EXHIBIT 24

~~FILED UNDER SEAL~~

U.S. CITIZENSHIP AND IMMIGRATION SERVICES ACADEMY

U.S. Citizenship and Immigration Services

FDNS OFFICER BASIC TRAINING

NATIONAL SECURITY PARTICIPANT GUIDE

FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE

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

April 2008

SYLLABUS

COURSE TITLE: National Security

COURSE NUMBER: 701

COURSE DATE:

LENGTH AND METHOD OF PRESENTATION:

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

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

DESCRIPTION:

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

TERMINAL PERFORMANCE OBJECTIVE (TPO):

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

ENABLING PERFORMANCE OBJECTIVE (EPOs):

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

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

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

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

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

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

EPO #7: Identify the steps involved in adjudicating a case involving national security concerns.

EPO #8: Specify the DHS guidelines concerning the use of classified information in a written decision.

STUDENT SPECIAL REQUIREMENTS:

METHOD OF EVALUATION:

Written Examination – Multiple Choice

TABLE OF CONTENTS

PAGE

OUTLINE OF INSTRUCTION

I. INTRODUCTION

USCIS leadership has identified national security protection as the agency's primary mission, and therefore these issues have become a central element in USCIS adjudications. Prior to the terrorist attacks on September 11, 2001, the legacy Immigration and Naturalization Service (INS) conducted security checks on less than one-third of applicants and beneficiaries seeking immigration benefits. Today, protecting against national security threats is a central mission for USCIS, and security checks are conducted on applicants, beneficiaries, derivatives, and petitioners seeking immigration benefits. USCIS performs security checks regardless of race, ethnicity, national origin or religion.

The security checks may reveal national security or criminal and public safety information, which is relevant to the eligibility of the applicant, beneficiary, derivative or petitioner for the benefit. If any of the various security checks reveal potentially derogatory information about the individual seeking the benefit, that information may impact eligibility and must be assessed as part of the adjudication. This oftentimes involves obtaining and reviewing complex, highly sensitive information resulting in a process that cannot be resolved quickly and may result in a denial of the benefit based on the adverse information.

It is essential for USCIS Officers to understand the background check process and the USCIS policy and procedures for identifying and processing cases with national security concerns. It is also important for USCIS Officers to understand the importance of their role in protecting the national security of the United States by properly handling sensitive information and ensuring that appropriate action is taken when a national security concern is identified.

USCIS continues to strive to meet its goal, ***"To deliver the right benefit to the right person at the right time, and no benefit to the wrong person."***

II. PRESENTATION

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

1. National security-Related Sections of the Immigration and Nationality Act (INA)

National security-related sections of the Immigration and Nationality Act (INA) are provided below for reference purposes. Activity related to national security is described in section 212(a)(3)(A), (B), and (F) and 237(a)(4)(A) or (B) of the INA and includes but is not limited to terrorist activities, espionage, sabotage, and the illegal transfer of goods, technology, and sensitive information outside of the United States.

Ineligibility for Asylum	Section 208(b)(2)(A)
Grounds of Inadmissibility	Section 212(a)(3)(A), (B), and (F)
Designation of Foreign Terrorist Organizations	Section 219
Removal of Aliens Inadmissible	Section 235(c)
Mandatory Detention of Suspected Terrorists	Section 236A
Grounds of Deportability	Section 237(a)(2)(D) and (4)(A) and 4(B)

2. Terms of Reference

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

Known or Suspected Terrorist (KST) hit - is a category of individuals who have been nominated and accepted for placement in the Terrorist Screening Database (TSDB), are on the

[1] See policy memorandum dated April 11, 2008 entitled, *"Policy for Vetting and Adjudicating Cases with National Security Concerns"*.

Terrorist Watch List, and have a specially coded lookout posted in the Treasury Enforcement Communications System(TECS)/Interagency Border Inspection System (IBIS) and/or the Consular Lookout Automated Support System (CLASS), as used by the Department of State.

Non-Known or Suspected Terrorist (Non-KST) NS Concern- is a category of the remaining cases with 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. Individuals and organizations who fall into the Non-KST grouping may also pose a serious threat to national security.

Material Support - Includes but is not limited to the provision of safe houses, transportation, communications, funds, transfer of funds or other material benefit, false documentation or identification, weapons (including chemical, biological, or radiological), explosives, or training for the commission of a terrorist act, to an individual who has committed or plans to commit such activity, or to a designated or undesignated terrorist organization.

Office of Fraud Detection and National Security (FDNS) – The office within USCIS established to enhance the integrity of the legal immigration system by identifying threats to national security and public safety, detecting and combating benefit fraud and removing systemic and other vulnerabilities**.**

Background Check Analysis Unit (BCAU) – A unit within the National Security Branch at Headquarters FDNS (HQFDNS) responsible for providing vetting and providing assistance to the field for cases with identified national security concerns.

National Security Adjudications Unit (NSAU) - A unit within the National Security Branch at HQFDNS responsible for providing adjudications assistance to the field for cases with identified national security concerns.

Background Check Unit (BCU) - Formerly known as the IBIS Triage Unit at USCIS Service Centers. The BCU is responsible for reviewing results of security checks and vetting cases with national security concerns.

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

Letterhead Memorandum (LHM) – A type of official response from the Federal Bureau of Investigation (FBI). USCIS receives LHMs as a result of a positive response to the FBI Name Check request. LHMs contain FBI investigative information. In some cases the FBI is in possession of information provided by another agency that cannot be released to USCIS under the Third Agency Rule. In such cases, the FBI will provide a Third Agency Referral that contains the name of the agency in possession of the relevant information.

Joint Terrorism Task Force (JTTF) - An organization run by the FBI which is responsible for all domestic and international terrorism matters. JTTF is composed of small cells of highly trained, locally based members from U.S. law enforcement and intelligence agencies throughout the United States. There are approximately 100 JTTFs within the U.S. and a National JTTF (N-JTTF), located in Washington, D.C.

Terrorist Screening Center (TSC) – In accordance with the Homeland Security Presidential Directive (HSPD) -6, the TSC was 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. The TSC is administered by the FBI.

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

External Vetting – Consists of inquiries to record owners in possession of the NS information to identify: (a) fact or fact patterns necessary to determine the nature and relevance of the NS concern, including status and results of any ongoing investigation and the basis for closure of any previous investigation; and (b) information that may be relevant in determining eligibility, and when appropriate, removability.

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

Background Check - The process of reviewing all available information on a subject or organization to determine whether the individual or organization poses a threat to the national security or public safety and is eligible for an immigration benefit. The process may include review of results of the security checks; additional systems checks; information obtained from law enforcement agencies, other U.S. agencies, or foreign governments; the A-file or other administrative files; and the application/petition relating to the subject or organization.

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

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

1. Office of Fraud Detection and National Security Division

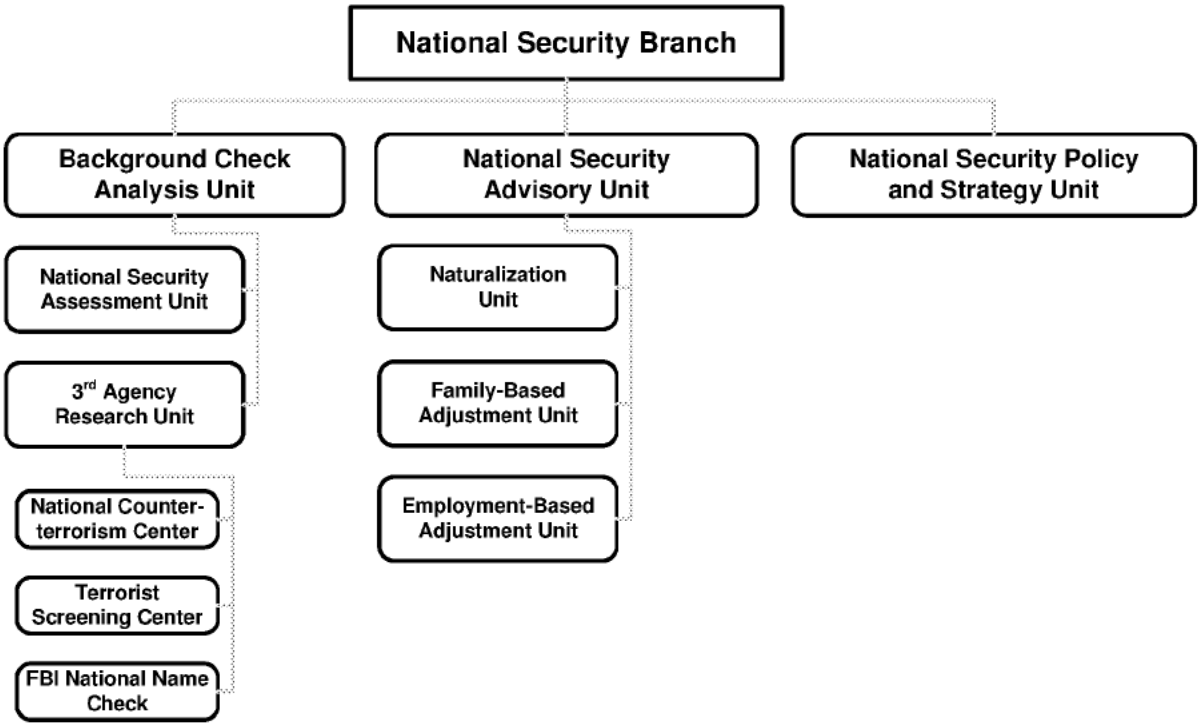
In the context of national security, FDNS assists to develop policy, procedures, and other guidelines, and advises and coordinates on matters involving national security. FDNS also oversees the resolution of security check hits and concerns identified through other sources pertaining to national security.

National Security Branch at Headquarters FDNS
The National Security Branch at HQ FDNS is comprised of the Background Check Analysis Unit (BCAU), National Security Adjudications Unit (NSAU) and the National Security Policy and Strategy Unit (NSPS).

Currently the BCAU conducts vetting on national security referrals also known as National Security Records (NSR) from the field to determine whether the concern is valid as well as provides advice and consultation to the field. BCAU staff is also detailed at three different locations to coordinate with outside agencies on matters of national security: Terrorist Screening Center (TSC), National Counterterrorism Center (NCTC), and the FBI's National Name Check Program (NNCP).

NSAU develops, coordinates, and implements case resolution strategies relating to national security cases. Furthermore, NSAU coordinates with Intelligence and Law Enforcement Agencies to declassify or to obtain permission to use classified information in certain cases.

NSPS provides policy analysis and guidance for the National Security Branch to help shape operations, procedures, and strategies.



2. Office of Domestic Operations

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

Service Center Operations provides operational direction to service centers and manages assignments and monitors the resolution of cases having confirmed or unresolved NS concerns.

Service Centers

Service Centers have established procedures to review all IBIS, FBI fingerprint & FBI name check results when the initial response is received; this includes the immediate review of Rap sheets. All national security and public safety related hits and concerns are referred to local Background Check Units (BCU) for resolution per established operating procedures.

Field Offices

Field Offices have established procedures to ensure all IBIS, FBI Fingerprint & FBI Name Check results have been received, reviewed, and are current prior to the granting of an immigration benefit. Each Field Office has an established referral process to the local FDNS

Immigration Officer for cases identified as having national security concerns. All of these cases are entered into FDNS-DS.

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

Each Headquarters' component of RAIO provides operational direction to its specific component: asylum offices, the Refugee Corps or USCIS offices overseas. RAIO manages assignments and monitors the resolution of cases having national security concerns.

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

Annually, USCIS receives approximately six million applications and petitions for immigration benefits. As part of the background check process, USCIS policy requires the completion of one or more security checks prior to granting immigration benefits. The background check process allows USCIS to conduct a comprehensive review of the facts of the case to include any identified public safety or national security issues. The background check process is not considered complete until USCIS has resolved all identified concerns.

Although only a small percentage of the security checks results in adverse information of a national security, because of the large number of applications filed each year, a significant number result in national security hits requiring intensive review and resolution.

1. Evolution of USCIS Policies for Cases involving National Security Concerns

To fully understand the nature and extent of the national security concerns within the population applying for immigration benefits, the resolution and adjudicative assessment of national security cases was centralized at USCIS Headquarters.

In May 2004, the Office of Fraud Detection and National Security (FDNS) was established at USCIS Headquarters and field offices within the Directorate of Domestic Operations. Part of FDNS's mission was to complete the conduct of background checks to identify applicants, petitioners, and beneficiaries who may pose a threat to national security; and to provide an adjudicative assessment to the field for national security cases in a manner that minimizes the risk to national security and expedites the processing of legitimate applications for immigration benefits.

In March 2005, FDNS was authorized to create a Background Check Analysis Unit (BCAU) at Headquarters to review and resolve all national security and egregious public safety hits resulting from security checks. The centralization policy required that adjudicative action be suspended on cases where a national security or public safety concern had been identified.

On March 29, 2005, the FOCUS Unit was established at USCIS Headquarters within the Directorate of Domestic Operations to apply adjudicative resources to the growing volume of national security cases. FOCUS's mission was to review pending applications and petitions involving national security and egregious public safety concerns and to determine whether any such adverse information had any relevance to an applicant's eligibility for the immigration benefit sought.

On February 3, 2006, USCIS Director Emilio Gonzalez created a new directorate within USCIS, the Directorate of National Security, Records and Verification (NSRV). BCAU as part of FDNS was transferred to this new directorate. FOCUS was also transferred to the new directorate and renamed the National Security Adjudications Unit (NSAU).

NSAU was placed under the auspices of FDNS when it was transferred to NSRV. This permitted closer coordination in the National Security Branch of HQFDNS between the BCAU officers who vet the security check results and the Adjudications Officers within NSAU who assess eligibility for immigration benefits in national security cases.

In cases where BCAU determined that the concern was not credible or no longer existed, the case was returned to the field and released for adjudication. In those cases where BCAU confirmed the concern existed or remained unresolved, the case was forwarded to NSAU for an adjudicative evaluation.

On February 16, 2007, the Field was advised that cases involving public safety concerns no longer required review by HQFDNS. Furthermore, in cases involving national security concerns, the Field was no longer required to suspend adjudication where they could close, dismiss, or deny the application or petition based on other than national security grounds.

In Spring 2007, a selected cadre of Adjudications Officers in the Field were trained by HQ USCIS on procedures for adjudicating cases involving national security concerns. HQ FDNS released the authority to this cadre of adjudications officers to adjudicate cases involving Known or Suspected Terrorists (KST) hits which had been vetted by the BCAU at HQ FDNS. The Adjudications Officers were also given the authority to coordinate with law enforcement on these cases to ensure that law enforcement was aware of the planned adjudicative activities.

2. Controlled Application Review and Resolution Program (CARRP)

On April 11, 2008, USCIS issued the following memorandum *"Policy for Vetting and Adjudicating Cases with National Security Concerns"*. This memorandum outlines USCIS policy for identifying and processing cases with national security concerns also known as Controlled Application Review and Resolution Program (CARRP) and is effective upon the issuance of operational guidance by the Domestic Operations Directorate and the individual components of the Refugee, Asylum, International Operations Directorate (RAIO).

Upon its effective date, this policy memorandum rescinds the following policy memoranda and guidance pertaining to reporting and resolving national security concerns

- *"Processing of Applications for Ancillary Benefits Involving Aliens Who Pose National Security or Egregious Public Safety Concerns,"* dated May 11, 2007;

- *"Processing of Form I-90s Filed by Aliens Who May Pose National Security or Egregious Public Safety Concerns,"* dated May 11, 2007;
- *"National Security Requirements,"* dated February 16, 2007;
- *"National Security Record Requirements,"* dated May 09, 2006;
- *"Permanent Resident Documentation for EOIR and I-90 Cases,"* dated April 10, 2006;
- Appendix A of the Inter-Agency Border Inspection System (IBIS) Standard Operating Procedure, dated March 1, 2006;
- Revised Instructions for Processing Asylum Terrorist/Suspected Terrorist Cases, dated January 26, 2005;
- Section VIII of the Asylum Identity and Security Check Procedures Manual.

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

1. USCIS Standard Security Checks

USCIS conducts security checks to ensure that the applicant, beneficiary, derivative, or petitioner is eligible for the immigration benefit and is not a risk to national security or public safety. In addition to records checks against USCIS immigration systems, these security checks may consist of the:

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

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

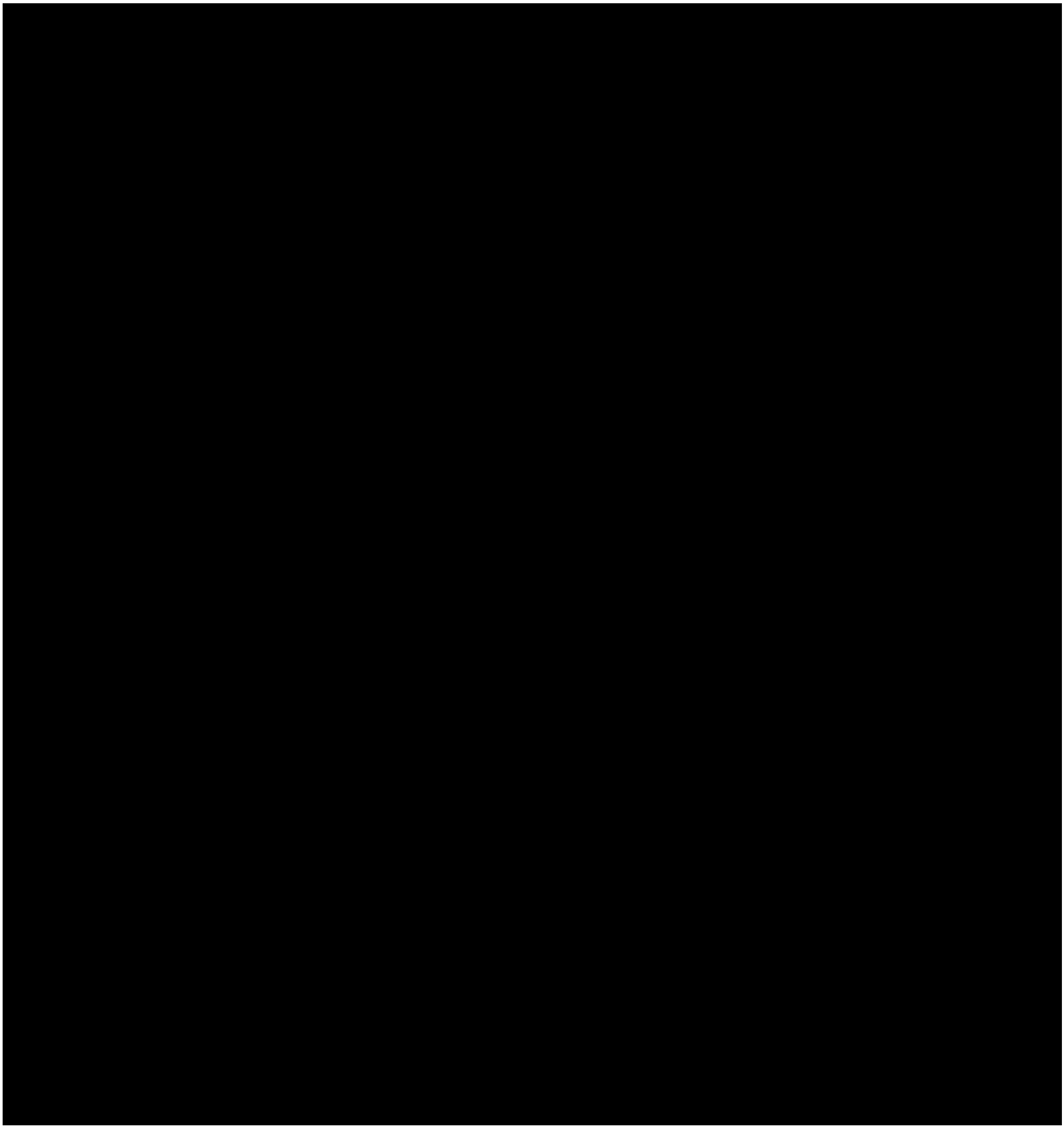
2. FBI Name Check

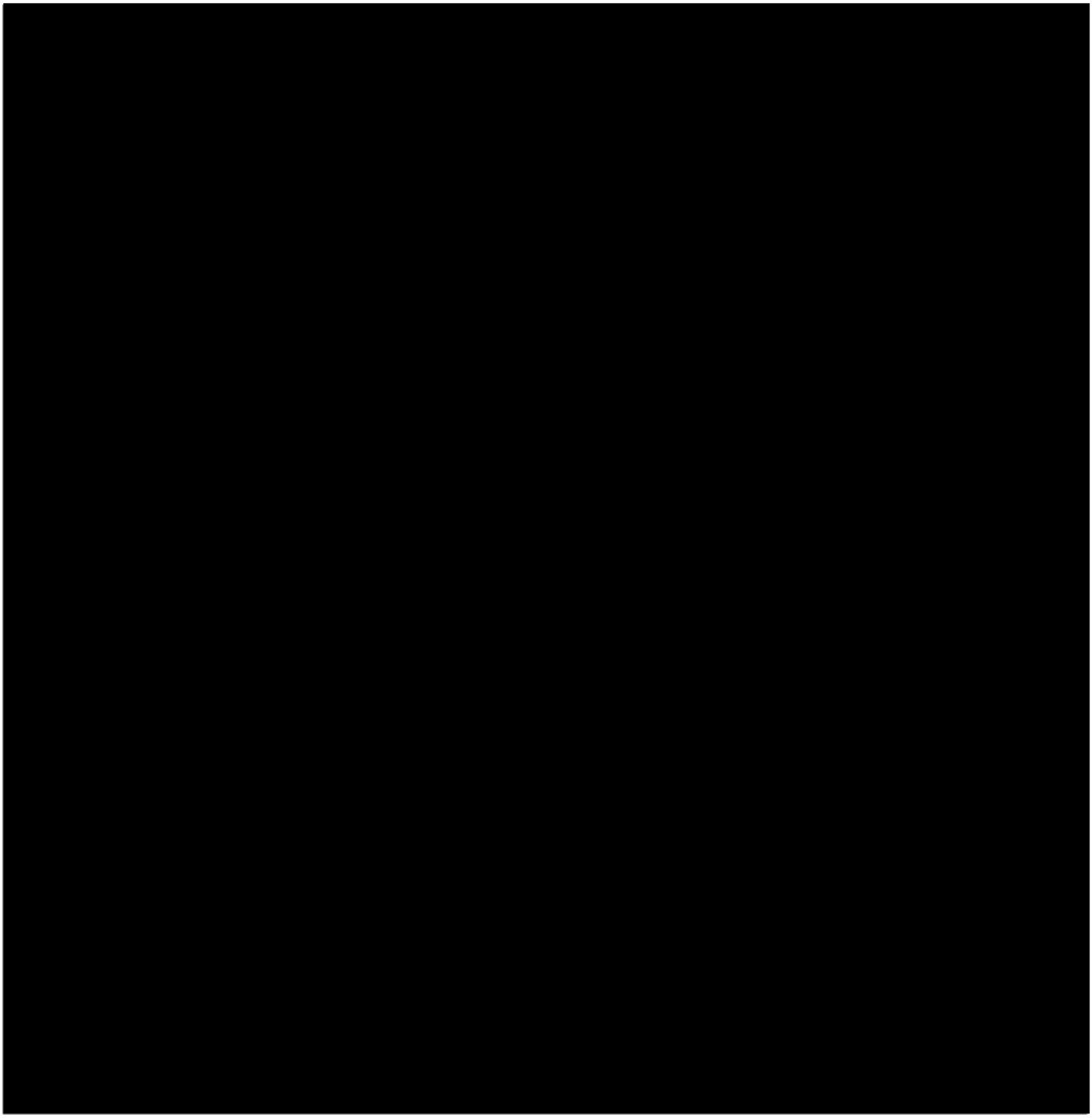
The FBI Name Check is conducted by the FBI's National Name Check Program (NNCP). NNCP reviews and analyzes potentially identifiable documents to determine whether a specific individual has been the subject of or mentioned in any FBI investigation(s), and if so, what (if any) relevant information may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

The results of the FBI Name Check do not necessarily reveal the same information as do the results of the FBI Fingerprint Check or TECS/IBIS.

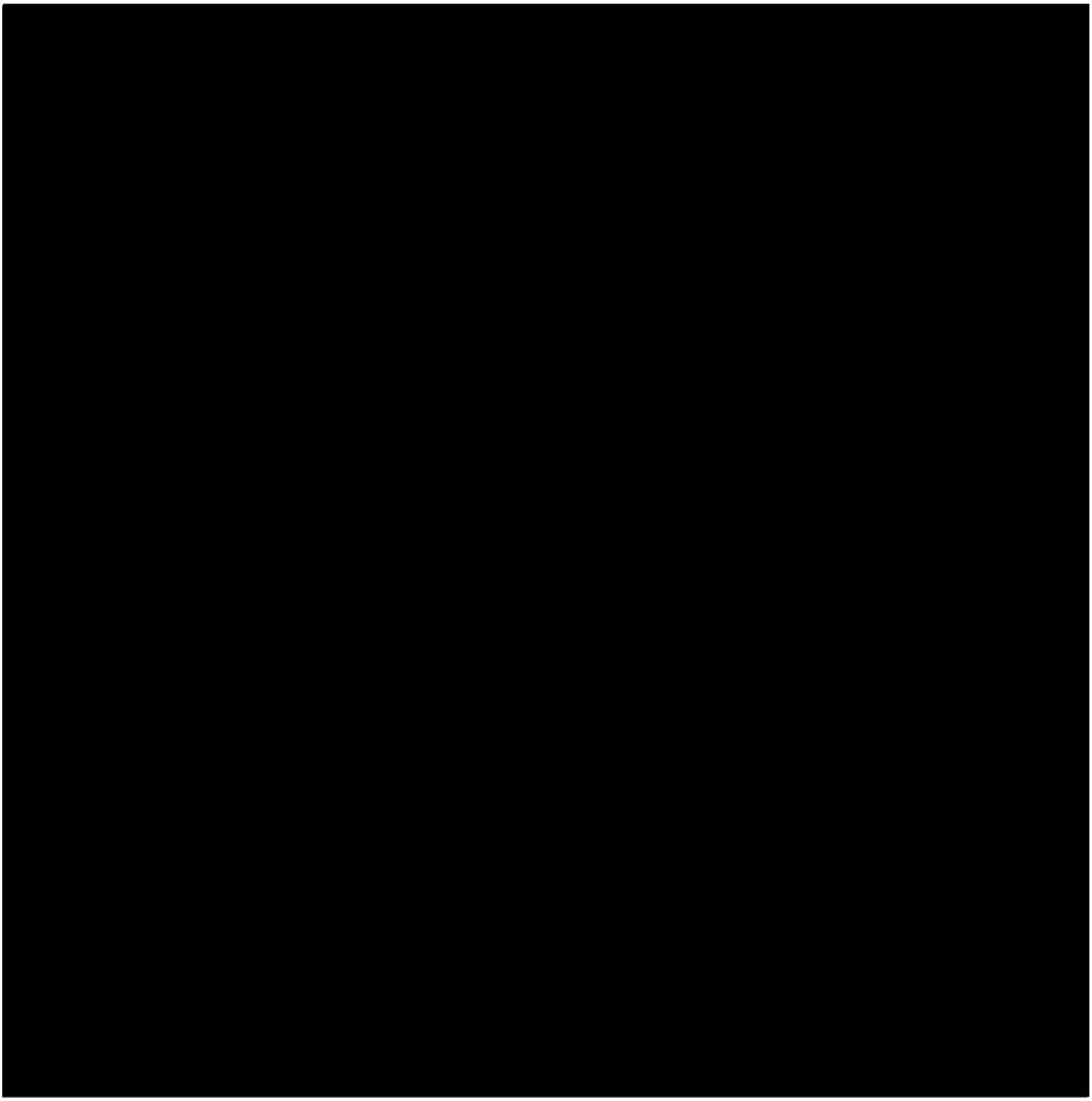
The NNCP conducts manual and electronic searches of the FBI's Central Records System (CRS) Universal Index (UNI). The CRS encompasses the centralized records of FBI Headquarters, field offices, and Legal Attache offices. The CRS contains all FBI investigative, administrative, personnel, and general files.[2]

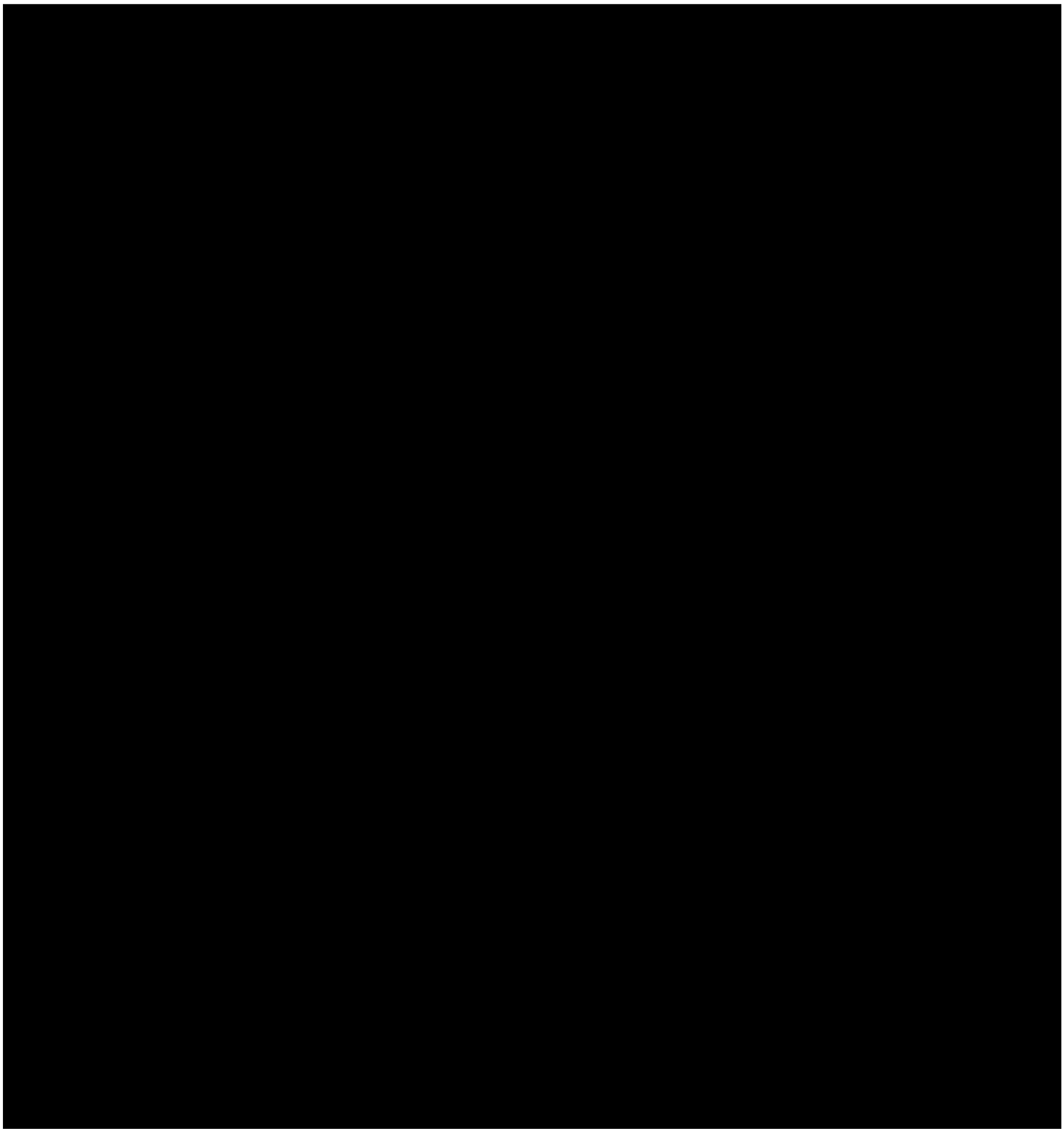
[2] Italicized portions in this section for Name Check are excerpts from the NNCP website, http://www.fbi.gov/hq/nationalnamecheck.htm.

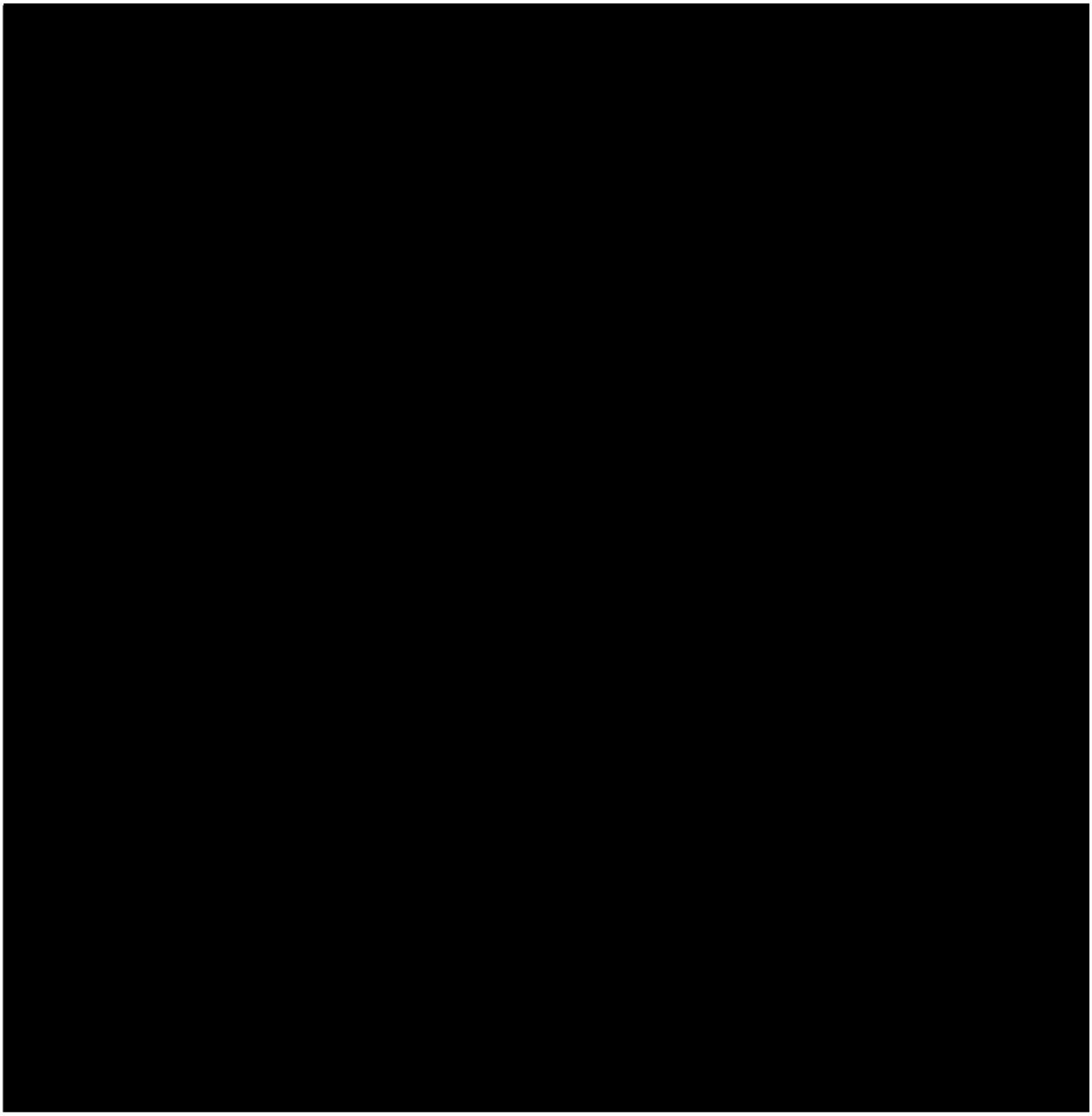


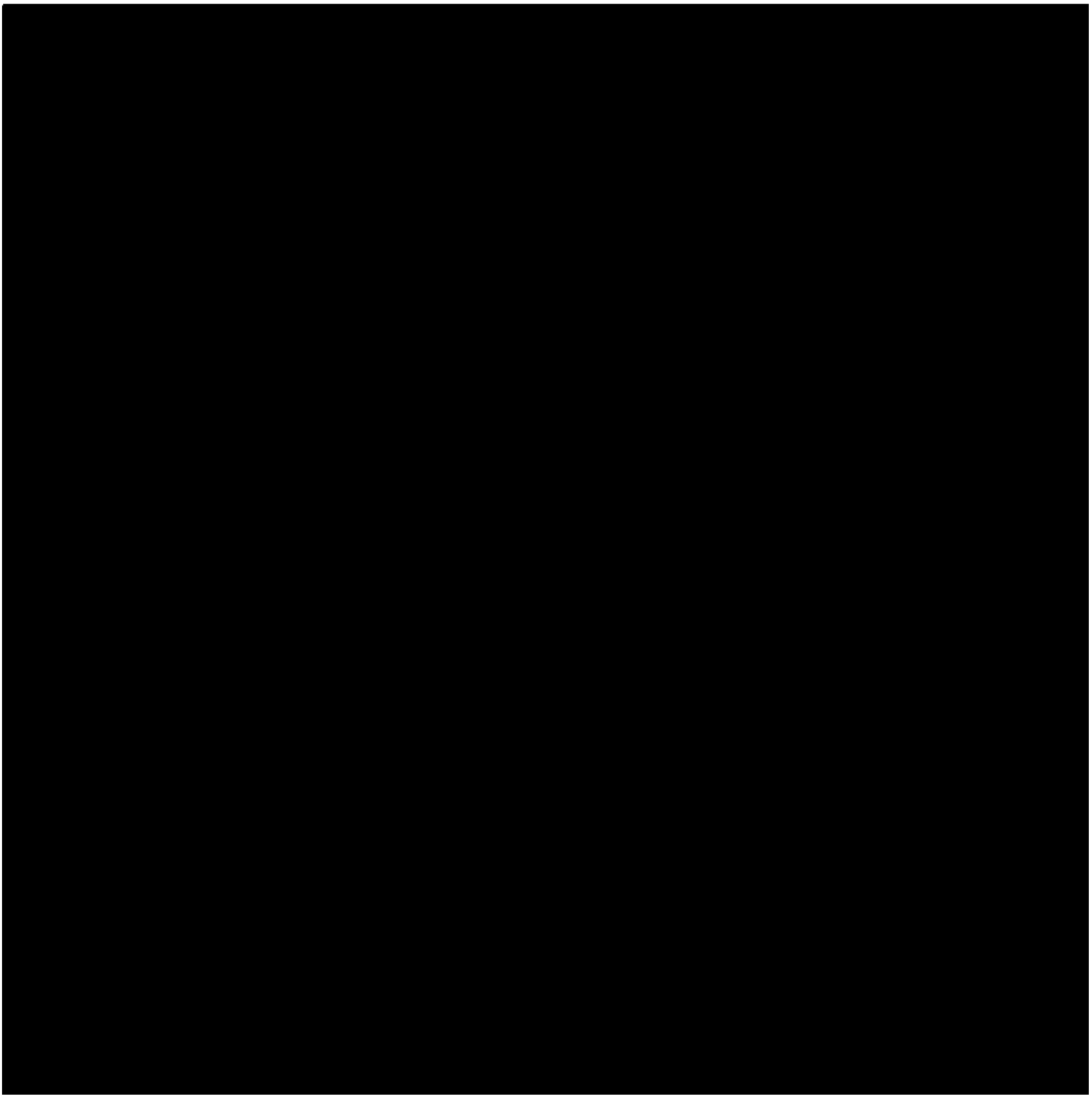


[3] See Appendix for a copy of this memo.









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

d. History of IBIS

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

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

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

e. IBIS Usage

Data in IBIS is "For Official Use Only (FOUO)" and should be marked accordingly. 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)."

All IBIS users must be certified through an on-line security certification test and must be re-certified every two years.

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

f. When to Query IBIS

IBIS queries must be run on the following subjects age 14 and over:

- Applicants
- Petitioners
- Beneficiaries
- Derivatives
- Household Members (for I-600, I-600A, I-290B, and EOIR-29 cases only.)

IBIS checks are not only conducted on the applicant and beneficiary but also on the petitioner (individual, business, organization):

- Employment based petitions
- Religious worker petitions
- To deny immigration benefits to ineligible petitioners in accordance with the Adam Walsh Act

g. Validity of IBIS Checks

IBIS must be run on all new applications/petitions within 15 calendar days of initial receipt. For applications/petitions filed at a service center or a lockbox, this process is run automatically through a process called Batch Processing.

The IBIS query must be valid before a decision can be rendered on a benefit. An IBIS query is valid for 180 days. At the time of adjudication if the validity has expired, a manual IBIS query must be completed.

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

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

6. USCIS Fact Sheet

On April 25, 2006, the USCIS Press Office released a fact sheet entitled, "Immigration Security Checks---How and Why the Process Works". The fact sheet was created for distribution to the public in order to explain the importance and necessity of the security checks as well as possible reasons for delay in the security check process. The fact sheet provides the following information:

- Security checks are performed on every applicant regardless of ethnicity, national origin or religion;
- Security checks enhance national security and ensure the integrity of the immigration process;
- The fact sheet explains the FBI Name Check, FBI Fingerprint Check, and IBIS.

6. Third Agency Rule

Records of other agencies either loaned to USCIS or a part of the USCIS files must be protected from unauthorized disclosure. The contents of an originating agency's report in possession of USCIS shall not be disclosed to another agency without the prior consent of the originating agency.

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

Immigration and Customs Enforcement (ICE), CBP, and the U.S. Secret Service (USSS) are components within the Department of Homeland Security (DHS). In accordance with DHS policy, all DHS components are considered one agency.[5] Information from these components is oftentimes "Law Enforcement Sensitive" and must be protected regardless. Component information shall not be disclosed to another agency without the permission of the owning component.

[5] See DHS memorandum dated February 1, 2007, entitled *"DHS Policy for Internal Information Exchange and Sharing"*

E. EPO #5– Discuss the term "national security concern" and methods used to identify cases involving national security concerns.

This section provides information to help officers recognize when the issue of a national security concern may arise as a result of the security checks, information self-reported by the applicant, beneficiary, derivative or petitioner, or information derived from another source. The USCIS Officer must analyze the facts of the case and consider the totality of the circumstances in order to determine whether a concern exists. This section does not provide an exhaustive list of criteria or methods for identifying national security concerns but should serve as a reference tool for USCIS Officers who are evaluating potential cases.

1. "National Security Concern"

A national security concern exists when an individual or organization has been determined to have an articulable link to prior, current or planned involvement in, or association with, an activity, individual or organization described in 212(a)(3)(A), (B), or (F), 237(a)(4)(A) or (B) of the Immigration and Nationality Act (INA). This includes but is not limited to terrorist activity; espionage; sabotage; and the illegal transfer of goods, technology or sensitive information. This determination requires that the case be handled in accordance with Controlled Application Review and Resolution Program (CARRP) policy[6].

Espionage includes but is not limited to activities of foreign powers and their agents that adversely affect national security such as obtaining inside information on our government's policies and intentions towards other countries; details on U.S. military plans and weapons systems; or our nation's scientific and technological innovations and research, both public and private.

Officers should understand the distinction between foreign intelligence and counterintelligence. The definitions below are cited in Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms".[7]

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

---

[6] See policy memorandum dated April 11, 2008 entitled, *"Policy for Vetting and Adjudicating Cases with National Security Concerns"*.

[7] Publication 1-02 can be found at http://[redacted]

Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

LE

According to the Intelligence Authorization Act (1992) and Executive Order 12333 (1981) which are still enforced today, counterterrorism is considered a subset of the official definition of counterintelligence because counterterrorism shares the same tools, employs the same tactics and benefits from the same strategies as counterintelligence.

2. Foreign Intelligence Surveillance Act (FISA)

The Foreign Intelligence Surveillance Act (FISA) of 1978, Title 50 U.S.C. 1801, permits law enforcement and intelligence agencies to domestically gather foreign intelligence information without requiring probable cause for a crime. FISA prescribes procedures for requesting judicial authorization for electronic surveillance and physical search of persons engaged in espionage or international terrorism against the U.S. on behalf of a foreign power. Although the duties of USCIS Officers do not fall under FISA, USCIS Officers may encounter terminology used under this statute when handling national security cases and therefore should be familiar with this terminology.

"Foreign Power" is defined in Title 50 USC 1801 (a):

- A foreign government or component thereof whether or not recognized by the U.S.;
- A faction of a foreign nation or nations (non-USPER);
- An entity openly controlled by a foreign government;
- A group engaged in international terrorism;
- A foreign-based political organization (non-USPER);
- An entity directed and controlled by a foreign government.

"Agent of a Foreign Power: non-U.S. Person" is defined in Title 50 USC 1801 (b)(1):

- Person who acts in the U.S. as an officer or employee of a foreign power or a member of an international terrorist group;
- Person who acts on behalf of a foreign power that conducts clandestine intelligence activities in the U.S., when that person engages, aids/abets, or conspires in such clandestine activities;

- Person who engages in international terrorism or activities in preparation thereof.

"Agent of Foreign Power: U.S. Person" is defined in Title 50 USC 1801 (b)(2):

- Knowingly engages in clandestine intelligence gathering activities for a foreign power and activities involve or may involve a violation of US criminal law;
- Pursuant to direction of intelligence service or network of foreign power, knowingly engages in any other clandestine intelligence activities for foreign power, and activities involve U.S. criminal law violation;
- Knowingly engages in sabotage or international terrorism or activities in preparation therefore, for a foreign power;
- Knowingly enters U.S. under false or fraudulent identity, or, in U.S., assumes such identity for a foreign power; or
- Knowingly aids, abets, or conspires to engage in one of the first three activities listed above.

U.S. Person (USPER) is also defined in this Title:

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

3. Terrorist Activity

USCIS Officers should understand the scope of the following terms defined in section 212(a)(3)(B) of the INA: "Terrorist Activity", "Engage in Terrorist Activity", and "Representative". The terrorism provisions in the INA were expanded by the USA PATRIOT Act and the REAL ID Act. These provisions cover more conduct than any of the over twenty other federal legal definitions of terrorism. Such conduct, among other, is covered under the INA for an individual who:

- Is a member of a designated or undesignated terrorist organization;
- Has been previously involved with or likely to engage in terrorist acts or activities;
- Received military training from or on behalf of a terrorist organization;
- Is a spokesperson for or member of designated or undesignated terrorist organizations;
- Is a spokesperson for or member of a group that endorses or espouses terrorist activity;
- Is the spouse or child of an alien who is inadmissible under terrorist grounds;
- Provided material support to designated or undesignated terrorist organizations.

a. Terrorist Attack Cycle

LE-DP

LE-DP

4. Terrorist Organization

Section 212(a)(3)(B)(vi) of the INA defines "Terrorist Organization" and delineates these organizations into three tiers.

a. Tier I

Designated Foreign Terrorist Organizations (FTO) are those designated by the Secretary of State under section 219 of the INA. *These organizations threaten U.S. nationals or the national security of the U.S. and* include such organizations as HAMAS, Al Qaeda, Hizballah, and Revolutionary Armed Forces of Colombia (FARC).

b. Tier II

Terrorist Exclusion List (TEL) provides a list of organizations designated by the Secretary of State in consultation with the AG or Secretary of DHS. There is no requirement that these organizations threaten U.S. nationals or the national security of the U.S.

A list of Tier I and Tier II organizations can be found at http://www.state.gov/.

c. Tier III

The definition of "undesignated terrorist organization" allows for any group of two or more individuals to constitute a "terrorist organization" under the INA if it engages in terrorist activity, or has a subgroup that engages in terrorist activity, even if the group or organization has not been designated as such through INA section 219 or through the Terrorist Exclusion List process. There is no official list for Tier III organizations.

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

The INA provides the Secretary of Homeland Security with the authority, in consultation with the Secretary of State and Attorney General, to conclude in his sole unreviewable discretion, that an organization should not be considered a terrorist organization under this section solely by virtue of having a subgroup that engages in terrorist activity.

Furthermore, there is an exception for some of the provisions related to Tier III organizations if the applicant can "demonstrate by clear and convincing evidence that he did not know, and reasonably should not have known, that the organization was a terrorist organization". This exception applies to (1) members of; (2) those who solicit funds, things of value or members for; and (3) those who provide material support to; Tier III (undesignated) terrorist organizations. The exception does not apply to representatives of undesignated terrorist organizations.

5. Material Support

a. Definition

"Material support" as defined in section 212(a)(3)(B)(iv)(VI) of the INA includes "a safe house, transportation, communications, funds, transfer of funds or other material financial benefit, false documentation or identification, weapons (including chemical, biological, or radiological weapons), explosives, or training". Food, housing, and money (war tax, ransom, extortion, donations) would also be considered material support.

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

b. Exceptions and Exemptions

An applicant who provided material support to an undesignated terrorist organization will not be found inadmissible or deportable on the basis of that support if the applicant can demonstrate *by clear and convincing evidence* that he or she did not know, and should not reasonably have known, that the organization was a terrorist organization.

Furthermore, section 212(d) of the INA, as revised by the REAL ID Act, includes a discretionary inapplicability provision for the material support ground of inadmissibility. This exemption can be exercised by the Secretary of Homeland Security, only after consultation with the Secretary of State and the Attorney General.

For those applicants who provided material support to a Tier III organization *and have met the threshold requirements*, Adjudications Officers will consider whether the applicant is eligible for one of the Tier III exemptions. The Tier III exemptions can be divided into two categories:

1) the Tier III duress exemption and
2) the group-based Tier III discretionary exemption for material support. The following organizations fall under the discretionary exemption for material support.

- Karen National Union/Karen National Liberation (KNU/KNL)
- Chin National Front/Chin National Army (CNF/CNA)
- Chin National League for Democracy (CNLA)
- Tibetan Mustangs
- Kayan New Land Party (KNLP)
- Arakan Liberation Pary (ALP)
- Cuban Alzados
- Karreni National Progressive Party (KNPP)
- Front Unifie de Lutte des Races Opprimees (FULRO)
- Hmong groups and individuals

If an exemption is granted under section 212(d)(3)(B)(i) of the terrorist-related inadmissibility ground, and if no other national security concern is identified, no further vetting is necessary and the application may continue through the routine adjudication process.

6. Terrorist Financing List

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

The Department of the Treasury Office of Foreign Assets Control (OFAC) maintains on its website a list of individuals and groups designated under this executive order. The list can be found on the OFAC's website at http://www.treas.gov/offices/enforcement/ofac/

7. State Sponsors of Terrorism

The Department of State (DOS) also designates "State Sponsors of Terrorism"[8]. More detailed information can be found at "Overview of State Sponsored Terrorism" in Country Reports on Terrorism at the DOS website. Below are a list of the current designees:

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

In addition to the resources found at the DOS website, a list of Special Interest Alien (SIA) Countries may be found in the Customs and Border Protection (CBP) SIA Handbook. The handbook was last updated on March 1, 2008 and contains thirty-four countries and two territories considered to be Special Interest Countries. This document is not for public dissemination but may assist USCIS Officers in determining whether further review and vetting is required.[9]

---

[9] See Appendix for SIA Handbook.

8. Known or Suspected Terrorist (KST) Hit

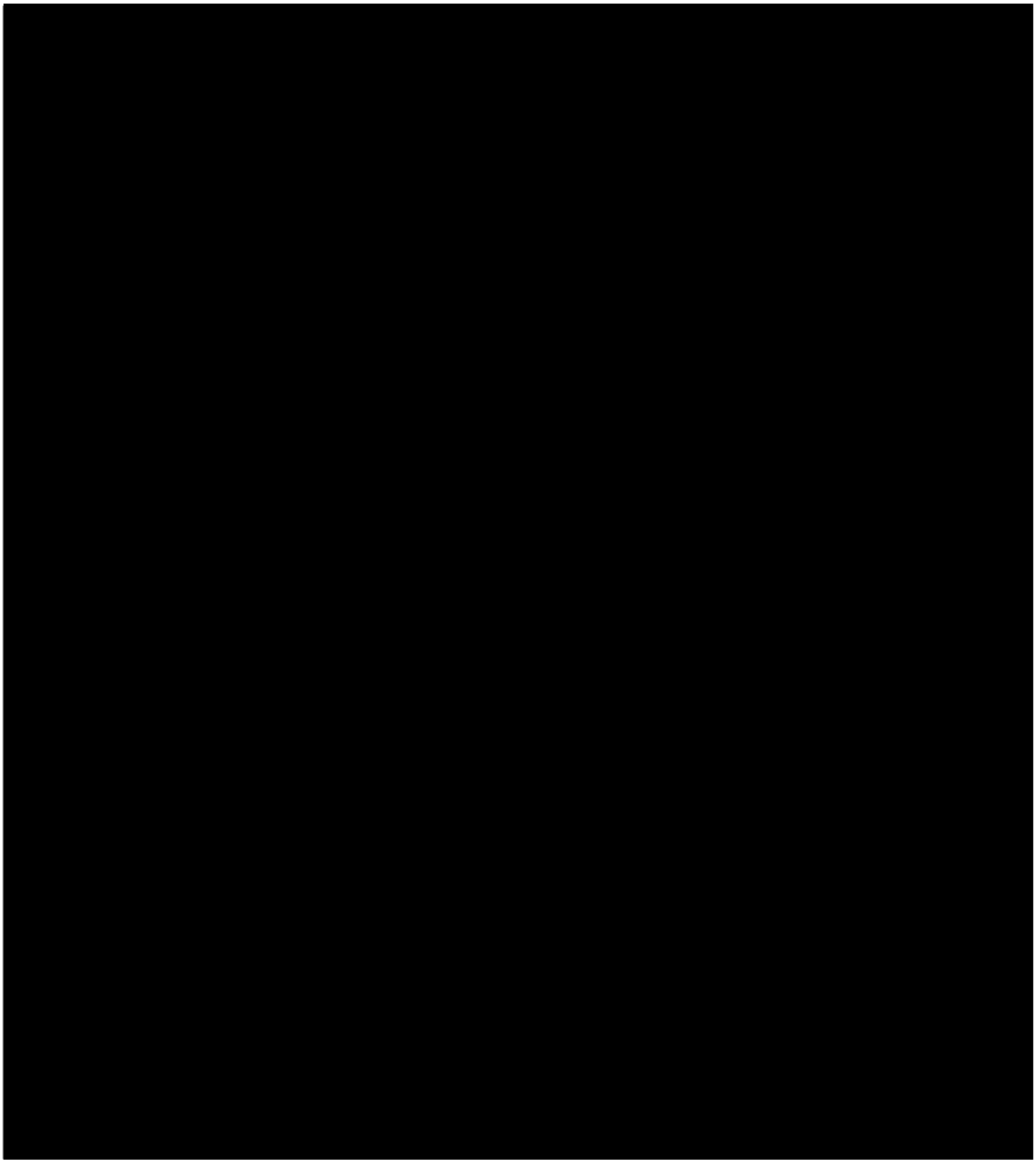
a. Definition
A KST hit is a category of individuals who have been nominated and accepted for placement in the Terrorist Screening Database (TSDB), are on the Terrorist Watch List, and have a specially coded lookout posted in the TECS/IBIS) and/or the Consular Lookout Automated Support System (CLASS),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

b. Homeland Security Presidential Directive-6
On September 6, 2003, the Homeland Security Presidential Directive-6 (HSPD-6) was signed into effect to further the integration and widen the use of terrorist screening information. It established the Terrorist Screening Center (TSC) to consolidate U.S. Government terrorist screening information. In addition, HSPD-6 directed federal agencies to provide appropriate terrorist information to the National Counterterrorism Center (NCTC), which in turn provides the TSC access to all appropriate terrorist information or intelligence.

The Terrorist Identities Datamart Environment (TIDE) is the U.S. Government's central repository of information on international terrorist identities. TIDE supports the U.S. Governments's various terrorist screening systems or "watchlist" and the U.S. Intelligence Community's overall counterterrorism mission.

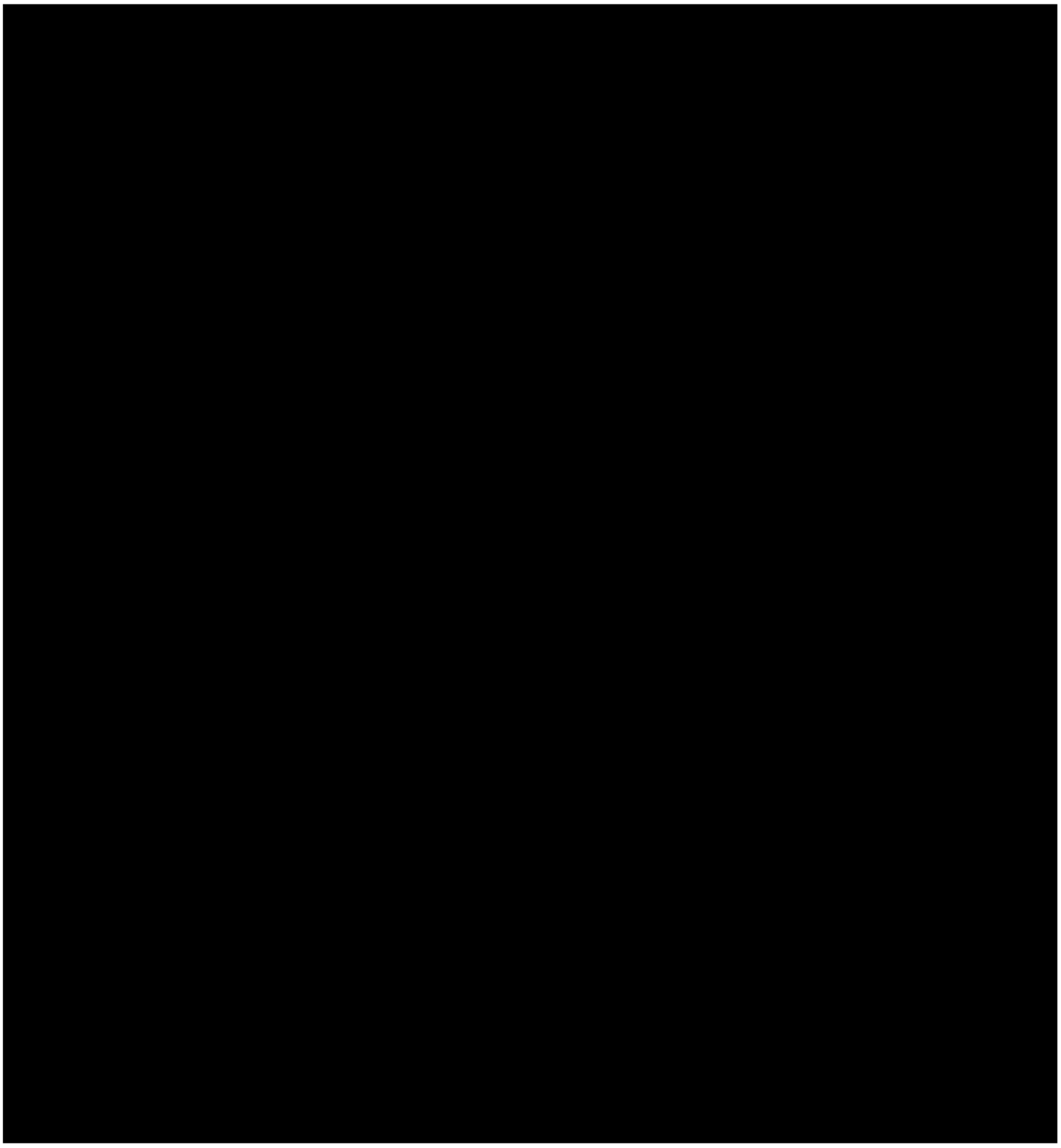
The TIDE database includes, to the extent permitted by law, all information the U.S. government possesses related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to terrorism, with the exception of Purely Domestic Terrorism information.

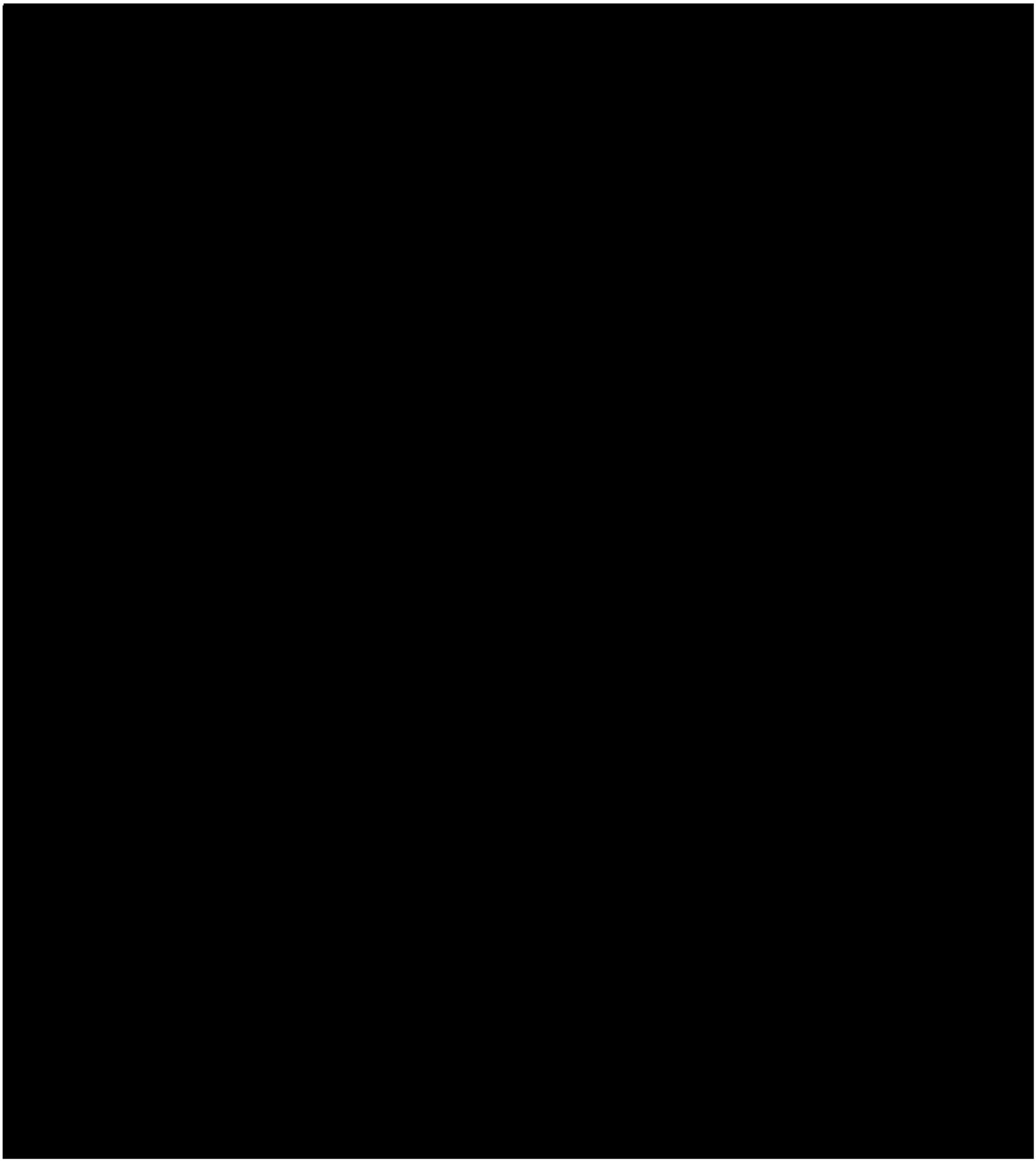
Information from TIDE is imported into the Terrorist Screening Database (TSDB), an unclassified but restricted database that houses the Terrorist Watchlist. Individuals on this list are considered to be Known or (appropriately) Suspected Terrorists (KST).

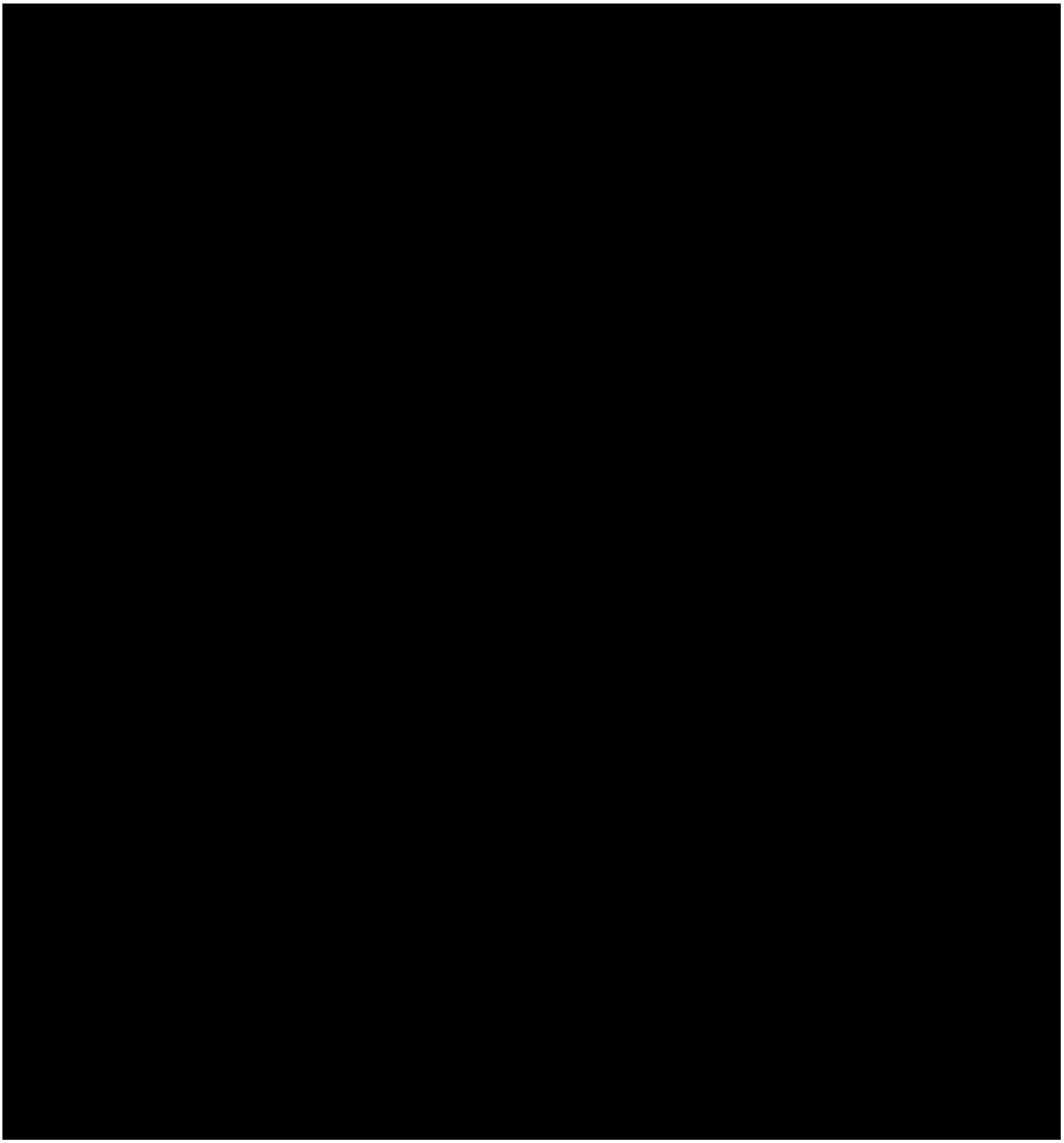


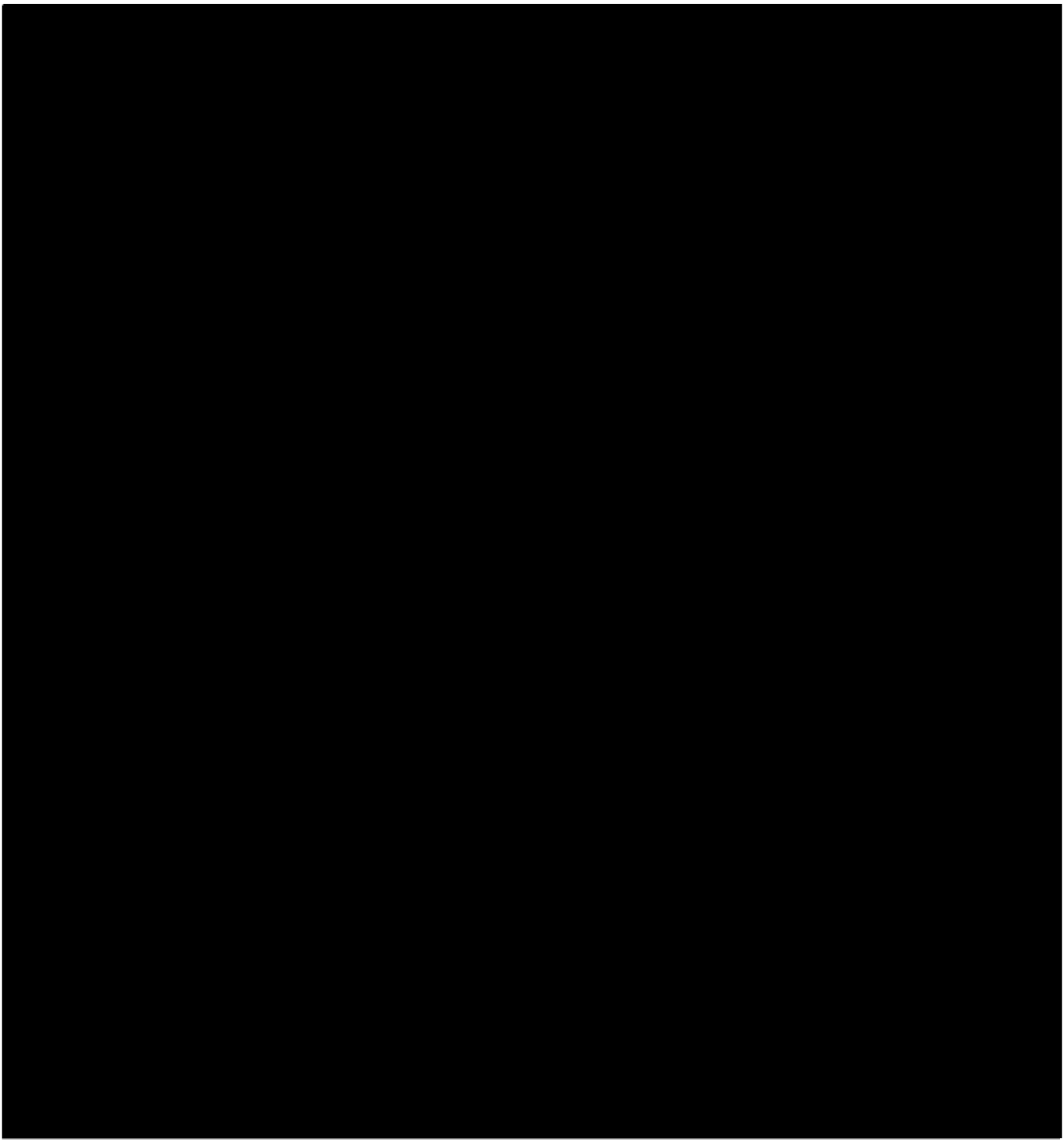
[redacted]

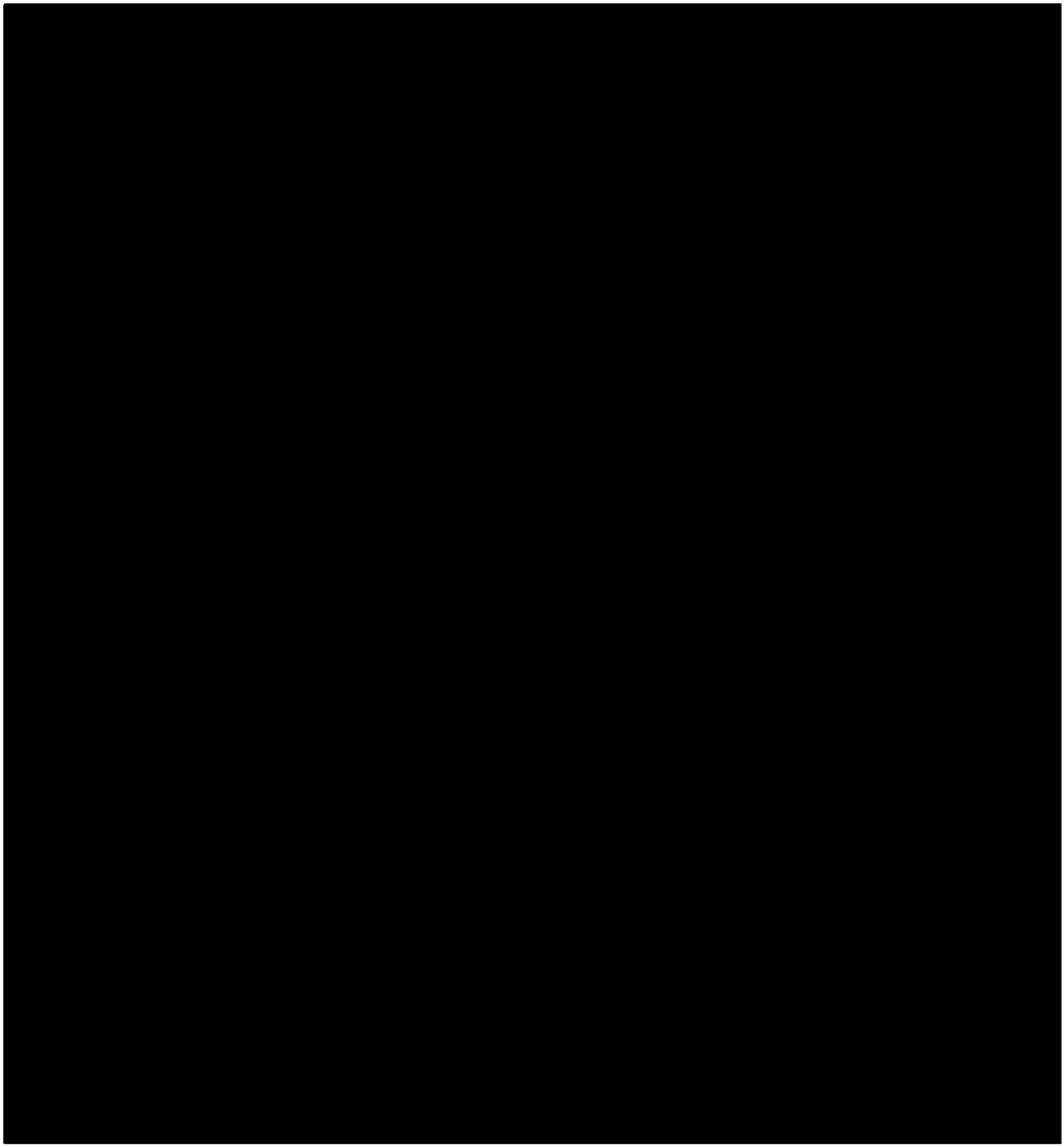
[redacted]

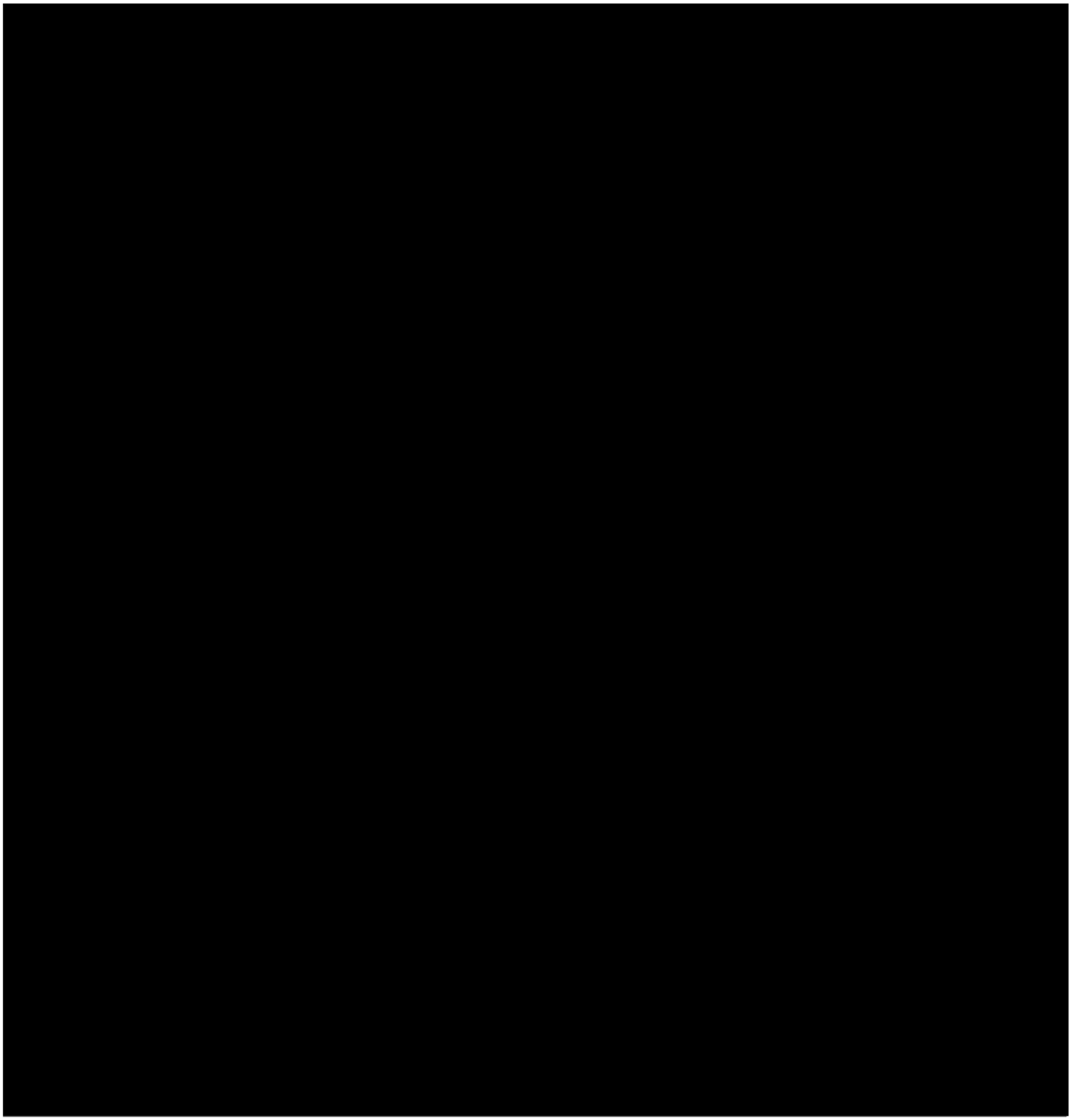












[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

f. Considerations for Information Sharing

During coordination, the Officer may desire or be requested to share information with the outside agency. In such cases, the Officer should remain cognizant of any restrictions that may apply such as the Privacy Act (PA), confidentiality provisions for asylum, legalization, Adam Walsh Act, or the Violence Against Women Act (VAWA), and the Third Agency Rule. Many of these provisions have exceptions relating to law enforcement use.

Officers are reminded that asylum confidentiality is breached when unauthorized disclosure of information in or pertaining to the asylum application allows the third party to link the identity of the applicant to the fact that the applicant has applied for asylum; specific facts or allegations pertaining to the individual asylum claim contained in an asylum application; or fact or allegations that are sufficient to give rise to a reasonable inference that the applicant has applied for asylum. Authorized disclosure can be obtained through written consent of the asylum applicant or specific authorization from the Secretary of Homeland Security. Disclosure may also be made to U.S. government officials or contractors and U.S. federal or state courts on a need to know basis related to certain administrative, law enforcement, and civil actions. Relatives and beneficiaries of the asylum applicant or asylee are considered third parties.[11]

Part I, Section 14 of the Records Handbook[12] addresses how to handle requests from outside agencies to review USCIS files. Outside agencies may be permitted to review a USCIS file for law enforcement purposes and under the routine use provision described by the specific Privacy Act notice for the type of record requested. State or local agencies who want access to records for reasons other than law enforcement or a routine use purposes described by the Privacy Act

[11] See Memorandum entitled "Confidentiality of Asylum Applications and Overseas Verification of Documents and Application Information" dated June 21, 2001 and Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants dated June 3, 2005.

[12] The Record Handbook can be found on the DHSONLINE Portal, at the USCIS Office of Records Services website: http://ors.uscis.dhs.gov/pol_imp/roh/index.htm.

notice may file a Freedom and Information Act (FOIA) request. Any questions regarding the sharing of files should be addressed to the Records section of USCIS.

Information regarding FOIA or the Privacy Act may be found at the USCIS Office of Records Services website[13]. A contact list of FOIA/Privacy Officers is also provided on the website.

g. Other Considerations for Non-KST External Vetting

When coordinating with law enforcement, the Officer should understand the importance to law enforcement agencies of the chain of custody of evidence in criminal proceedings. The Officer should also be aware that agencies post hits in TECS for a variety of reasons. Some hits are to gather information and evidence for criminal prosecution and some hits are for informational and historical purposes. Other hits are for intelligence collection which may support investigative initiatives or may be for targeting or pattern analysis. The objective of the conversation with the record owner is to determine if the reason the hit was posted was based on an articulable concern.

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

h. National Targeting Center (NTC) IBIS Hits

The NTC was established on October 22, 2001 within CBP. It is a 24/7 operation with the centralized mission of coordinating anti-terrorism targeting and supporting all CBP Anti-Terrorism activities. NTC supports and responds to inquiries from the field, conducts tactical targeting to identify actionable targets, develops Automated Targeting System (ATS) rules, and supports Intelligence Driven Special Operations (IDSO). All Terrorist Watch list encounters by CBP are processed through the NTC. Liaisons assigned to the NTC-P: U.S. Coast Guard, ICE, TSA, Office of Intelligence, Federal Air Marshal Service and FBI.

Frequently Asked Question

CBP's website[14] on the DHSONLINE Portal provides the answer to the following frequently asked question:

[13] http:/[redacted]

[14] http://[redacted]

Q:

LE

A:

LE

Handling NTC Hits

LE

All other hits requesting contact with the NTC should be vetted by the local ICE liaison as indicated above.

i. Guardian Threat Tracking System

The Guardian Threat Tracking System is an FBI web-based counterterrorism incident management application that allows terrorism threats and suspicious activities to be viewed instantaneously by all users. The purpose of the system is to ensure that threat information is available immediately to all users, to have the capability to search incidents for trends and patterns to be able to forward threat data to other divisions or users and to ensure that no terrorism incident is left uninvestigated.

j. Joint Terrorism Task Force (JTTF)

JTTF was established in the 1980s. The FBI is the lead agency for terrorism investigations and the JTTFs. JTTFs serve three main purposes: prevent terrorist attacks; respond to and investigate terrorist incidents or terrorist-related activity; and identify and investigate domestic and foreign terrorist groups and individuals targeting or operating within the U.S.

The task forces are composed of federal, state, local agencies and are located in over 100 locations throughout the U.S. The National JTTF (N-JTTF) located at FBI headquarters, includes representatives from a number of other agencies.

USCIS liaises with JTTF through the ICE representative on JTTF. The following list of agencies are full-time members of JTTFs:

- Air Force Office of Special Investigations (AFOSI)
- Bureau of Alcohol, Tobacco, and Firearms (ATF)
- Central Intelligence Agency (CIA)
- Customs and Border Protection (CBP)
- Defense Criminal Investigative Service
- Department of Interior's Bureau of Land Management
- Diplomatic Security Service (DSS) (within DOS)
- Federal Protective Service (FPS) (within ICE)
- Immigration and Customs Enforcement (ICE)
- Internal Revenue Service (IRS)
- Naval Criminal Investigative Service (NCIS)
- Postal Inspection Service
- Treasury Inspector General for Tax Administration
- U.S. Border Patrol (within CBP)
- U.S. Park Police
- U.S. Army
- U.S. Marshall Service (USMS)
- U.S. Secret Service (USSS)

k. Intelligence Community

Executive Order 12333, "United States Intelligence Activities" dated December 4, 1981, requires all government agencies and departments involved in intelligence activities to provide the President and the National Security Council with intelligence information to protect the United States from security threats. Government agencies and departments within the executive branch that have a national intelligence mission are collectively called the Intelligence Community (IC). Members of the IC include:

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

More recently, Executive Order 13354, "National Counterterrorism Center" dated August 27, 2004, requires all government agencies that possess or acquire non-domestic terrorism and counterterrorism information to immediately notify the National Counterterrorism Center (NCTC). [15]

Requests for information from the intelligence community should be routed to HQFDNS. HQFDNS has the capability to query classified systems and send official requests to members of the intelligence community.

3. Deconfliction

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

Deconfliction may take place at any stage during the adjudication process. It may even occur multiple times during the course of adjudication of a single application or petition. Since FDNS Immigration Officers, and in certain instances, officers within the Background Check Units (BCU), are the primary liaison with the law enforcement community, these Officers should deconflict with the appropriate record owner.

The primary goal of deconfliction is to ensure that USCIS actions will not interfere with the interest or investigation of another agency. During the course of coordinating with the outside agency, the USCIS Officer may obtain information relating to the subject's eligibility, admissibility, or removability.

External vetting differs from deconfliction in that the primary goal of external vetting is to obtain national security information from the outside agency in order to determine the nature and extent of the concern. While coordinating with the outside agency, the USCIS Officer may likely obtain information that will assist USCIS in adjudicative decision such as information relating to the subject's eligibility, admissibility, or removability.

USCIS Officers should ensure any information that is obtained during deconfliction or external vetting is appropriately marked (e.g. FOUO or by classified markings), protected and not disclosed without the appropriate authorization. When documenting the results of external vetting and deconfliction, the USCIS Officer should annotate the source and the date.

---

[15] Excerpts describing Executive Order 12333 and 13354 are taken from DHS OIG Report, OIC-08-29, entitled, "The DHS Process for Nominating Individuals to the Consolidated Terrorist Watchlist" dated February 2008.

4. Documenting Activities

Documenting vetting and deconfliction activities is required in order to outline a set of facts that can be used to determine whether a national security concern exists, existed at one time but is no longer present or has not yet been eliminated to the satisfaction of the investigating agency.

Documenting also provides a record of the status and results of security and systems checks, as well as results of inquiries to and responses from offices within USCIS, components within DHS and external agencies which provides information relevant to USCIS' determination of eligibility.

The Officer must document the results of vetting and deconfliction activities on the non- record side (right-side) of the file and in the appropriate tabs of FDNS-DS. These activities include the results of systems checks, whether positive or negative, as well as inquiries to law enforcement and IBIS record owners. Officers are reminded that classified information may **NOT** be entered into FDNS-DS or placed. Furthermore, classified information may not be placed in an immigration file without that file being classified by the USCIS Office of Records. The Records Division will make the determination as to whether a classified temporary file should be made.

The source of information and date the information is obtained should be clearly annotated in order to protect against any unauthorized disclosure of Third Agency information or information protected by confidentiality provisions, such as Asylum, VAWA, Legalization, etc.

If results of an internet search are referenced, the website address (URL) and date the information was retrieved from the website should be annotated in the record at a minimum.[16]

[16] UCLA Library "Citing Internet Sources" website Retrieved March 31, 2008 from http://www.library.ucla.edu/url/referenc/citing.htm, provides examples of citing websites as references.

Ensure that the appropriate caveats are on the prepared documents (e.g. memoranda to file, e-mail correspondence).

> FOR OFFICIAL USE ONLY (FOUO) - LAW ENFORCEMENT SENSITIVE
> This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO. It contains information that may be exempt from release under the Freedom of Information Act (5 U.S.C.§ 552).
>
> Add below to FOUO caveat when TECS/IBIS information is present:
> This document and the data herein are derived from TECS and are loaned to USCIS for official use only. This document or the information contained herein should be directed to the agency from which the document/information originated or Customs and Border Protection - Freedom of Information Act (FOIA) Office. Disclosure provisions have been established by the document, Memorandum of Understanding between Customs and Border Protection (CBP) and U.S. Citizenship and Immigration Services (USCIS) for use of the Treasury Enforcement Communications System (TECS).

The Officer may desire to place the DHS FOUO Coversheet on top of the record of vetting activities in the file. This coversheet is available in the Department of Homeland Security Management Directive System MD Number: 11042.1 entitled "Safeguarding Sensitive But Unclassified (For Official Use Only) Information".

EPO #7: Identify the steps involved in adjudicating a case involving national security concerns.

Adjudication of national security cases is a process which requires a solid knowledge of the law, great attention to detail, the ability to conduct research, the ability to clearly articulate ideas verbally and in writing and communication skills in order to coordinate with internal components of USCIS and with external agencies. The process is meant to ensure that USCIS does not grant a benefit to an individual who poses a threat to national security and is not eligible for the benefit. Often the adjudication process is time intensive and laborious due to the sensitivity and complexity of the nature of the concern.

Of utmost importance, is that the Officer does not disclose third agency, sensitive or classified information without the express permission and/or appropriate authority to release that information. When there is an ongoing national security or criminal investigation, close coordination with the respective investigating agency for deconfliction purposes is required so as not to disrupt or impede the investigation. When national security issues have been identified that would make the applicant inadmissible or ineligible, USCIS will seek to deny the application. Before relying on the national security grounds for denial, however, USCIS will seek to deny based on any other legal grounds. In so doing, USCIS seeks to avoid disclosure of LEA information except as a last resort and only if coordinated with the LEA.

To more effectively conduct internal and external vetting, the Vetting Officer should understand the steps involved in adjudicating a national security case as well as the types of information the Adjudications Officer relies upon to determine eligibility for the benefit sought. The Vetting Officer should look for any principles and techniques used by the Adjudications Officer which may enhance the vetting process.

1. Adjudicative Steps for Cases Involving National Security

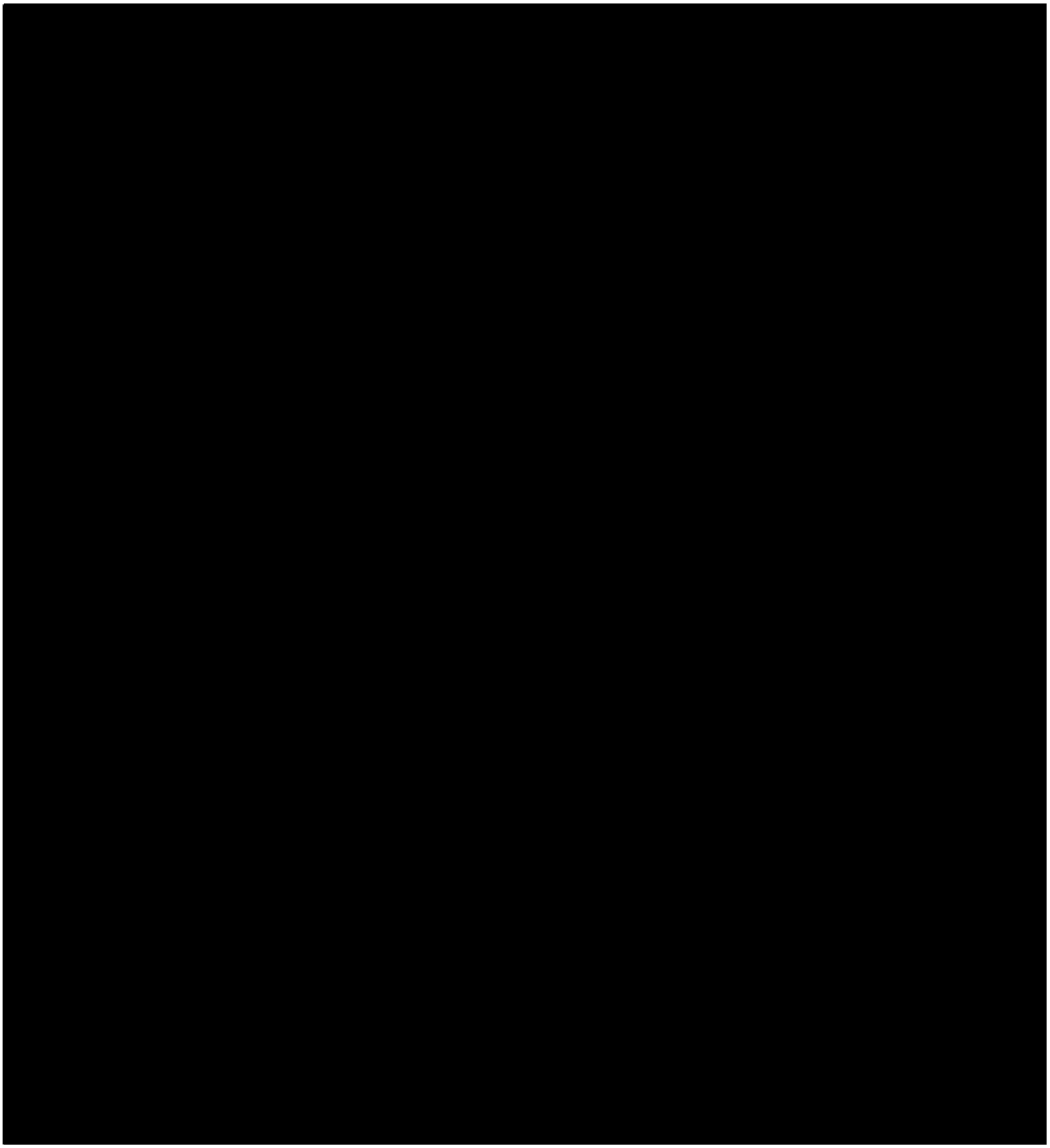
a. Credibility

A major consideration for the Adjudications Officer is the overall credibility of the individual applying for the benefit which can be established by reviewing any applications, supporting documents, and testimony for consistency.

Evaluation of the credibility of an individual's testimony is fundamental to the evaluation of the individual's eligibility and, in some cases, is the determining factor. A credibility finding must be clearly articulated and based on objective facts; it cannot be based on "gut feelings" or intuitions. Intuition and gut feelings are unreliable, particularly when interviewing a stranger from a different culture and sometimes through an interpreter.

To help determine credibility of the individual, an officer needs to review the entire file, compare applications and petitions, and make a list of all discrepancies found in the applications and petitions. The officer must consider if the information on the application and during the interview is consistent with all systems checks, open source information and supporting documentation provided by the applicant. The officer must also provide the individual with a chance to respond to inconsistencies either during the interview or through a written notice such as a Notice of Intent to Deny.

[redacted]



[redacted]

3. Litigation

Within the national security workloads are a number of cases that present special issues—particularly in the naturalization area. Law, regulations, court decisions, media coverage, and a number of other factors work to create pressure for the issuance of decisions, often before USCIS has resolved all national security issues. It is important to know the options an Adjudications Officer has when managing these cases. Over time, strategies have been developed to ensure that "no decision is issued before its time." These strategies do not promote needless delay of decisions; indeed, it is in the national interest to move on a national security threat as soon as possible and refer the case for further proceedings whenever possible. The goal is to ensure that no individuals who pose a threat to national security are granted benefits.

Even though the Vetting Officer does not generally adjudicate these cases, it is still important for the Vetting Officer to be aware of court deadlines and what they mean for USCIS. Remember, the goal is for the Adjudications Officer to adjudicate when ready and not before. An important key to these cases is communication between the Vetting and Adjudications Officers.

Below are some of the problems that are likely to be encountered as the Adjudications Officer works national security cases:

a. 336(b) Actions
Naturalization applicants may file Federal Court actions asking the court to naturalize them when USCIS has not adjudicated an Application for Naturalization within 120 days of an interview. With these types of actions, the court has sole jurisdiction. The Adjudications Officer must know the local court they are dealing with and must always communicate with USCIS Counsel when handling the case.

b. Mandamus Actions
Applicants and petitioners often file Federal Court actions to compel USCIS to act on an application or petition when the applicant or petitioner feels that he/she has waited too long for a decision. A mandamus action may be filed on the basis of any pending application or petition. In these cases, the court will issue instructions to USCIS and other agencies to complete certain tasks within certain timeframes. For instance, a court may order the FBI to complete the FBI Name Check request within 45 days of the court's order with USCIS instructed to adjudicate the application within 45 days of the completion of name check. But, for these types of cases it is important to remember that USCIS maintains jurisdiction over the filing unlike in the 336(b) suits. Officers must be mindful of the court deadlines and notify USCIS Counsel as early as possible if USCIS cannot meet those deadlines. It is better to ask for an extension than to be found in contempt of court.

In either case, it is important that Adjudications Officers be mindful of court orders, restrictions on adjudicative authorities, and the need for communication between operations, USCIS Counsel, and the Assistant US Attorney (AUSA) handling the case. Promises should never be made that can't be kept and remember the key is communication between Adjudications Officer, USCIS Counsel, and Vetting Officer, if applicable.

c. Coordination with Counsel: Communication, Communication, Communication
When learning that an application or petition is subject to a court action, the Adjudications Officer must notify local USCIS Counsel as soon as possible. USCIS Counsel is the link between the Adjudications Officer and the AUSA and must be kept aware of the development of the litigation as well as the status of the application/petition. The Adjudications Officer must also notify his or her supervisor that the case is subject to litigation so that the supervisor can prioritize the case and allot time for it to be worked. The Adjudications Officer should discuss the status of the case with the USCIS attorney and offer to be a part of any exchanges with the AUSA where eligibility is discussed. The Adjudications Officer may indicate the existence of classified information, but **may not** discuss the substance of that information except when certain that all parties to that discussion have the appropriate clearance **AND** need to know.

When determining "need to know", it is important to remember that if a denial is contemplated based on unclassified information, the classified will not usually need to be discussed and may not even need to be mentioned.

The Adjudications Officer should maintain custody of the A-file, T-file, or receipt files, but may make a copy for USCIS Counsel. The Adjudications Officer is the key to defending against mandamus actions as well as any other court activity. While USCIS Counsel works with the AUSA to address court inquiries, the Adjudications Officer holds the application which is the root of the court's interest. In some cases, court hearings may be held to determine an applicant's eligibility for a benefit. The Adjudications Officer, better than anyone, understands eligibility standards that are applied to immigration benefits applications and must be ready to articulate those standards to USCIS Counsel, the AUSA, and possibly the court. As such, the Adjudications Officer will be instrumental in developing courtroom lines of questioning in matters where a judge will determine eligibility.

The Adjudications Officer must be mindful of court deadlines for answers, hearings, and other activities and must coordinate with USCIS Counsel in a manner that will allow USCIS to meet those deadlines. The Adjudications Officer should become familiar with basic court procedures in their respective areas so that they can anticipate court orders and actions and respond appropriately. The Adjudications Officer should also become familiar with local precedent on matters that affect immigration benefit applications. For instance, in some Federal Circuits, concurrent jurisdiction is observed – effectively giving USCIS the opportunity to interview and request evidence from an applicant while the case is subject to court action. In other Circuits, courts hold that they have exclusive jurisdiction and that USCIS cannot take any action without the permission of the court, either through a remand or specific instructions.

The Local USCIS Counsel will coordinate appropriate information-sharing activities with the AUSA and will identify appropriate parties to the discussion. *Since the AUSA is employed by the Department of Justice, the Third Agency rule prohibits the disclosure to the AUSA of any law enforcement sensitive information in the possession of USCIS which originated with another agency, unless that source agency has consented to such a disclosure to the AUSA.*[17]

In addition to restrictions imposed by the third agency rule, where information is classified, additional legal restrictions exist on any dissemination of such information. Violation of those restrictions can bring administrative or criminal penalties.[18]

---

[17] *See* Department of Homeland Security, Management Directive System, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information,* MD 11042.1, Part6 H.8, (January 1, 2005). The term used with DHS for law enforcement sensitive information and similar information is "For Official Use Only" information.

[18] *See* 18 U.S.C § 798 (Disclosure of Classified Information); 50 U.S.C. § 783(b) (Communication of classified information by Government officer or employee); Executive Order 12958, 60 Fed. Reg. 7977 (February 26, 1966),

Whether working a 336(b) case or a mandamus case, the Adjudications Officer will likely find that he or she is working with counsel more frequently than normal. ICE and USCIS attorneys are familiar with court procedures in their areas, and are used to working with the AUSAs who are assigned to immigration work. AUSAs are familiar with court procedures and the preferences of individual judges. Whenever the Adjudications Officer contemplates taking an action (scheduling an interview, issuing a Request for Evidence, issuing a decision, etc.), USCIS Counsel should notify the AUSA of the intended action. USCIS Counsel or the AUSA may offer advice regarding decisions, to include review of the decision to determine legal sufficiency and/or risk of bad case law. However, **the decision is ultimately USCIS's**.

d. Vetting Officer's Role in Litigation Cases

The guidance followed by Adjudications Officers for cases in federal litigation should also be applied to cases that are in the vetting stage and in federal litigation. In short, the Vetting Officer must work closely with USCIS Counsel and the USCIS Adjudications Branch to ensure that both parties are aware of litigation filings, deadlines, regularly receive status updates, and are notified of any issues or concerns as they arise. USCIS Counsel represents the Vetting Officer and USCIS Counsel act as the liaison with the AUSA for the Vetting Officer.

4. Inadmissibility - 212(a)(6)(C)(i) vs. Good Moral Character (GMC)

National security cases are often denied because of inadmissibility grounds, specifically misrepresentation or fraud, or due to lack of Good Moral Character (GMC). Whether the underlying factors are travel, residence, employment, taxes, criminal issues, entry into the U.S., marriage fraud, responses claimed on forms, information gathered through public sources or through different systems, this information will help an Adjudications Officer determine whether there has been misrepresentation committed by the applicant and if that relates to a finding of a lack of GMC for N-400 applicants or inadmissibility grounds for other applications.

a. 212(a)(6)(C)(i) of the INA

Misrepresentation at time of admission into the U.S. is covered under Section 212(a)(6)(C)(i) of the INA. Anyone who either by fraud or willfully misrepresenting a material fact seeks to procure a visa, documentation, or admission into the U.S. or for any other immigration benefit is inadmissible. It does not need to be under oath and it does not matter if given orally or in writing. Examples: Submitting a fraudulent birth certificate to establish a mother/daughter relationship for Form I-130, Petition for Alien Relative; using a fraudulent passport at time of entry; submitting fraudulent employment history to obtain an employment visa; falsely claiming

---

as amended by Executive Order 13292, 68 Fed. Reg. 15315, 15324-15325 (March 25, 2003), Sec. 4.1 (c), (e) (covering classified information); 32 CFR § 2001.61(b) (4) (vi) (A), (B) (covering classified information)

immigration status to a CBP officer. Remember a material fact is a fact or information that is necessary for the alien to be eligible for the benefit and consider the alien may be eligible to apply for a waiver of this inadmissibility under 212(i).

b. Good Moral Character

Good moral character (GMC) for naturalization is covered under Sections 101(f) and 336(d) of the INA and 8 CFR 316.10(b)(2)(vi). False testimony under oath for the purpose of obtaining an immigration benefit constitutes a bar to a finding of GMC if the testimony was given in the period the applicant must show GMC. This would be true even if the testimony is not material. However, to qualify as false testimony, it must be under oath and given orally. It can be at an interview other than the naturalization, such as an I-130 interview. At the time of naturalization, an Adjudications Officer should review all prior petitions or applications to determine if the applicant was truthful at the time they obtained the benefit. Case law supports the idea that misrepresentation need not be material at the time of the N-400 interview but in order to support a finding of poor moral character the misrepresented fact must be linked to some area of eligibility. Example: USCIS knows the applicant has a criminal record but during interview the applicant claims no record. For false testimony, not only does the applicant need to admit to the criminal record but they need to admit why they kept the information from the interviewing officer. Other false statements, such as on an application, can lead to a conclusion that a person lacks GMC, but the automatic bar only apply to false testimony.

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

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

5. Communication between the Vetting Officer and the Adjudications Officer

Communication between the Vetting Officer and the Adjudications Officer is of utmost importance when adjudicating national security cases.

The Vetting Officer is primarily responsible for internal vetting, deconfliction, and external vetting with the record owner. The Vetting Officer should consider discussing the case with the Adjudications Officer prior to deconfliction or external vetting in order to develop a thorough line of questioning and/or to have a clear understanding of any adjudication concerns. The Vetting Officer should also consider the benefits of including the Adjudications Officer in any meetings or conversations with the record owner.

National security cases may require additional special handling due to litigation, congressional interest, or management inquiries at any stage of the process. The Vetting Officer may desire to request a supplemental eligibility review of the case by an Adjudications Officer based on new information or may have questions relating to the adjudication of the application or petition. And vice versa, the Adjudications Officer may have questions about law enforcement terminology or systems checks results for the Vetting Officer. A good line of communication and an open door will assist both offers in completing the task at hand.

H. EPO #8: Specify the DHS guidelines concerning the use of classified information in a written decision.

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

The DHS policy for disclosing classified evidence requires multiple steps which include:

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

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

USCIS Officers should keep in mind that classified information may be used as a "pointer" for both vetting and adjudications purposes such as to search a specific open source site, or develop Requests for Evidence (RFE) and lines of inquiry; keeping in mind USCIS should deconflict with the appropriate agencies prior to dissemination of RFEs and interview questions and ensure that no tracks indicate that classified information was used as a "pointer". Do NOT compromise ongoing investigations by divulging availability or knowledge of classified information.

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

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

HQ – Adraine Gilmore at (202) 272-0935
Field – Karen McGuire at (802) 872-4137 or Danielle Esposito at (802) 872-4134

IV. APPLICATION

A. In-Class Exercises

- **Find that FTO!**
- **22 Scenarios for Applying Referral Criteria**

V. REFERENCES

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

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

VI. POLICY MEMORANDA

A. National Security

1. USCIS Policy Memorandum, *"Policy for Vetting and Adjudicating Cases with National Security Concerns"*, dated April 11, 2008.
2. USCIS Operational Memorandum, *"Processing of Applications for Ancillary Benefits Involving Aliens Who May Pose National Security or Egregious Public Safety Concerns,"* dated May 11, 2007.
3. USCIS Operational Memorandum, *"Processing of Forms I-90s Filed by Aliens Who May Post National Security or Egregious Public safety Concerns,"* dated May 11, 2007.
4. USCIS Operational Memorandum, *"National Security Reporting Requirements,"* dated February 16, 2007. (FOUO)
5. USCIS Operational Memorandum, *"National Security Record Requirements,"* dated May 9, 2006.
6. USCIS Operational Memorandum *"Permanent Resident Documentation for EOIR and 1-90 Cases,"* dated April 10, 2006.

B. FBI Name Check

1. USCIS Operational Memorandum, *"FBI Name Check Process and Clarification for Domestic Operations,"* dated December 21, 2006.

2. USCIS Memorandum, *"Revised National Security Adjudication and Reporting Requirements,"* dated February 4, 2008.

C. Department of Homeland Security

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

2. DHS Secretary's Memorandum, *"Department of Homeland Security Guidelines for the Use of Classified Information in Immigration Proceedings,"* dated October 4, 2004.

D. Asylum-related

1. *"Disclosure of Asylum-Related Information to U.S. Intelligence and Counterterrorism Agencies"* dated April 18, 2007.

2. *"Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants"* dated June 3, 2005.

3. *"Protocols for Handling Asylee Adjustment Cases That May Warrant Initiation of the Asylum Status Termination Process"* dated July 19, 2004.

4. *"Confidentiality of Asylum Applications and Overseas Verification of Documents and Application Information"* dated June 21, 2001.

VII. ADDITONAL ELECTRONIC RESOURCES

A. 2008 Customs & Border Protection Special Interest Alien Handbook

B. Fraudulent Document Laboratory (FDL) Guides

1. Middle Eastern Calendar Guide
2. North African & Middle Eastern Stamp Guide (entry & exit stamps)

C. 2008 National Counterterrorism Center Calendar

D. Al Qaeda Manual

E. A Guide to Naming Practices

F. National Security Terms of Reference Tables

G. USCIS Fact Sheet, *"Immigration Security Checks—How and Why the Process Works,"* dated April 25, 2006.

H. Statement of Mutual Understanding of Information Sharing with Dept of Citizenship and Immigration Canada

I. Websites for Basic and Supplemental Systems Checks

J. Department of Homeland Security For Official Use Only (FOUO) Coversheet

K. Sample Background Checklist

L. Sample Classified Notes Page