frozen. The purpose of a public OFAC list is to give banks notice of all SDGTs so that their assets can be frozen. Financial institutions are required to check the list prior to all large financial transactions.

National Background, Identity, and Security Check Operating Procedures

A 'Ctrl F' search of the link provided above can pinpoint ORGANIZATIONS that a SUBJECT may be affiliated with or a SUBJECT himself. After going to the OFAC web page simply press 'CTRL F.' This will bring up a search query box that will allow you to type in key words or names to search the page for (NOTE: The page is in chronological order). Common names may require you to hit the 'find next' button in order to scroll through all of the hits on the page. In recent years the list has focused more on entities than individuals so it may be more common for you to locate an entity match than a name match.

One drawback to the list is that once the terrorist organizations on the list have their assets frozen, they simply start a new 'front' group and carry on with their business as usual. The list certainly lags well behind this curve, but it is a strong tool in many of the cases that have been pending for any substantial amount of time. The list is generally updated once or twice a month. Since this list is compiled by three agencies, it is not as comprehensive as the FBI's designations which are referenced by   **LE**   records, but nevertheless it is OPEN SOURCE.

https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx
http://www.treas.gov/offices/enforcement/ofac/sdn/sdnlist.txt

12. Open Source Enterprise - OSC provides username and password. Collects and analyzes open source information of intelligence value across all media – print, broadcast and online. It is a useful site for international media coverage and country conditions information. OSC provides foreign media reporting and analysis to government institutions and strategic partners. Database contains timely and authoritative open source intelligence information for analysis and operations. https://www.opensource.gov/public/content/login/login.fcc

13. SOCIAL SECURITY DEATH INDEX (OPEN SOURCE) - The Social Security Death Index (SSDI) is generated from the U. S. Social Security Administration's Death Master File. The SSDI does not include death records for everyone who has been issued a Social Security Number (card). Common reasons for exclusion include the following: The death was not reported to the Social Security Administration (SSA). The death occurred before the Death Master File was maintained in a computer database. About 98 percent of the deaths in this database occurred between 1962 and the present. The person did not participate in the Social Security program. Survivor death benefits were (are) being paid to dependents or spouse. A recent death may not be indexed yet. https://search.ancestry.com/search/db.aspx?dbid=3693

National Background, Identity, and Security Check Operating Procedures

Appendix K: System Generated Notifications

System Generated Notification (SGNs) are automatic notifications in FDNS-DS that indicate potential National Security concerns, Public Safety threats, and Fraud leads. SGNs were developed by FDNS, with input from across USCIS, as an enhancement to FDNS-DS. SGNs supplement the work currently performed by USCIS personnel by:

- Helping to identify potential National Security concerns, Public Safety threats, and Fraud leads earlier in the application screening process.
- Confirming applicant biographic and biometric information.
- Ensuring the integrity of the immigration process.

FDNS will continue to enhance screening capability in order to assure the integrity of the United States immigration system. FDNS is currently working to develop, test, and deploy additional screening rules, which are checks that produce an SGN for a positive match, to improve the effectiveness of the SGN process. In conjunction with this effort, FDNS will establish an on-going dialogue with stakeholders to ensure transparency surrounding the SGN implementation process.

SGNs are created when FDNS screens biographic, biometric, and form data against DHS and partner agency systems and databases to alert FDNS of potential National Security concerns, Public Safety threats, and Fraud leads. SGNs are then triaged (reviewed, confirmed, and distributed to appropriate POCs, in accordance with local policy) by designated USCIS personnel, known as Gatekeepers.

Gatekeepers: USCIS Gatekeepers are responsible for triaging SGNs. Gatekeepers may triage SGNs by:

- Querying FDNS-DS by SGN Rule number and by office location.
- Grabbing and assigning SGNs to the "My SGN" list.
- Confirming a SGN match with an applicant's biographic and biometric information.
- Determining if there is any derogatory information associated with an applicant.
- Creating or linking a Case Management Entity (CME)[55] or referring a SGN to the appropriate Gatekeeper for CME creation.[56]
- Referring CMEs to duly assigned personnel to conduct administrative investigations.[57]
- Recording time spent triaging each SGN under the Hours column.

---

[55] A CME may alternatively by referred to as a Record.
[56] For example, in the case that a Fraud SGN is converted to a National Security Concern, the initial Gatekeeper may refer the SGN to a different Gatekeeper for CME creation.
[57] Designated personnel who perform administrative investigations follow existing policy and procedures.

National Background, Identity, and Security Check Operating Procedures

Every Gatekeeper must have the appropriate level of clearance, which is dependent upon the type of Rule being triaged.

Complete guidance for SGN Gatekeepers is contained in the SGN User Guide.

For more information, read up on the IDENT Error Resolution for SGN Gatekeepers and the SGN Operational Guidance and SOP located in the NaBISCOP Document Library.

288
FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE
Please Note: This document is current only as of the date of access. Please do not create/retain electronic or paper versions of the NaBISCOP----in whole or in part----unless absolutely necessary. Updates to the NaBISCOP are made on a regular basis. Therefore, users must refer to the NaBISCOP ECN for the most recent procedural guidance.