

EXHIBIT 28

~~FILED UNDER SEAL~~



U.S. CITIZENSHIP AND IMMIGRATION SERVICES
HANDBOOK

**National Background Identity and Security Checks
Operating Procedures**

Handbook Number: USCIS HB-FDNS-602-001

Issue Date: December 17, 2010

MRD: December 17, 2012

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

This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. § 552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to Sensitive But Unclassified (SBU) information, and is not to be released to the public or other personnel who do not have a valid "need-to-know" basis without prior approval from the originator.

Foreword

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.

This HB describes FDNS policies and procedures for planning, implementing, and assessing the effectiveness of FDNS systems. 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 After two years, this document will be reissued without change, revised, or withdrawn from the U.S. Citizenship and Immigration Services Knowledge Management Directory.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.

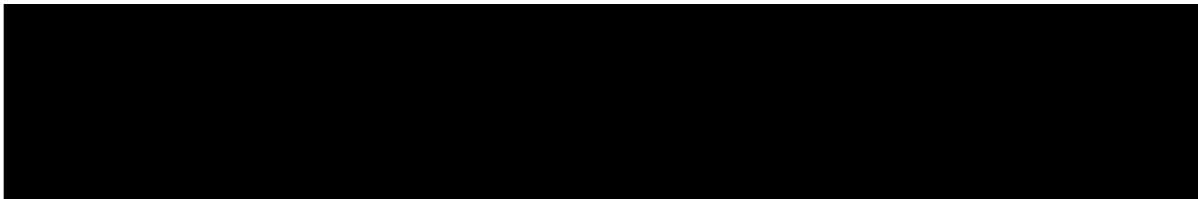
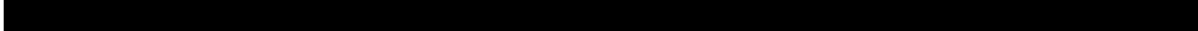
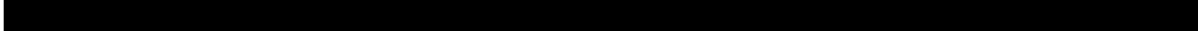
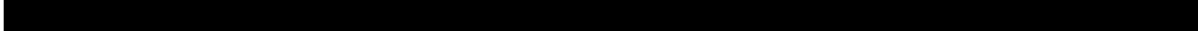

These materials must be handled and safeguarded in accordance with DHS management directives governing protection and dissemination of such information. At a minimum, these materials shall only be disseminated on a “need-to-know” basis.

Questions or comments regarding any part of this document should be directed to USCIS FDNS NSB at [REDACTED]@dhs.gov.

NOTE: Copies of this document may be obtained from FDNS directly or by downloading it from the Executive Secretariat Home Page: [http://\[REDACTED\]](http://[REDACTED])

**NaBISCOP
USCIS FDNS-HB 602-001**

Table of Contents

Figures	vi
Tables	vi
Table of Revisions	1
I. Introduction	5
A. Scope and Use	6
B. Authority	7
C. Background	7
D. Implementation	7
E. Contact Information	7
II. Employee Safety	8
III. Protecting Sensitive Information from Unauthorized Disclosure	9
A. For Official Use Only (FOUO)	9
B. DHS: One Agency for Information Sharing Purposes	10
C. Third Agency Rule	11
D. Safeguarding Classified Information	11
E. Personally Identifiable Information (PII)	13
F. Privacy Act	15
G. Confidentiality	16
1. Asylum and Refugee	17
2. Violence Against Women Act/T and U Nonimmigrant Visas	17
3. Legalization/Seasonal Agricultural Worker (SAW)	18
4. Temporary Protected Status (TPS)	18
IV. Background Check Process	19
A. Who Requests and Reviews Background Checks	20
B. Overview of Background Check Process	21
	22
	24
	25
	25
	25
C. Overseas Processing	25
D. Refugee Processing	26
E. Service Center Processing	27
V. Security Check: TECS	29

NaBISCOP
USCIS FDNS-HB 602-001

A. TECS 30

 1. About TECS 30

 2. About NCIC 30

B. Who Requires TECS Queries 31

C. TECS – Batch Query Procedures 35

D. TECS – SQ11 Query Procedures 37

 1. SQ11 Search Criteria 39

 2. Name and DOB Rules 41

E. TECS – SQ16 Query Procedures 50

 SQ16 Search Criteria 51

F. TECS – SQ94 Query Procedures 52

 1. SQ94 Nonimmigrant Information System Queries 52

 2. INQUIRY (I-94) Report 53

 3. Archive Data Query 55

G. [REDACTED] 55

 [REDACTED] 55

 [REDACTED] 55

H. [REDACTED] 58

I. [REDACTED] 59

 [REDACTED] 59

 [REDACTED] 59

 [REDACTED] 61

 [REDACTED] 64

J. [REDACTED] 68

 [REDACTED] 68

 [REDACTED] 68

 [REDACTED] 69

 [REDACTED] 70

 [REDACTED] 71

 [REDACTED] 71

 [REDACTED] 72

 [REDACTED] 74

 [REDACTED] 74

 [REDACTED] 75

 [REDACTED] 79

 [REDACTED] 82

 [REDACTED] 82

K. [REDACTED] 83

 [REDACTED] 83

NaBISCOP
USCIS FDNS-HB 602-001

	...	84
	...	84
L.	...	84
M.	...	85
	...	85
	...	86
	...	87
	...	87
	...	88
	...	88
	...	89
N.	...	89
O.	...	89

VI. Security Check: FBI Name Check	92
A. FBI Name Check.....	92
B. Who Requires FBI Name Checks	93
C. FBI Name Check Procedures.....	94

D.	...	97
	...	100
	...	101
	...	101
	...	103
E.	...	105
F.	...	106
G.	...	106
H.	...	106

VII. Security Check: FBI Fingerprint Check	108
A. FBI Fingerprint Check.....	108
B. Who Requires FBI Fingerprint Checks	109

	...	111
	...	112
C.	...	112
D.	...	114
E.	...	115
F.	...	116
G.	...	117
H.	...	117
	...	117

NaBISCOP
USCIS FDNS-HB 602-001

I.	[REDACTED]	118
VIII.	Security Check: US-VISIT/IDENT	121
A.	About US-VISIT/IDENT	121
	[REDACTED]	121
	[REDACTED]	122
	[REDACTED]	122
B.	[REDACTED]	126
C.	[REDACTED]	127
	[REDACTED]	127
D.	[REDACTED]	127
E.	[REDACTED]	127
F.	[REDACTED]	127
IX.	Resolution: National Security Concerns (CARRP)	128
A.	CARRP Policy and Operational Guidance	128
B.	Definition of NS Concern	129
1.	Known or Suspected Terrorist (KST)	130
2.	Non-KST NS Concern	130
3.	Non National Security (NNS)	131
C.	Four Step Approach to Cases with National Security Concerns	131
D.	Employment and Travel Authorization Applications with NS concerns	132
E.	Form I-90 with NS Concerns	133
F.	Santillan (EOIR Grants) with NS Concerns	133
G.	Request for Assistance to HQFDNS National Security Branch (NSB)	134
X.	Resolution: Egregious Public Safety Concerns & Other Criminal Cases	136
A.	Egregious Public Safety (EPS) Policy and Guidance	136
B.	EPS Case Definition	136
C.	Adam Walsh Act	137
D.	International Marriage Broker Regulation Act	138
E.	Referral to ICE (RTI) for EPS Case	138
F.	Referral to ICE for Other Criminal Cases	139
G.	Exceptions to EPS RTI Criteria	140
H.	Employment and Travel Authorization Applications with EPS Concerns	140
I.	Form I-90 with EPS Concerns	141
J.	Santillan (EOIR Grants) with EPS Concerns	141
XI.	Resolution: Immigration Fraud	143
	Immigration Benefit Fraud Policy and Guidance	143

NaBISCOP
USCIS FDNS-HB 602-001

XII. Appendices 144

 Security Check Requirements by Form Type & Quick Reference..... 145

 Description of Form Numbers 149

 TECS Terms Indicating Possible NS Concerns 151

 List of Acronyms 158

 Glossary of Terms 164

 MS92 173

 List of References 179

 Notice to INTERPOL..... 185

 Quick Reference 187

Figures

Figure 1: [REDACTED] . 19

Figure 2: [REDACTED] . 22

Figure 3: [REDACTED] . 23

Figure 4: [REDACTED] . 39

Figure 5: [REDACTED] . 51

Figure 6: [REDACTED] . 62

Figure 7: [REDACTED] . 64

Figure 8: [REDACTED] . 66

Figure 9: [REDACTED] . 93

Figure 10: [REDACTED] . 95

Figure 11: [REDACTED] . 97

Figure 12: [REDACTED] 102

Figure 13: [REDACTED] 109

Figure 14: [REDACTED] 113

Figure 15: [REDACTED] 114

Tables

Table 1: [REDACTED] . 12

Table 2: [REDACTED] . 12

Table 3: [REDACTED] . 21

Table 4: [REDACTED] . 23

Table 5: [REDACTED] . 32

Table 6: [REDACTED] . 36

Table 7: [REDACTED] . 36

Table 8: [REDACTED] . 38

**NaBISCOP
USCIS FDNS-HB 602-001**

Table 9:	...	42
Table 10:	...	43
Table 11:	...	43
Table 12:	...	44
Table 13:	...	44
Table 14:	...	44
Table 15:	...	45
Table 16:	...	45
Table 17:	...	45
Table 18:	...	45
Table 19:	...	46
Table 20:	...	46
Table 21:	...	47
Table 22:	...	47
Table 23:	...	47
Table 24:	...	48
Table 25:	...	48
Table 26:	...	49
Table 27:	...	50
Table 28:	...	53
Table 29:	...	56
Table 30:	...	56
Table 31:	...	63
Table 32:	...	93
Table 33:	...	96
Table 34:	...	98
Table 35:	...	102
Table 36:	...	109
Table 37:	...	114
Table 38:	...	123

NaBISCOP
USCIS FDNS-HB 602-001

Table of Revisions

Title	Description	Change Made	Affected Page	Date Effective
Name and DOB Rules	The issue relates to the NaBISCOP's name query requirement of querying additional name variations when it relates to last names with hyphens: i) Name and DOB Rules: Names with Hyphens Table 18: Examples of SQ-11 Name Queries (Names with Hyphens)	Updated tables 11, 12 and 18 to show the proper TECS Manual Query based on TECS guidance and policy along with adding a note that users can use the F2 button within TECS to pull up the TECS manual.	<u>V. D. 2 : Name and DOB Rules</u>	12/13/2011
Safeguarding Classified Information Update	Updates the page covering classified information, to incorporate a recent Executive Order on classified material, and OSI guidance on leaked classified documents (e.g., Wikileaks).	Removed language related to the Third Agency Rule, as the Executive Order modifies this requirement for classified information. Provided updated links to OSI guidance for officers to get more information on handling requirements. Provided language from OSI regarding the handling of classified information when it is submitted as evidence by an applicant, petitioner, or witness.	<u>III.D. Safeguard Classified Information</u>	10/5/11

**NaBISCOP
USCIS FDNS-HB 602-001**

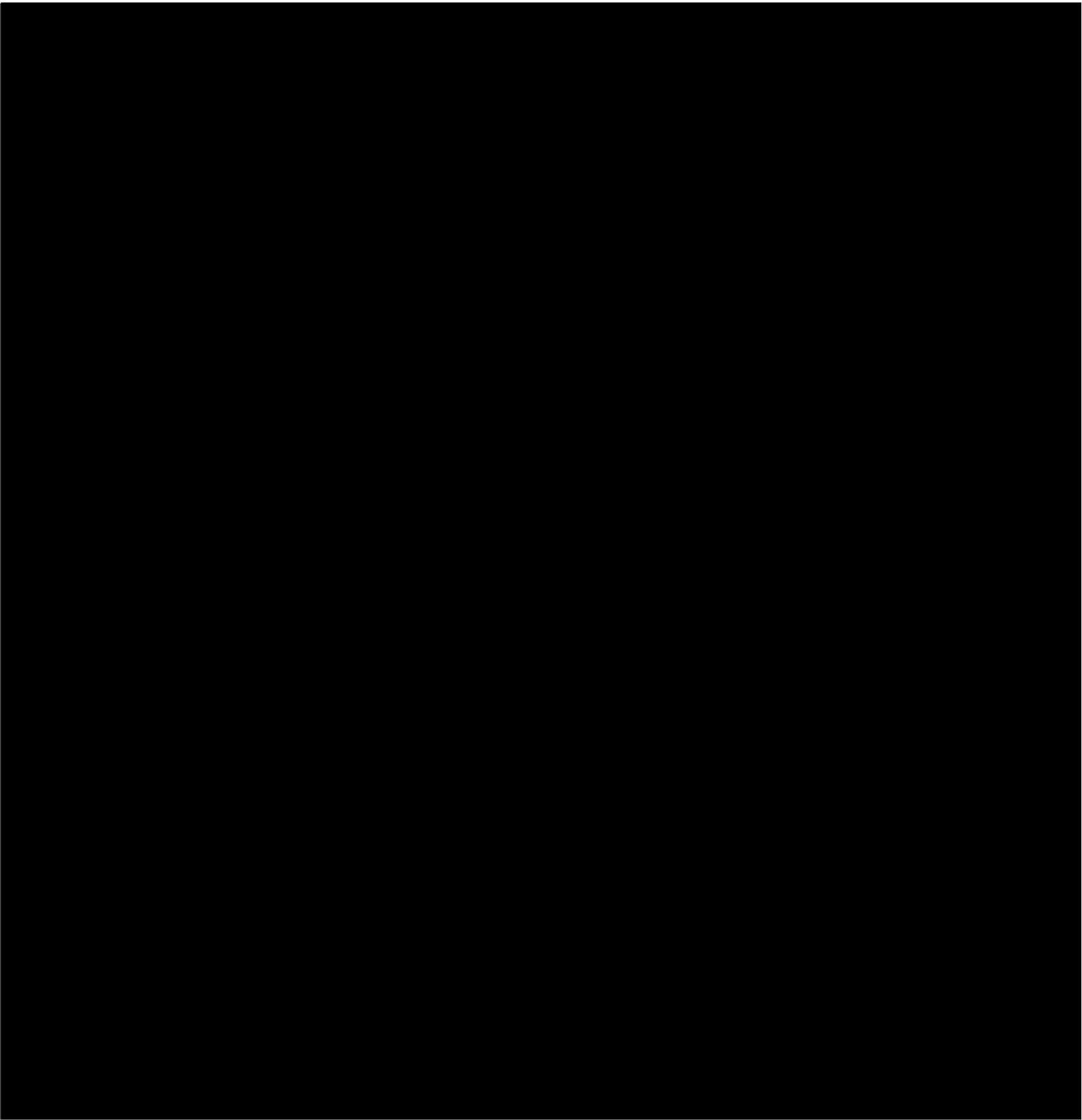
Title	Description	Change Made	Affected Page	Date Effective

NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

File	Description	Change Made	Affected Page	Date Effective
Reviewing Digitized A-Files	Clarify the requirement to review an electronic A-file in certain circumstances.	Added line: "Note: Review of the digitized filing is not required for adjudication of Temporary Protective Status re-registration."	V. B. Who Requires TECS Queries	1/19/2011
Leap Year Birthdates	Clarified the requirements for querying birthdates when the birthdate falls on a leap day.	Added "and" between the two bullets.	V. D. 2. Name and DOB Rules, Table 26, example 5.	1/18/2011
Special Interest Countries	Deleted references to Special Interest Countries, as there is no single list of	Deleted "Requires record owner contact if subject is from a Special Interest Country." Added "See	Appendix C: TECS Terms Indicating Possible NS Concerns	1/18/2011

NaBISCOP
USCIS FDNS-HB 602-001



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

Title	Description	Change Made	Affected Page	Date Effective

NaBISCOP
USCIS FDNS-HB 602-001

I. Introduction

The National Background Identity and Security Checks Operating Procedures (NaBISCOP) Handbook (HB) establishes standards for United States Citizenship and Immigration Services (USCIS) personnel specific to conducting security and background checks during the immigration benefit process.

The background check process is a critical element in USCIS's mission to ensure the integrity of the U.S. immigration system. This 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.

This HB is the principal source of procedural guidance for the performance of background and security checks by USCIS personnel. The HB is intended for use by all USCIS personnel who perform security and background checks when processing requests for immigration benefits. USCIS personnel include USCIS employees and contractors.

USCIS personnel must have (1) a need-to-know, (2) the required training, and (3) the appropriate level of background and security clearances to conduct these checks. See section IV(A) for more details.

A. Scope and Use

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

The NaBISCOP incorporates all current USCIS policies and procedures related to USCIS background and security checks. As those policies and procedures change, the NaBISCOP HB will be updated to reflect the changes.

USCIS employees and offices are not authorized to revise, supplement, disregard or deviate from these procedures. 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.

**NaBISCOP
USCIS FDNS-HB 602-001**

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.

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: [REDACTED]

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 e-mail to the FDNS-NaBISCOP mailbox: [REDACTED]

[Return to the Table of Contents](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

II. Employee Safety

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 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:

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.

[Return to the Table of Contents](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

III. Protecting Sensitive Information from Unauthorized Disclosure

Section Contents

- A. For Official Use Only (FOUO)
- B. DHS: One Agency for Information Sharing Purposes
- C. Third Agency Rule
- D. Safeguarding Classified Information
- E. Personally Identifiable Information (PII)
- F. Privacy Act
- G. Confidentiality
 - 1. Asylum and Refugee
 - 2. Violence Against Women Act/T and U Nonimmigrant Visas
 - 3. Legalization /Seasonal Agricultural Worker (SAW)
 - 4. Temporary Protected Status (TPS)

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.

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

[Return to the Table of Contents](#)

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

**NaBISCOP
USCIS FDNS-HB 602-001**

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.

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

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.

Source: “*DHS Policy for Internal Information Exchange and Sharing*,” dated February 1, 2007

[Return to the Section Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

[Return to the Table of Contents](#)

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.

[REDACTED] 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.

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

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.

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).

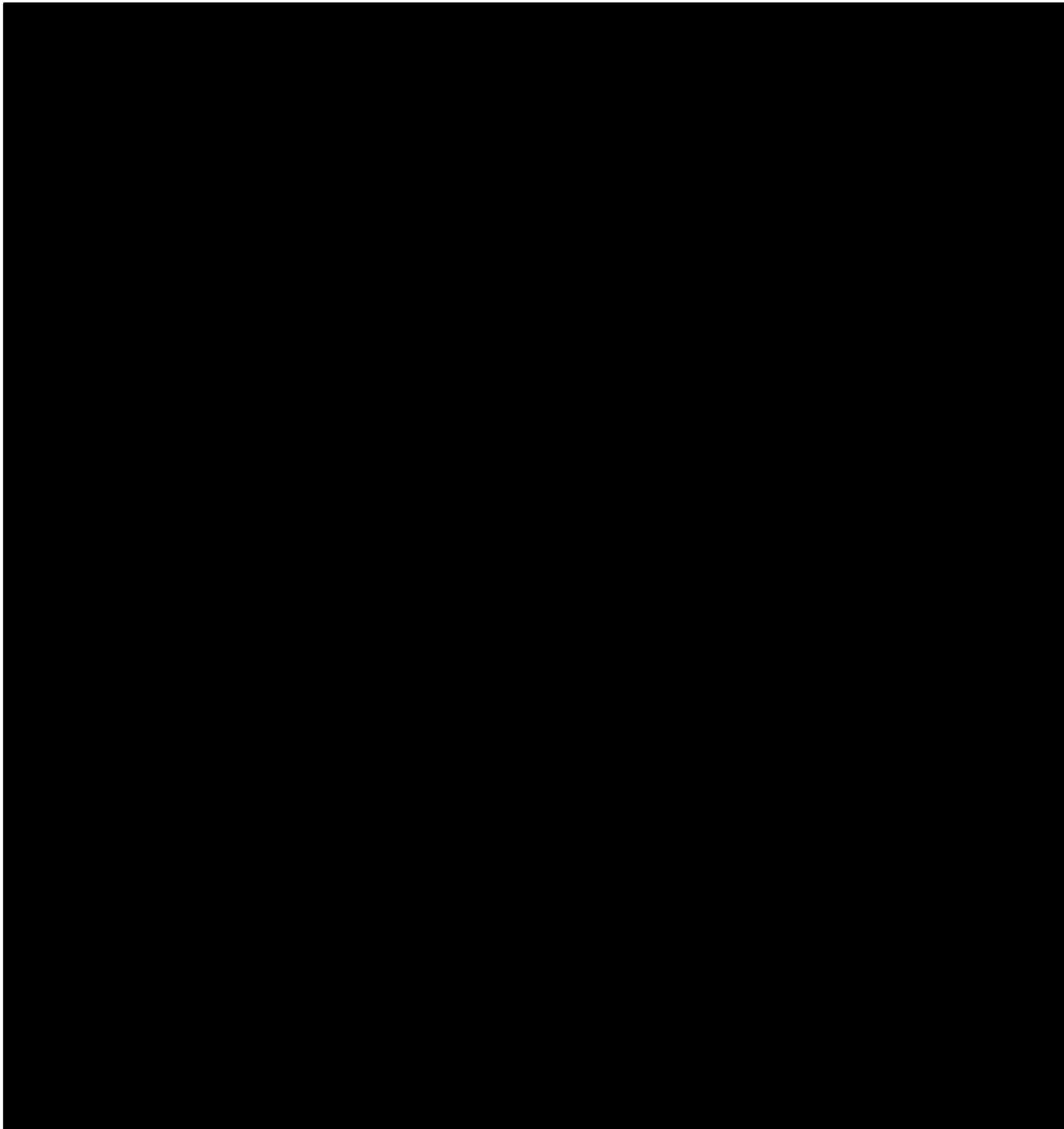
Consult OSI guidance and training material at [REDACTED] OSI's Administrative Security Division, or the local OSI field security manager (FSM) for the best way to safeguard classified information. The OSI pamphlet entitled *Safeguarding Classified and Sensitive Unclassified Information* provides specific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

[REDACTED]

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. See this pamphlet for more information:

[REDACTED]

**NaBISCOPE
USCIS FDNS-HB 602-001**

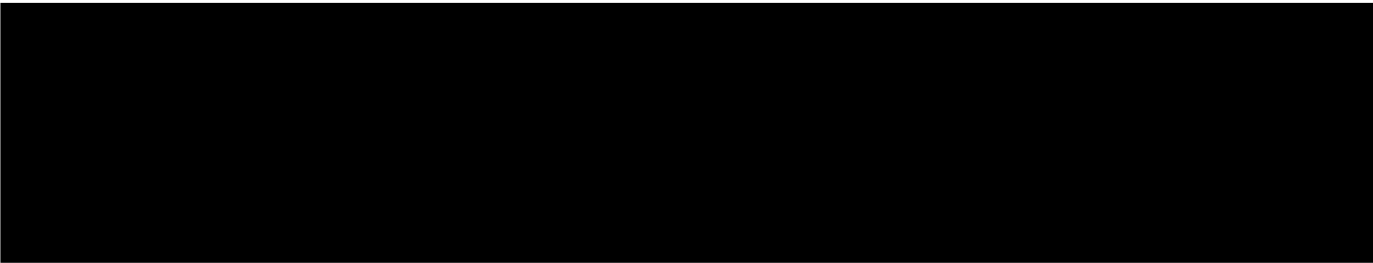


NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

Safeguarding Classified National Security Information: DON'Ts

- Do not take classified material to your home or other unauthorized area.
- Do not discuss classified information on a telephone unless using STE or STU-III equipment.
- Do not fax classified information on a non-secure fax machine.
- Do not reproduce classified information on a copy machine that has not been accredited by OSI.
- Do not store funds, weapons, medical items or items of intrinsic value in the same container used for storage of classified information.
- Do not store combinations of safes containing classified information anywhere but inside a GSA-approved security container.
- Do not dispose of classified information in regular waste baskets and recycle bins.



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

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*,”



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



**NaBISCOP
USCIS FDNS-HB 602-001**

[REDACTED] provide detailed guidance on securing PII and reporting possible improper disclosure. Proper procedures include:

- Share or discuss sensitive personal information only with those personnel who have a ***need to know*** 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. See Encrypting Files for instructions [REDACTED] 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. See DHS's guidelines on Protecting Information from Accidental Exposure for details [REDACTED]
 - **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 [REDACTED] for details on the only times you are authorized to use SSNs at USCIS.

[Return to the Section Contents](#)
[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

F. Privacy Act

The Privacy Act of 1974 (http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html) 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, 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 (CIS), the FBI Fingerprint Check, and in TECS.¹ 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*,”

[REDACTED] can be accessed on the Office of Privacy webpage [REDACTED]. Click on Documents for more information.

Some common exceptions include:

- Information may be disclosed to an employee of the owning agency if that employee needs the information to perform his/her job duty. As stated in section I(C) (DHS: One Agency for Information Sharing Purposes) of this document, all agencies within DHS are considered to be one agency, for the purpose of this law. A USCIS officer may share information with an Immigration and Customs Enforcement (ICE) officer if that ICE officer has a need to know the information.
- Information may be disclosed to the Government Accountability Office (GAO).

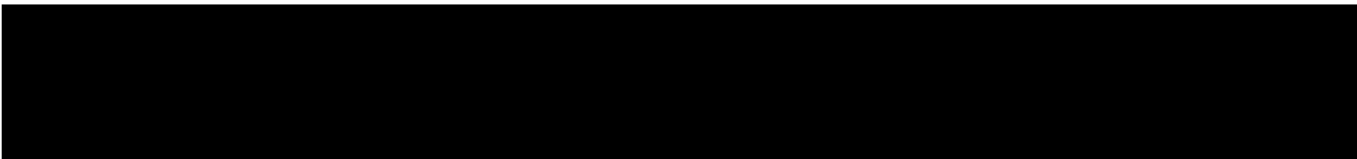
¹ Formerly, security checks by USCIS were referred to as the Interagency Border Inspection System (IBIS) checks. However, IBIS is no longer a separate database and all information formerly in IBIS is now accessed through TECS, formerly the acronym for the Treasury Enforcement Communications System. References to IBIS or TECS/IBIS are now obsolete, and any such references in older documents should be interpreted as now referring to TECS.

NaBISCOPE
USCIS FDNS-HB 602-001

- Information may be disclosed if a “routine use” exists. The Federal Register lists a number of “routine uses” for information contained in A-files and elsewhere in CIS. USCIS can share information with the Department of State (DOS) for processing an application/petition for immigration/nationality benefits.
- USCIS can share information with any law enforcement agency:
 - In order for that agency to carry out its law enforcement responsibilities.
 - If USCIS records indicate a United State citizen (USC) or a legal permanent resident (LPR) may have violated a law that is enforced by that agency.
- USCIS has issued Systems of Record Notices (SORN) for many of its records systems. These notices contain “routine uses” which may permit the sharing of information for purposes set forth in these SORNs. When in doubt, check with the system owner, your supervisor, or with the USCIS privacy officer to determine whether USCIS may disclose information outside of DHS.

Even if disclosure of certain information is permitted by the Privacy Act, disclosure of that information may still be restricted by other disclosure or information sharing policies, regulations, and statutes, such as the Third Agency Rule.

In general, any federal agency that maintains a system of records, where a name or unique identifying number of an individual can be used to retrieve information on that individual, must provide access and redress (the ability to correct inaccurate information) to the records maintained on the individual. USCs or LPRs may request information on themselves maintained in USCIS systems of records by submitting a [FOIA/Privacy Act Request](#). This form is available at the website, <http://www.uscis.gov/g-639>.



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, DC 20229

[Return to the Section Contents](#)
[Return to the Table of Contents](#)

G. Confidentiality

NaBISCOPE
USCIS FDNS-HB 602-001

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 8 CFR 208.6, information regarding an individual's status as an asylum seeker or asylee, information contained in or pertaining to his or her application, and records pertaining to any credible 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 8 CFR 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 8 CFR 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*,"

[REDACTED] 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, 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) nonimmigrants.

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. 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

NaBISCOP
USCIS FDNS-HB 602-001

providing benefits, to be used solely in making determinations of eligibility for benefits pursuant to 8 U.S.C. § 1641(c). 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 U.S.C. § 1367(b).

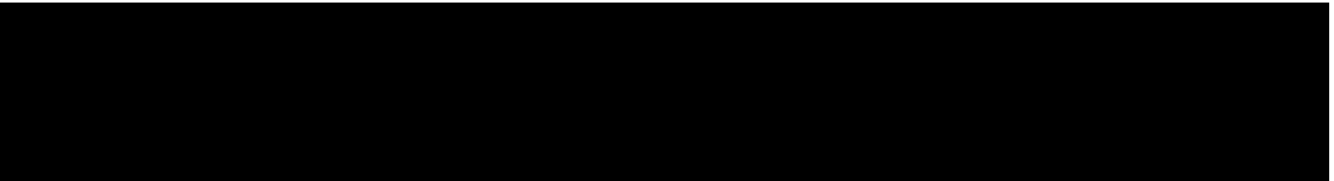
USCIS personnel seeking authorization to disclose information pursuant to an exception listed at 8 U.S.C. § 1367(b) should contact the Office of Chief Counsel.

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 CFR 245a.3(n)(4)(i) and (ii) and 8 CFR 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.



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 CFR 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 purposes of enforcement of the Act or any criminal proceeding.

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

IV. Background Check Process

Section Contents

A.

B.

C.

D.

E.

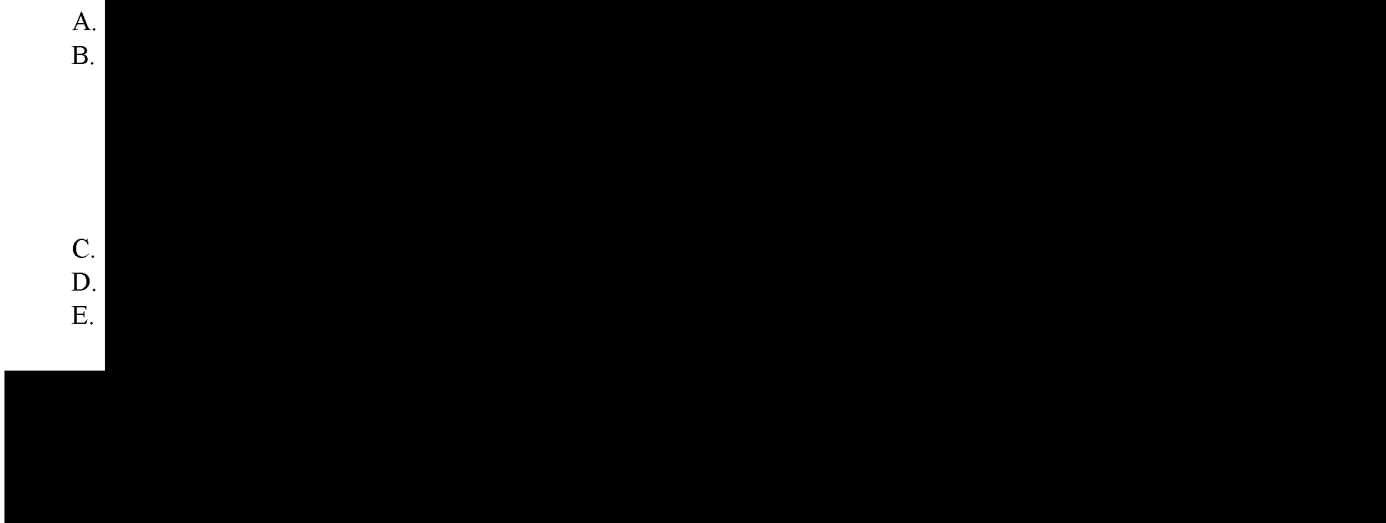
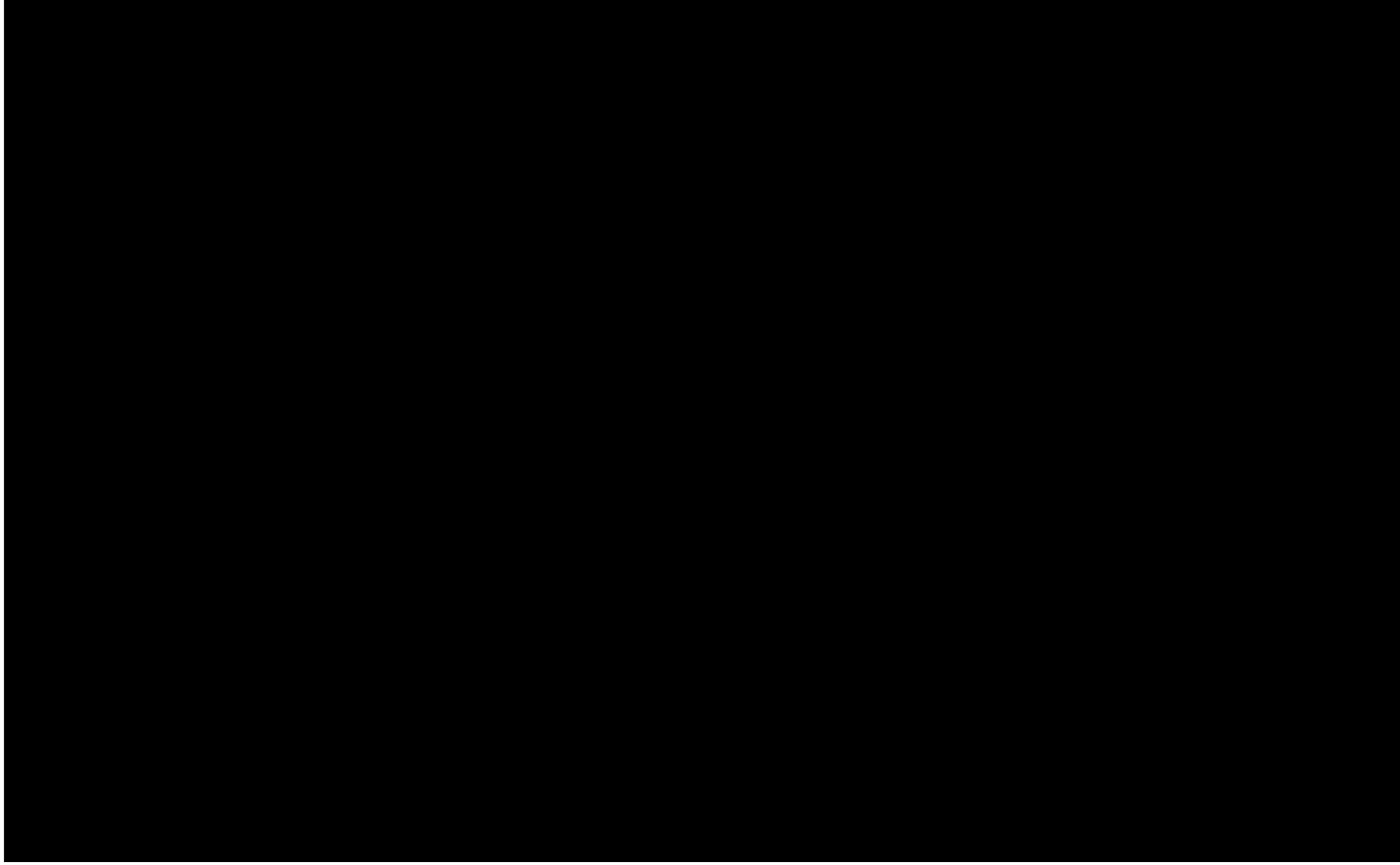
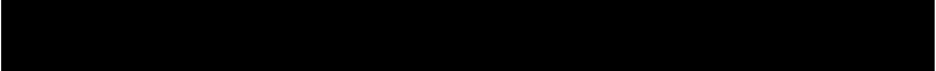
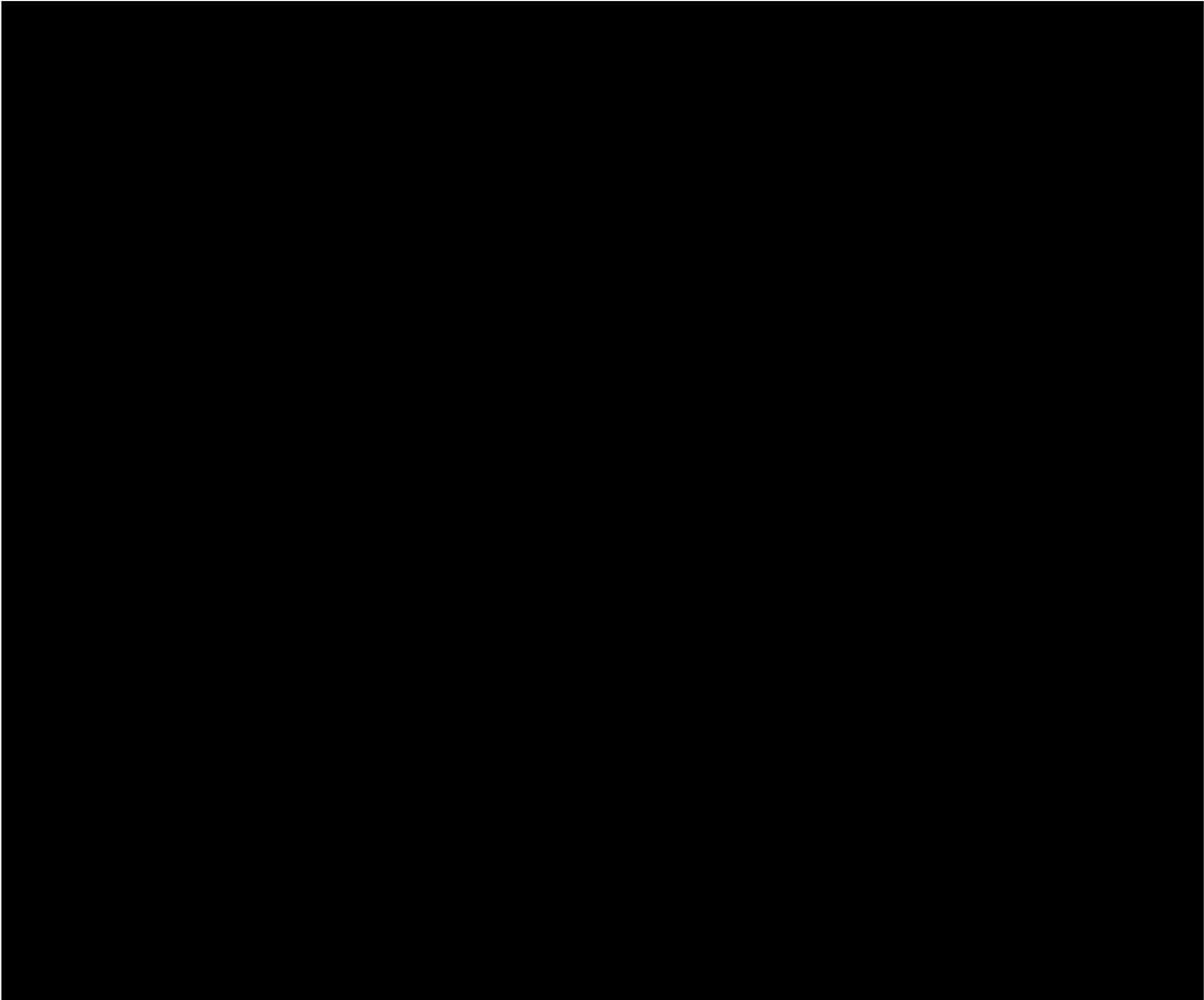


Figure 1:



**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)
[Return to the Table of Contents](#)

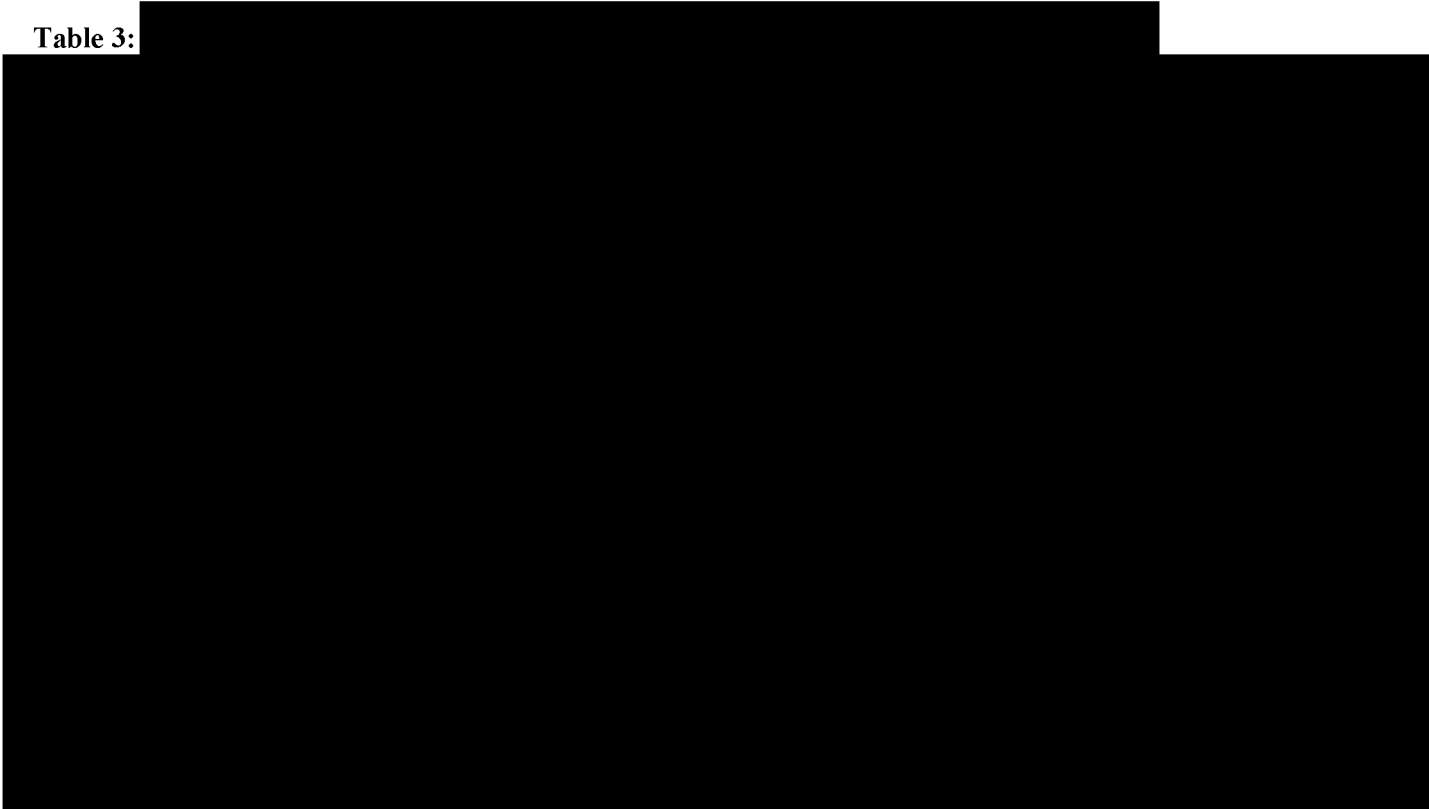
A.



NaBISCOP
USCIS FDNS-HB 602-001



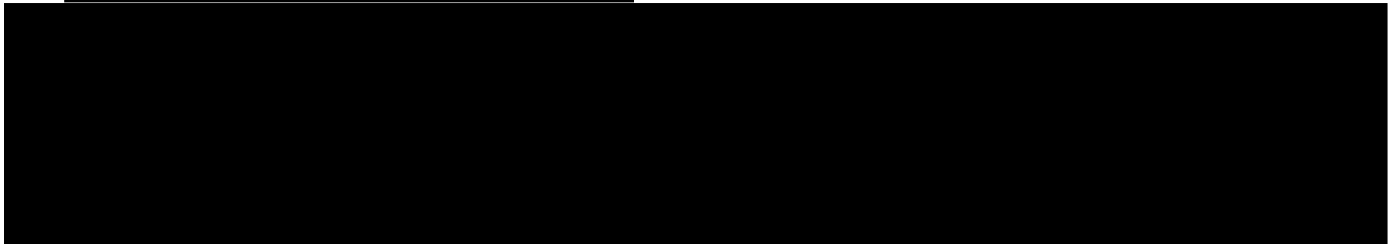
Table 3:



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

B.



**NaBISCOP
USCIS FDNS-HB 602-001**

Figure 2:



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

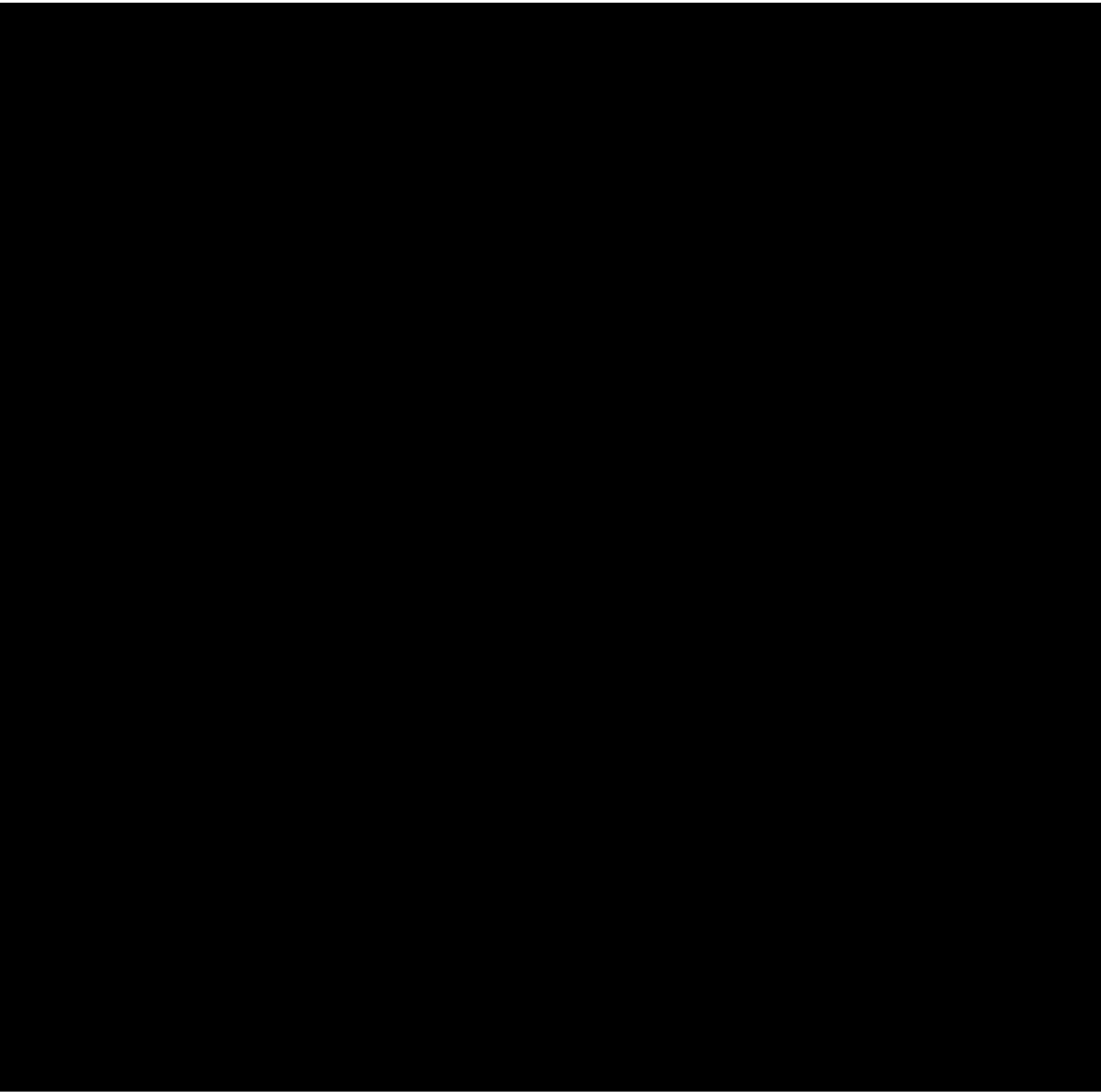
Figure 3:



Table 4:



NaBISCOP
USCIS FDNS-HB 602-001



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

C. 


[Return to the Section Contents](#)

[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

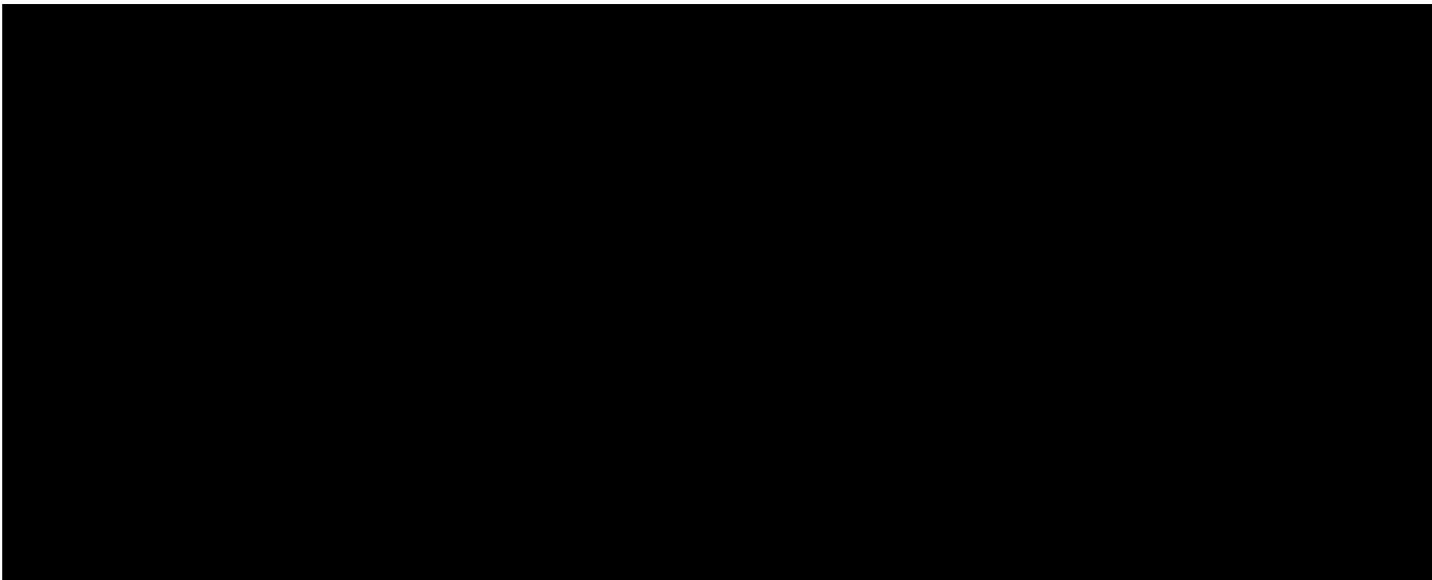
D.



NaBISCOP
USCIS FDNS-HB 602-001

26

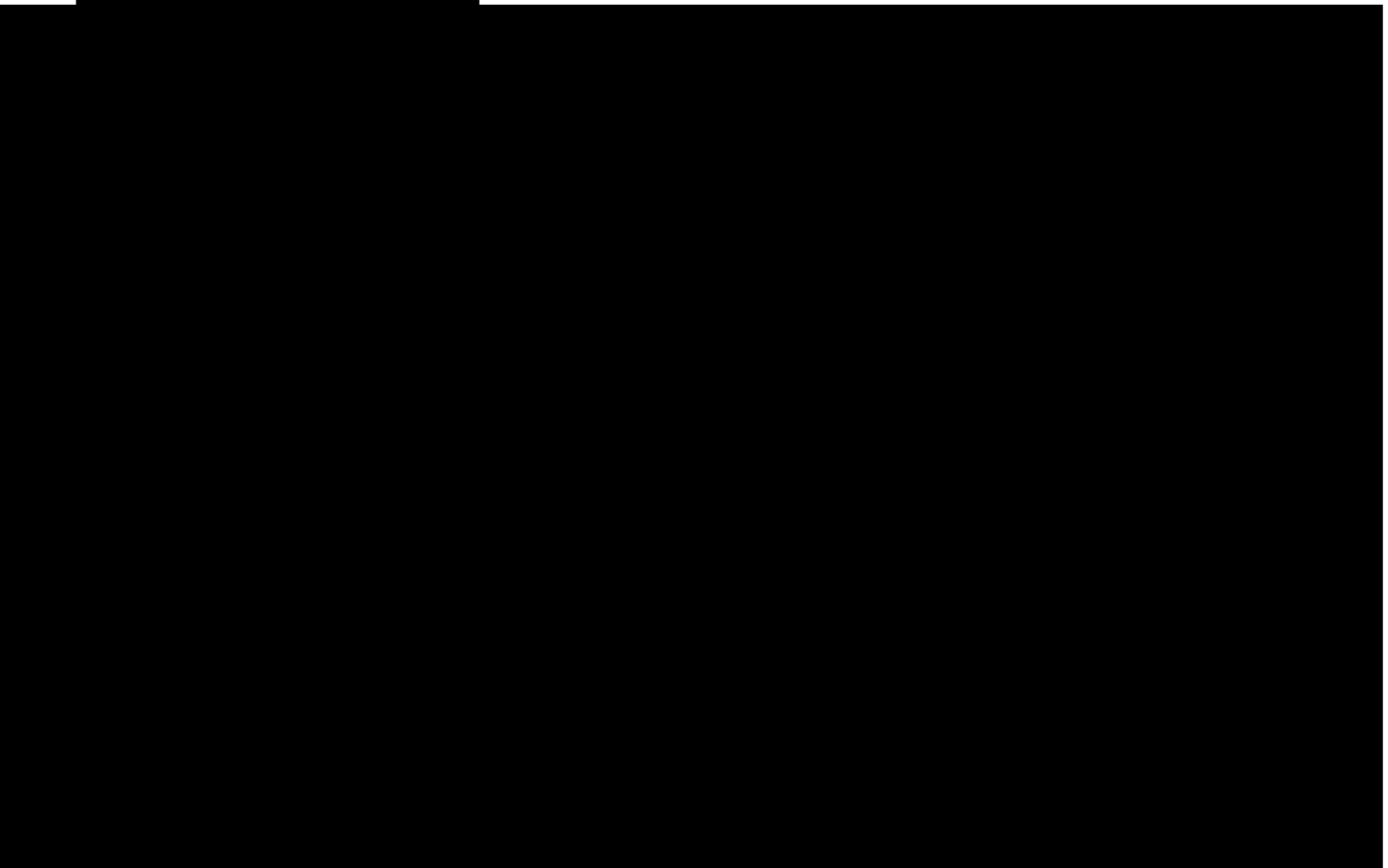
FOUO-LES



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

E.



NaBISCOP
USCIS FDNS-HB 602-001

[Return to the Section Contents](#)

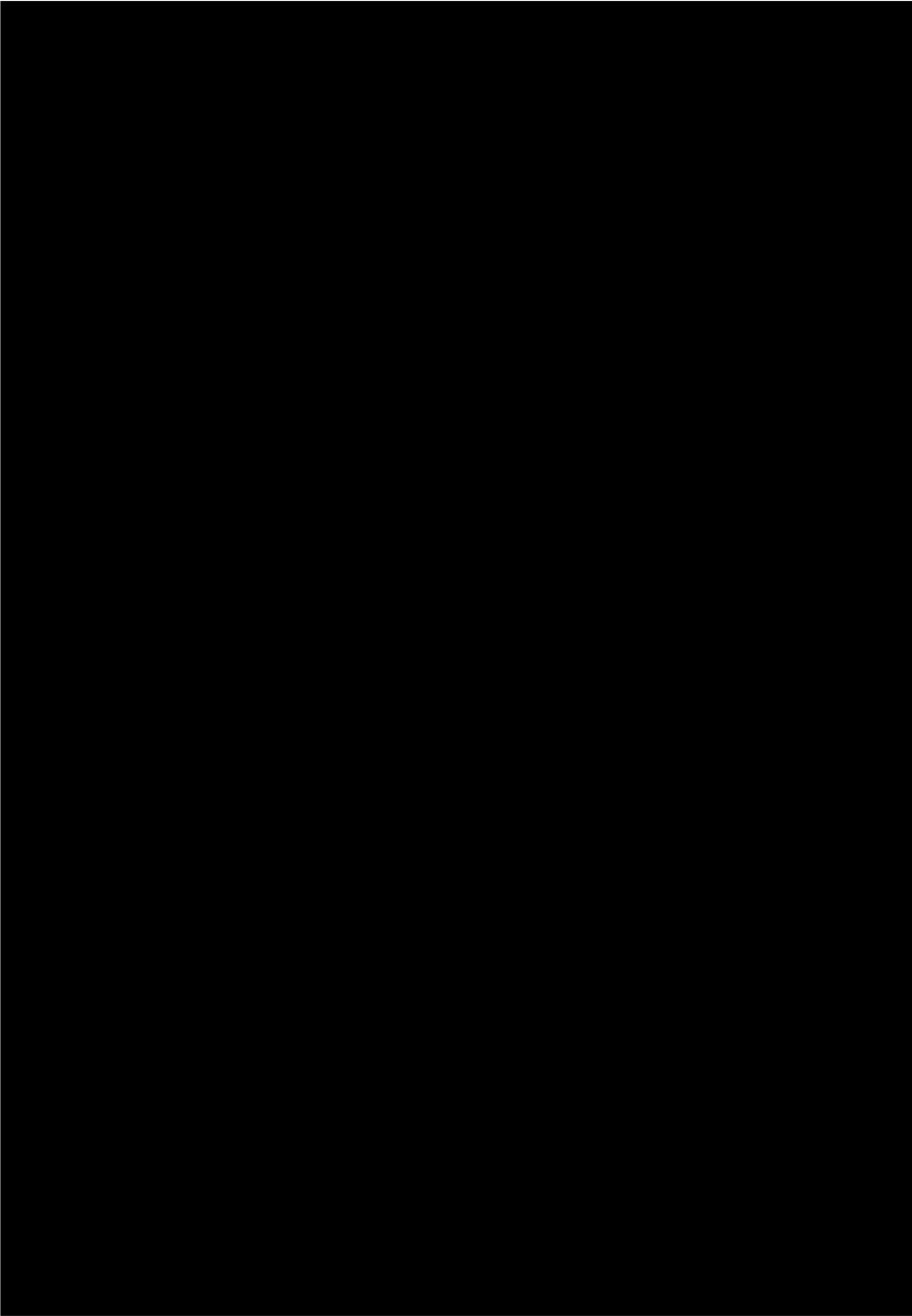
[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

V. Security Check: TECS

Section Contents

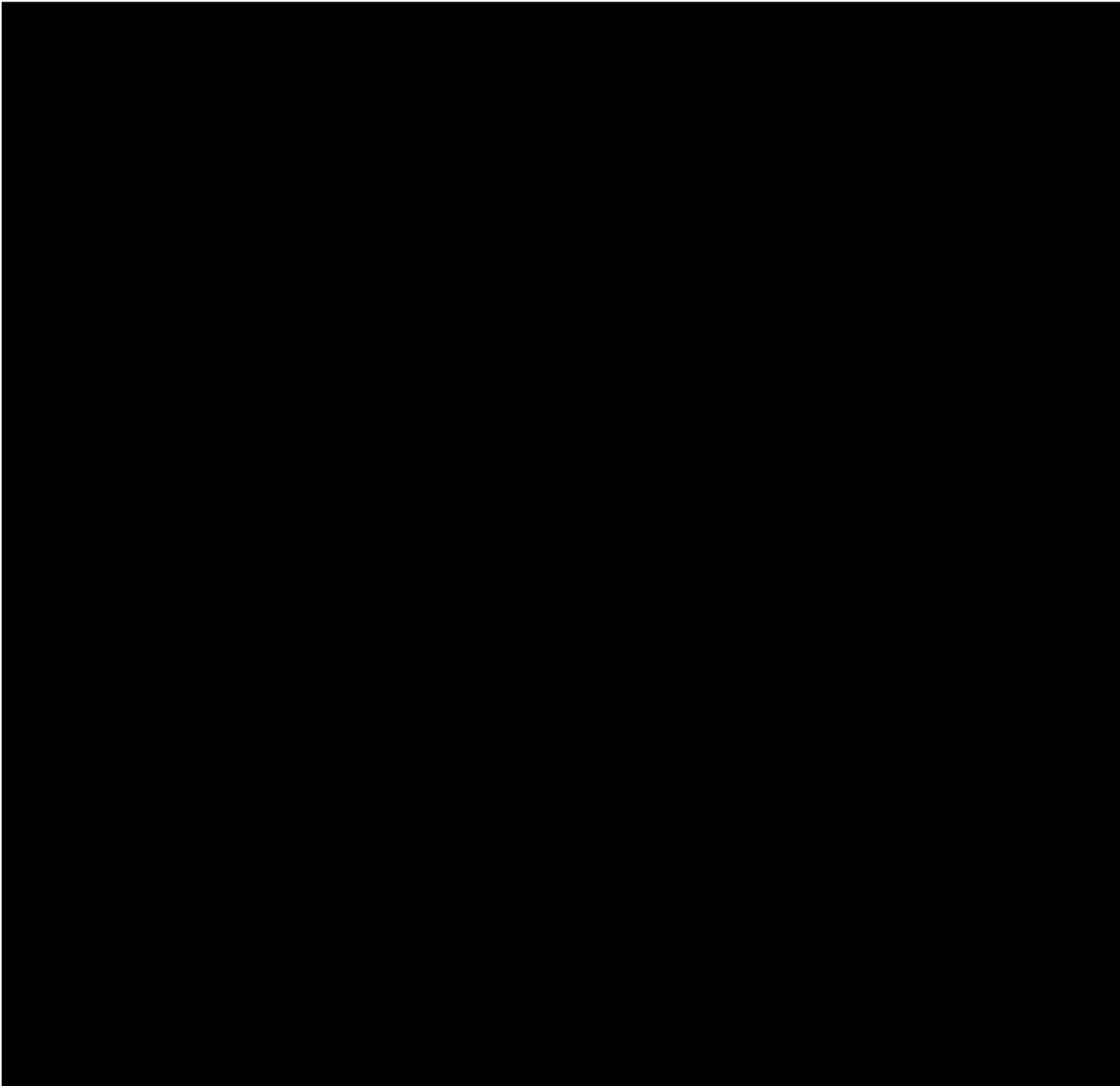
- A.
- B.
- C.
- D.
- E.
- F.
- G.
- H.
- I.
- J.
- K.
- L.
- M.



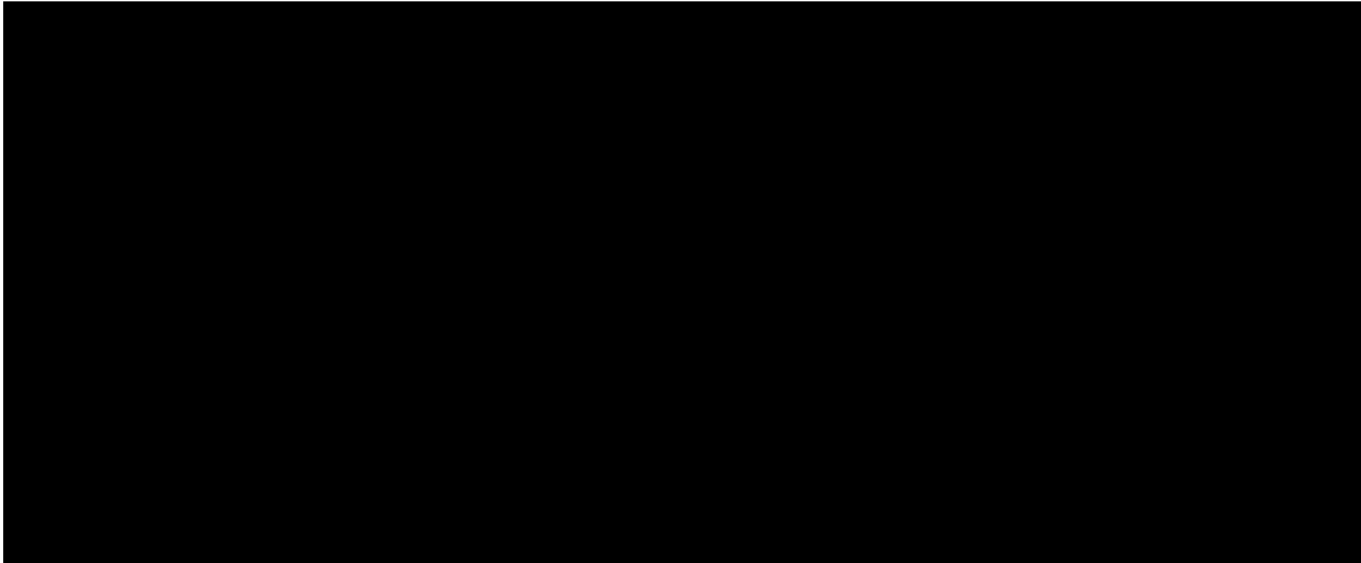
**NaBISCOP
USCIS FDNS-HB 602-001**



A.



**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

B.



**NaBISCOP
USCIS FDNS-HB 602-001**

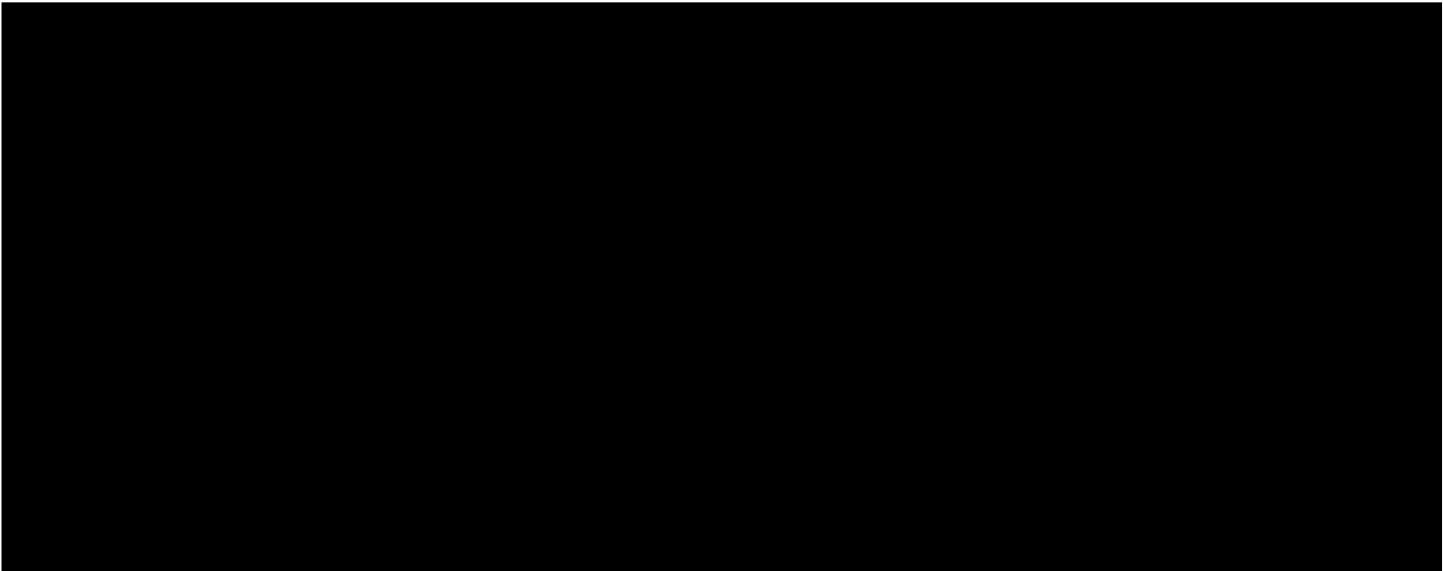


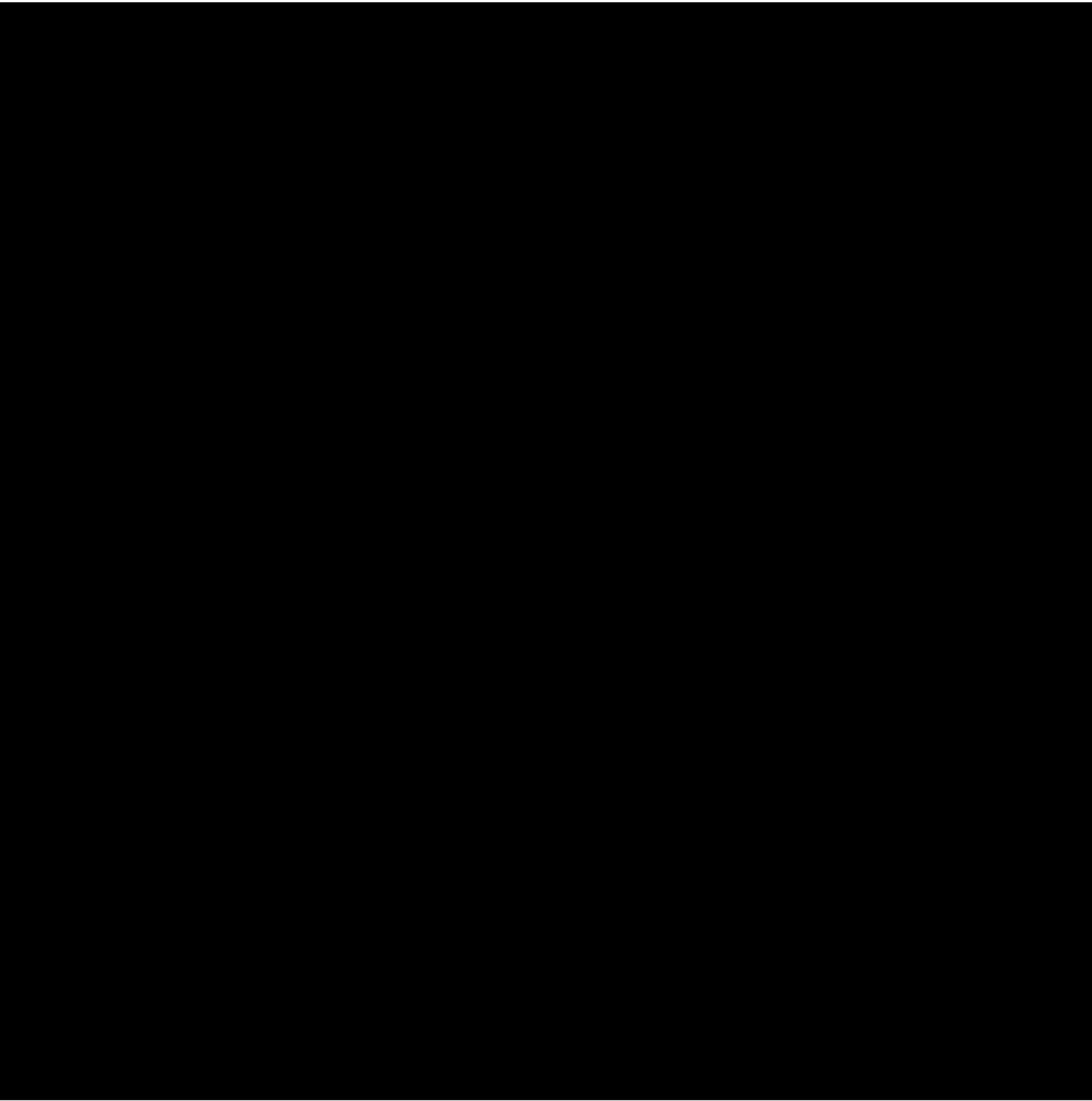
Table 5: [Redacted]

NaBISCOP
USCIS FDNS-HB 602-001

NaBISCOP
USCIS FDNS-HB 602-001

33

FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

C. 

NaBISCOP
USCIS FDNS-HB 602-001

Table 6:

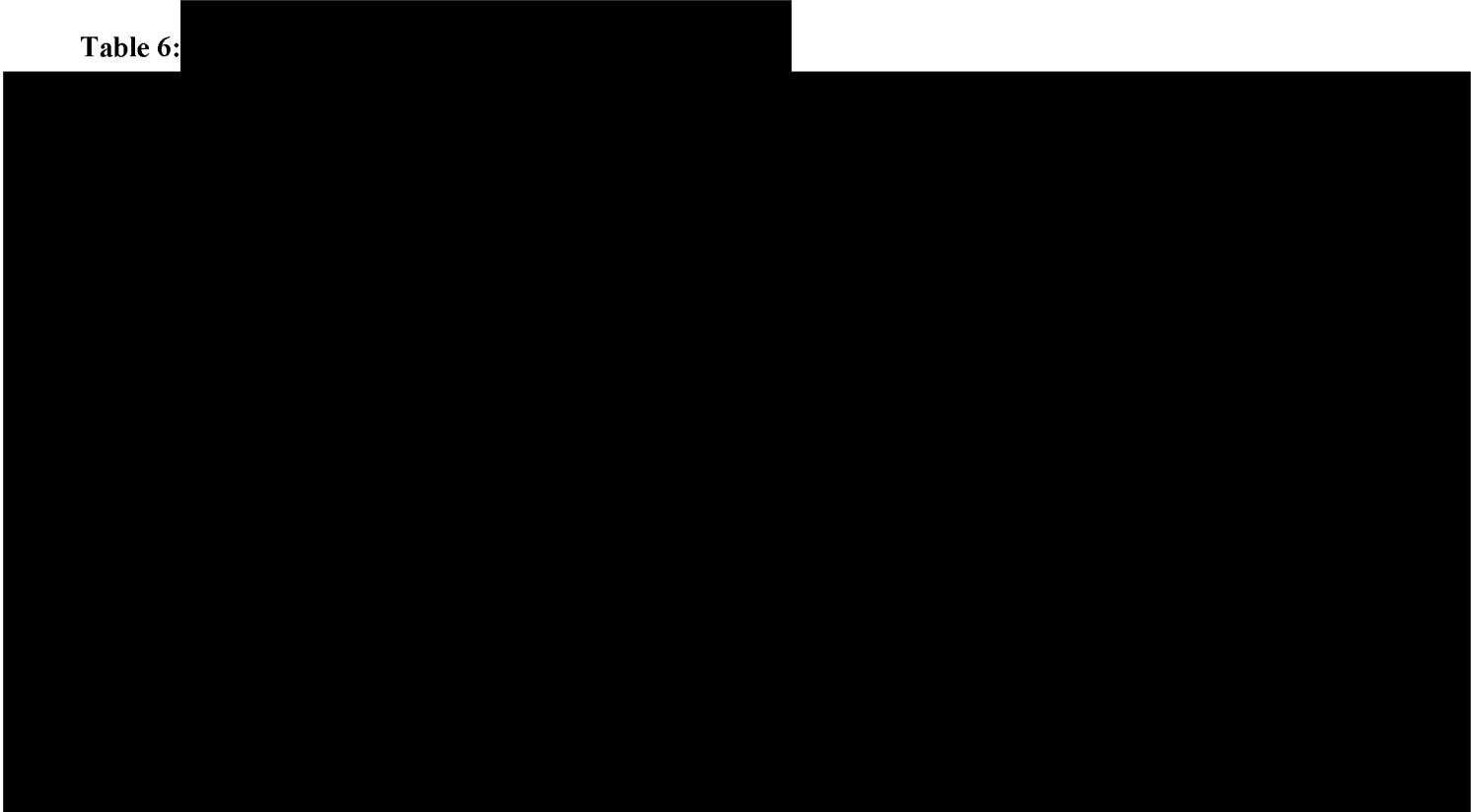
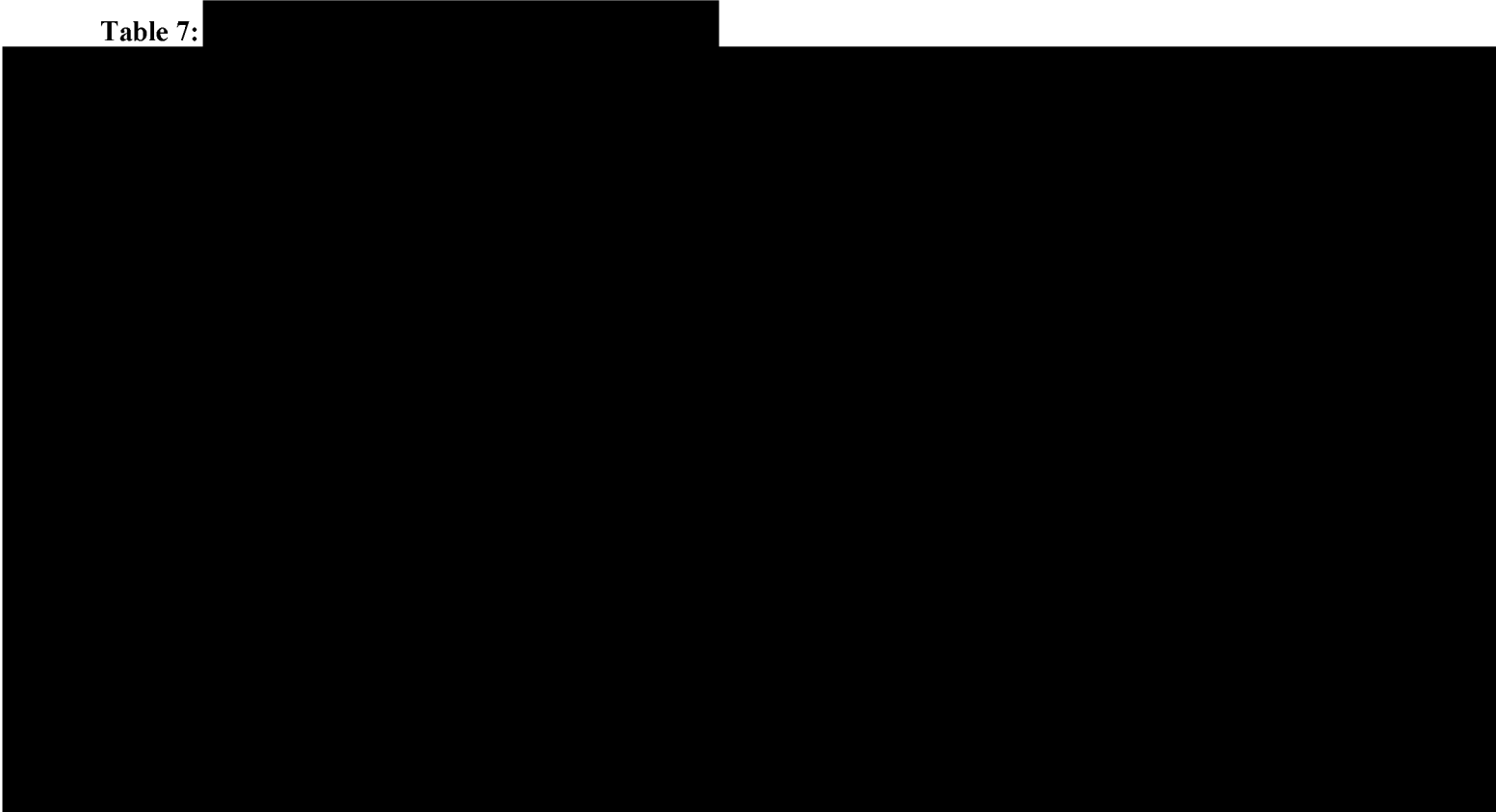
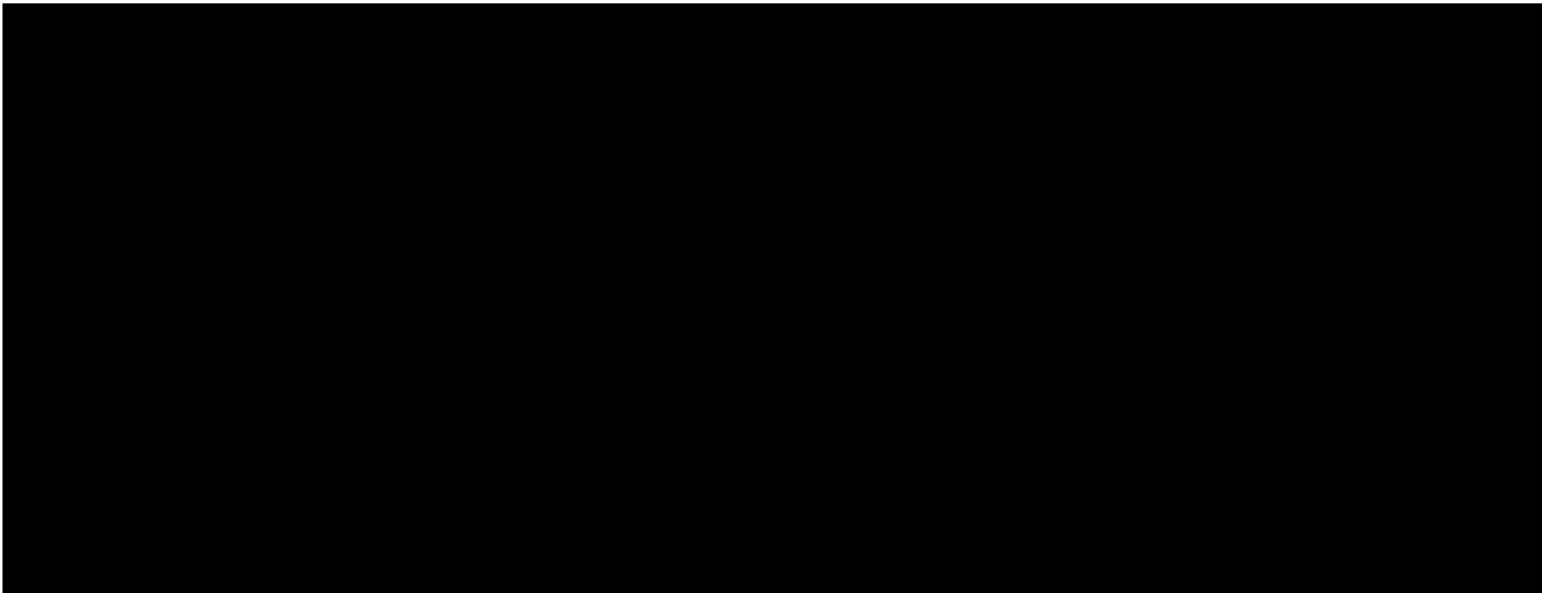


Table 7:



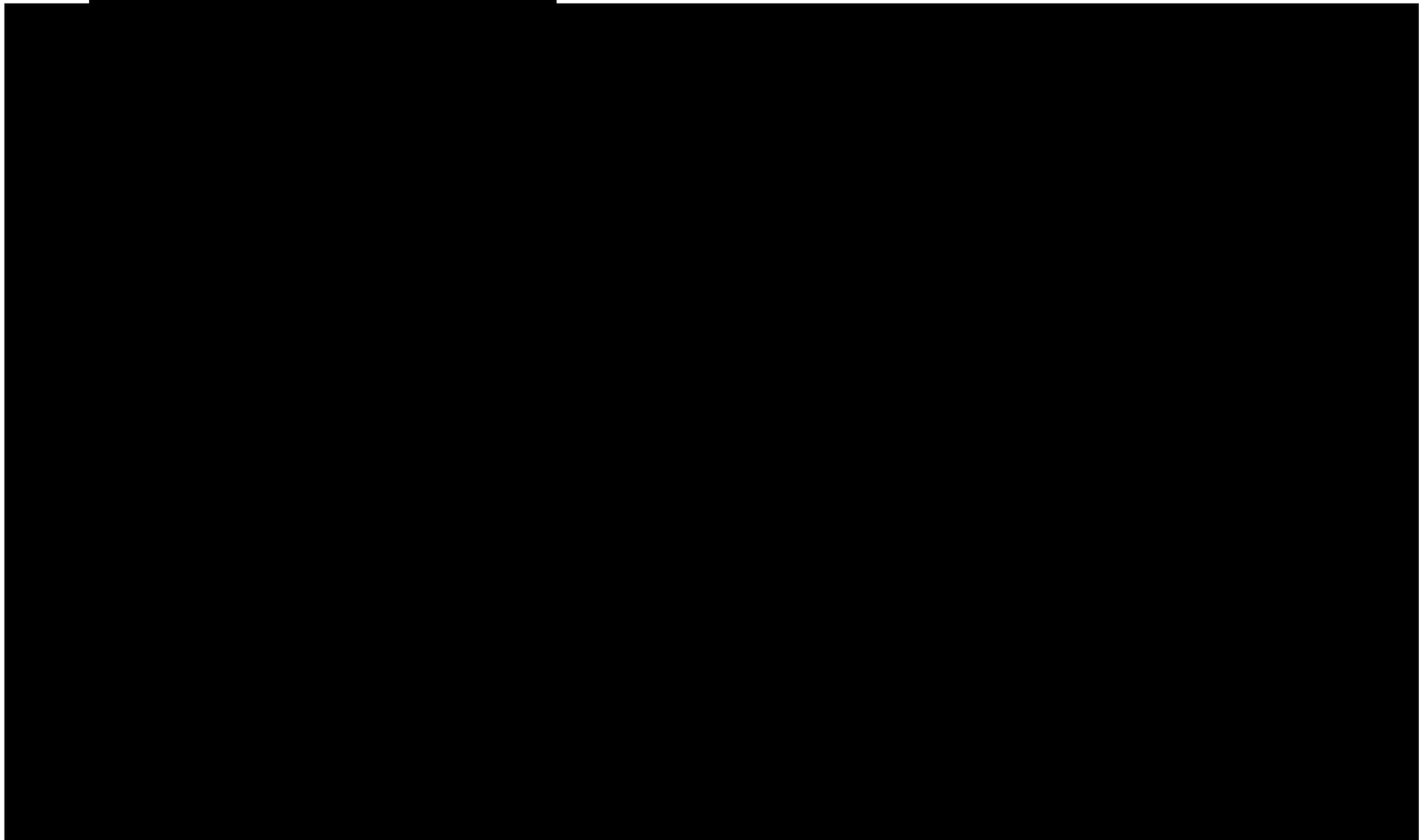
**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

D. 



NaBISCOP
USCIS FDNS-HB 602-001

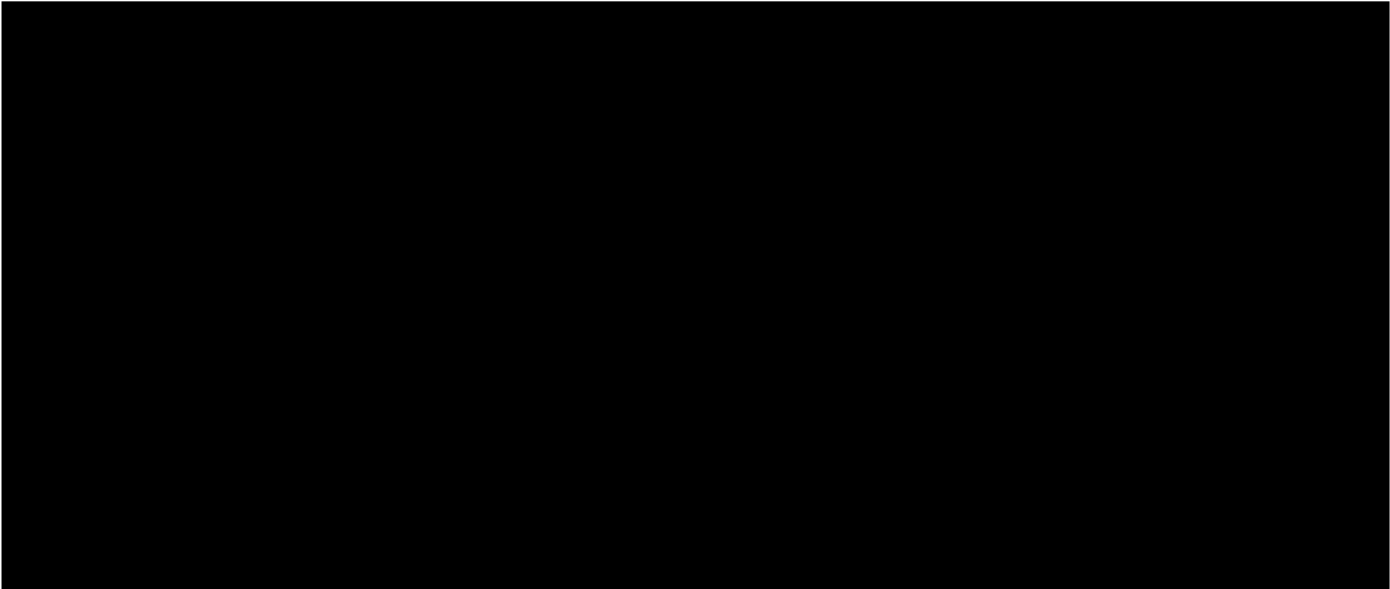
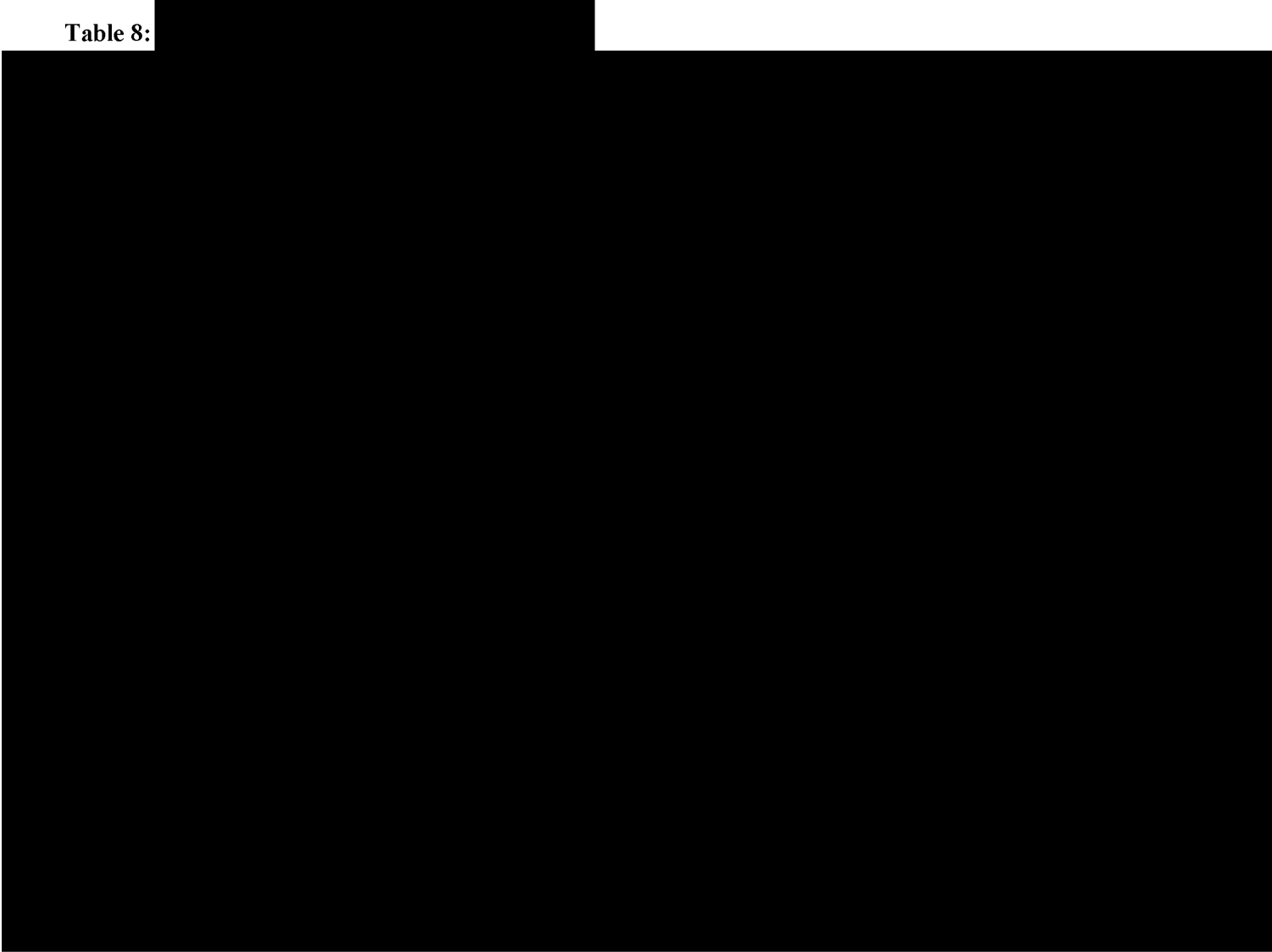


Table 8:



**NaBISCOP
USCIS FDNS-HB 602-001**

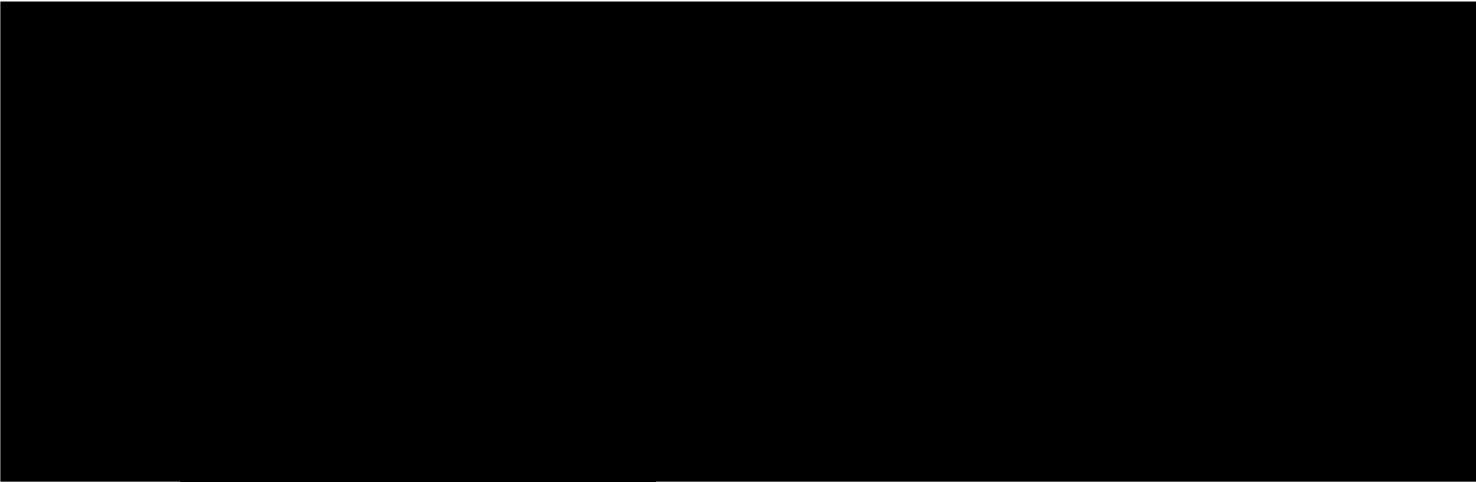
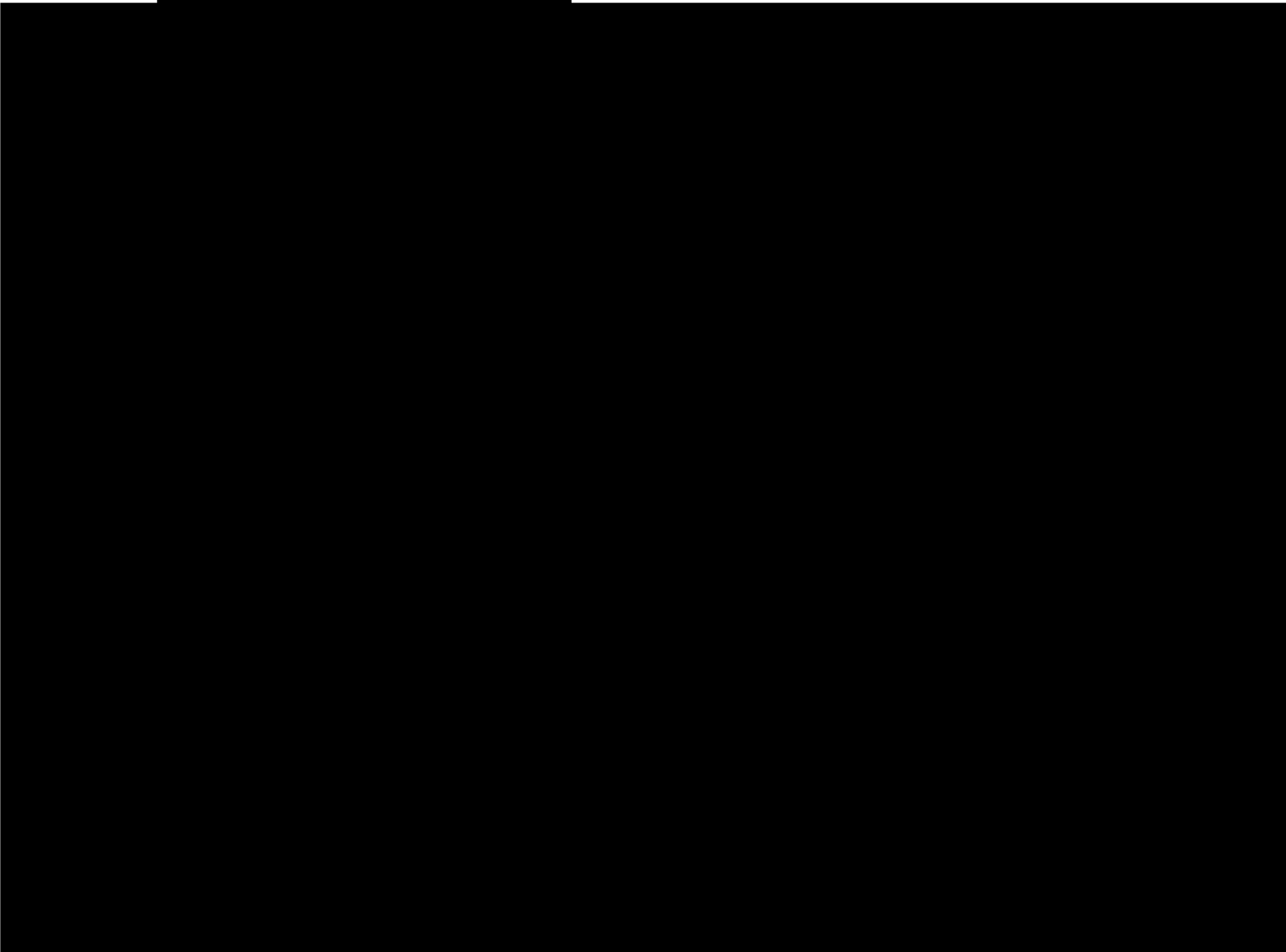
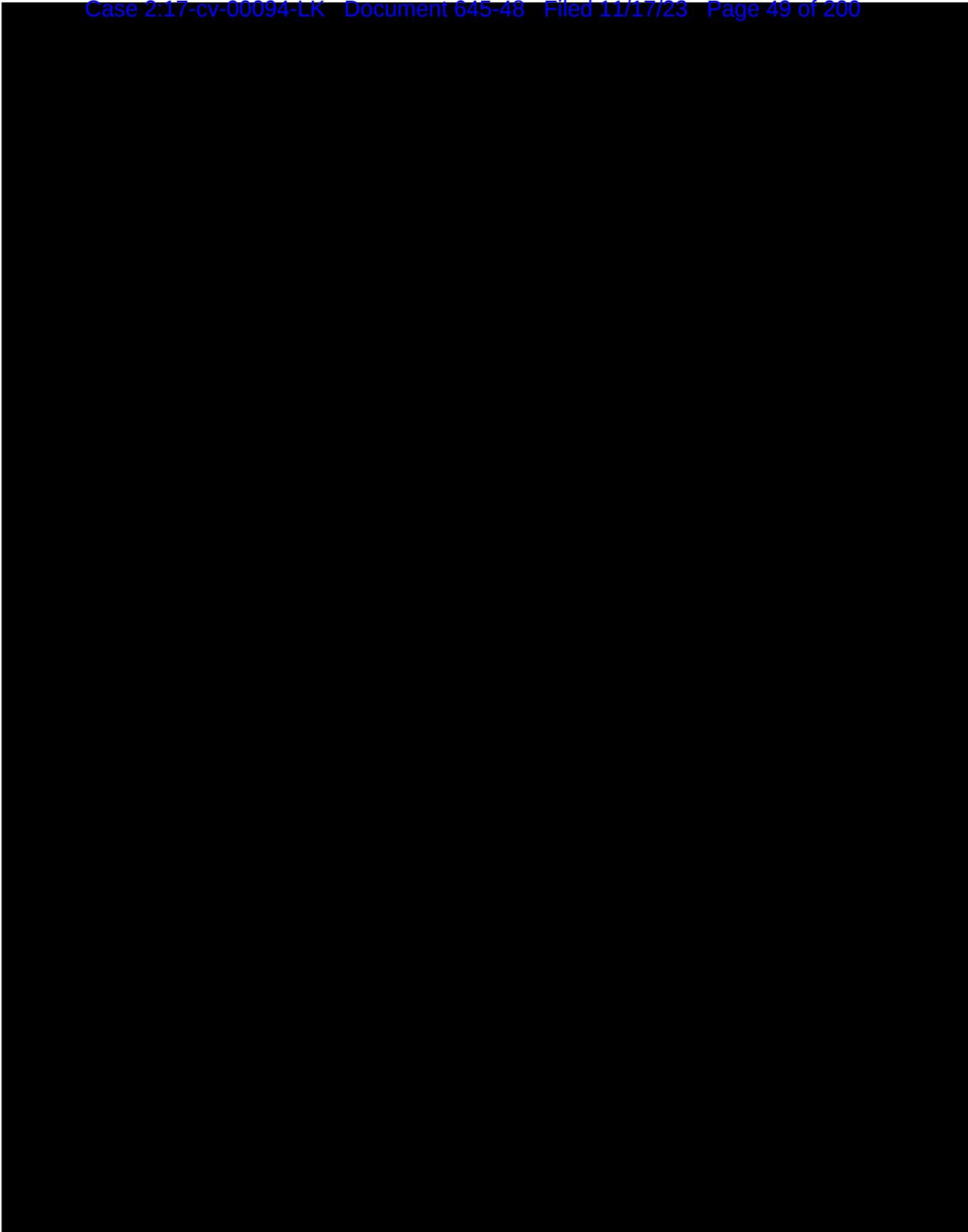


Figure 4:

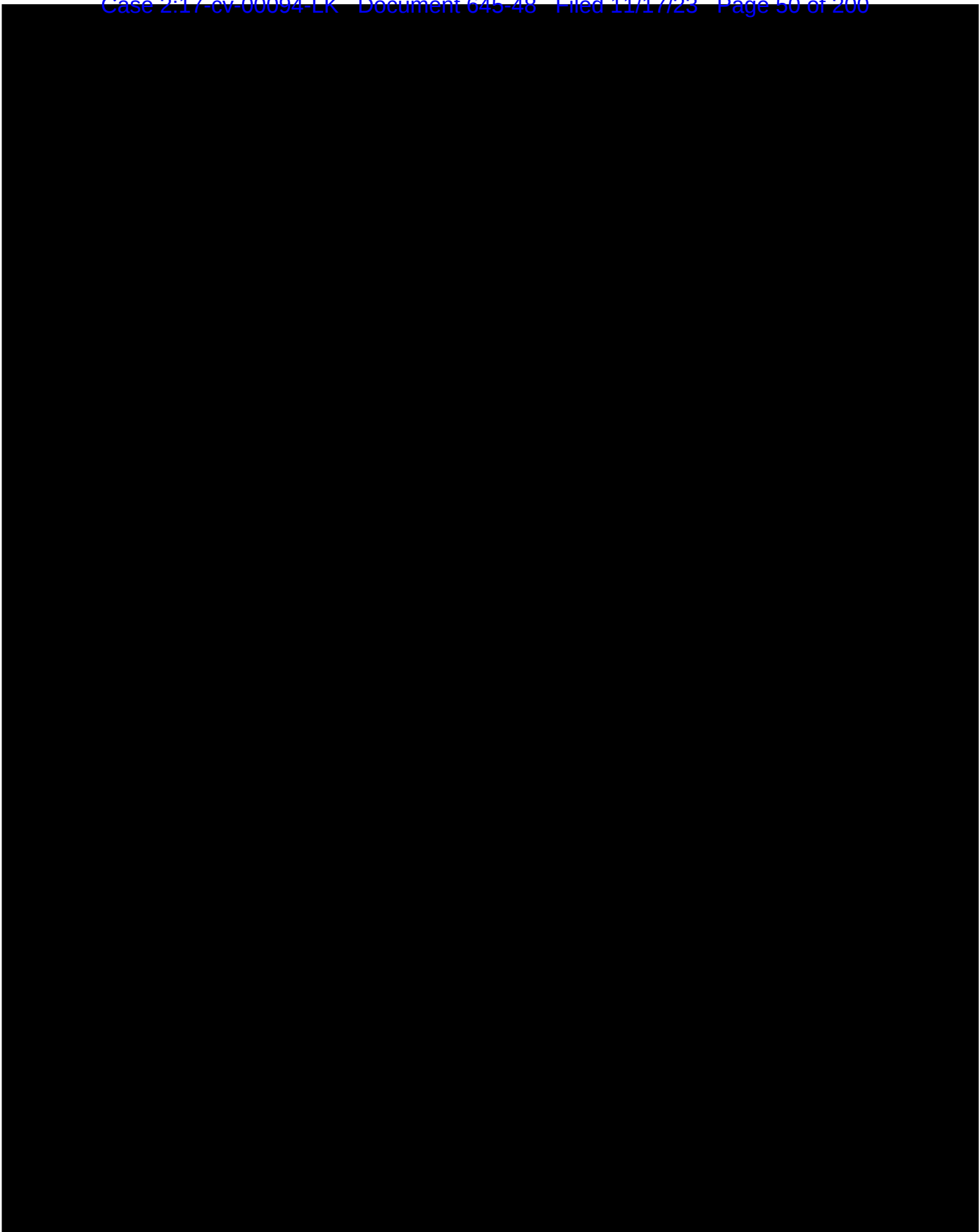


**NaBISCOP
USCIS FDNS-HB 602-001**



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001



Table 9:

A large, solid black rectangular redaction covering the entire content area of the table, obscuring all data and text.

**NaBISCOP
USCIS FDNS-HB 602-001**

[REDACTED]

Table 10:

[REDACTED]

Table 11:

[REDACTED]

**NaBISCOP
USCIS FDNS-HB 602-001**

[REDACTED]

Table 12:

[REDACTED]

Table 13:

[REDACTED]

Table 14:

[REDACTED]

**NaBISCOP
USCIS FDNS-HB 602-001**

[Redacted]

Table 15:

[Redacted]

Table 16:

[Redacted]

Table 17:

[Redacted]

Table 18:

[Redacted]

**NaBISCOP
USCIS FDNS-HB 602-001**

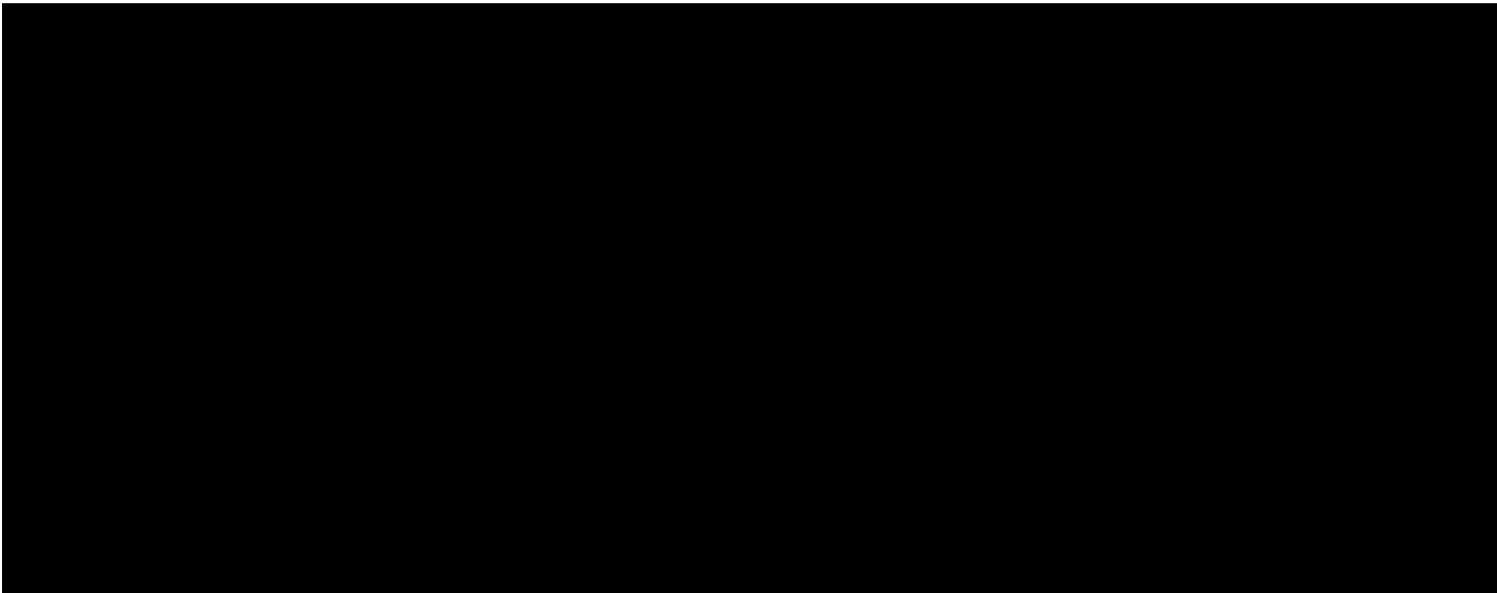


Table 19:

The content of Table 19 is completely redacted with a solid black box.

Table 20:

The content of Table 20 is completely redacted with a solid black box.

**NaBISCOP
USCIS FDNS-HB 602-001**

[REDACTED]

Table 21:

[REDACTED]

Table 22:

[REDACTED]

Table 23:

[REDACTED]

**NaBISCOP
USCIS FDNS-HB 602-001**



Table 24:

A large black rectangular redaction box covering the entire content area of Table 24.

Table 25:

A large black rectangular redaction box covering the entire content area of Table 25.

**NaBISCOP
USCIS FDNS-HB 602-001**

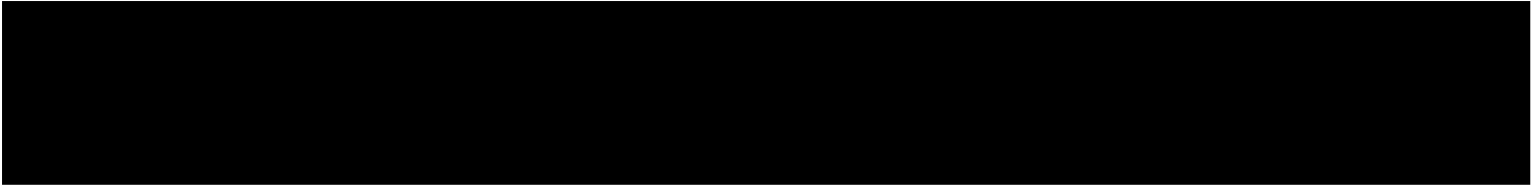


Table 26:

A large, solid black rectangular redaction box covering the entire content area of the page, obscuring the table and any other text that might have been present.

**NaBISCOP
USCIS FDNS-HB 602-001**

[Return to the Section Contents](#)
[Return to the Table of Contents](#)

E. 


Table 27: 


NaBISCOP
USCIS FDNS-HB 602-001



Figure 5:

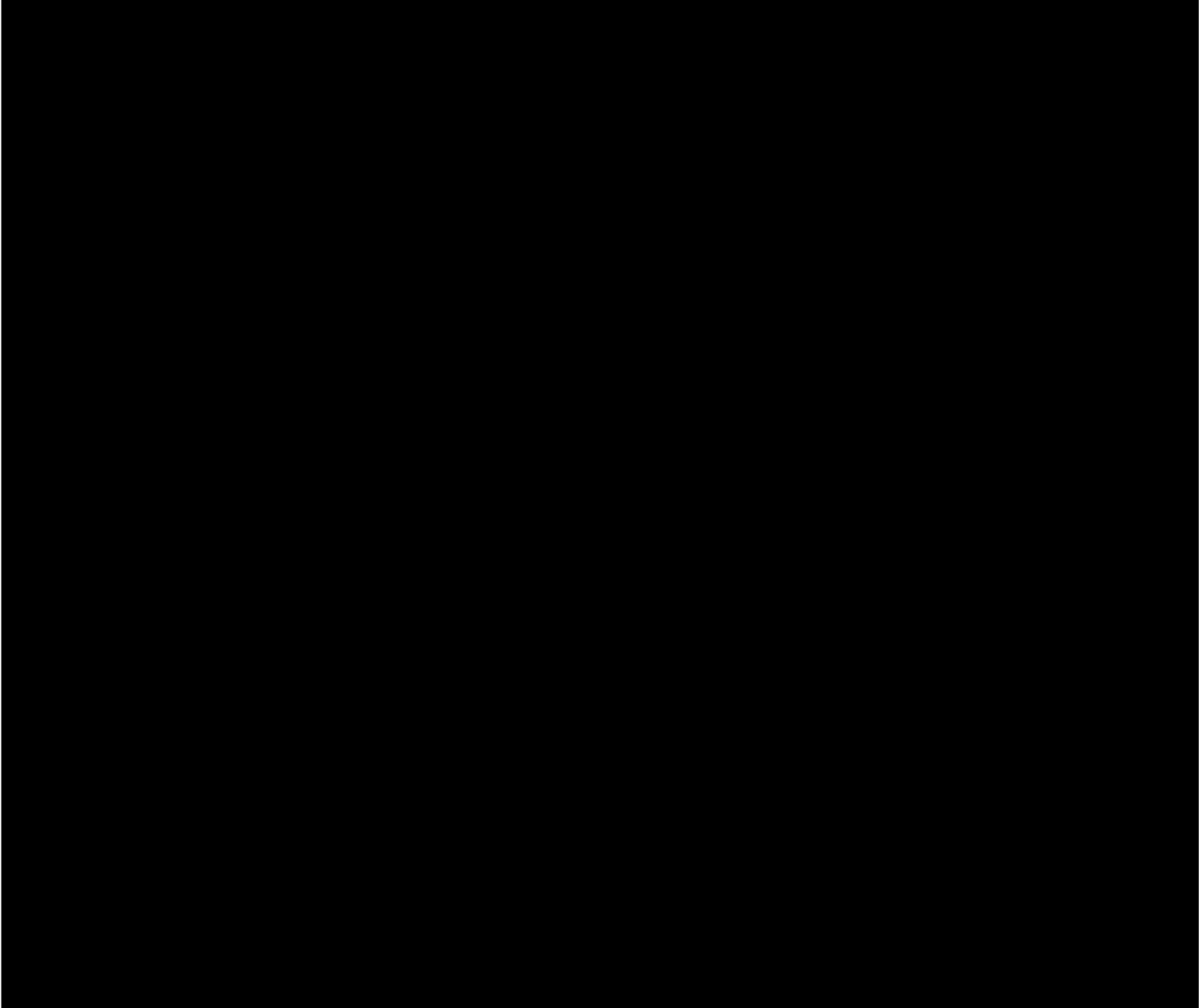
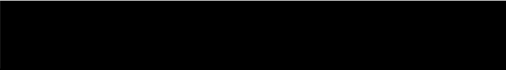


**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)
[Return to the Table of Contents](#)

F.



NaBISCOP
USCIS FDNS-HB 602-001

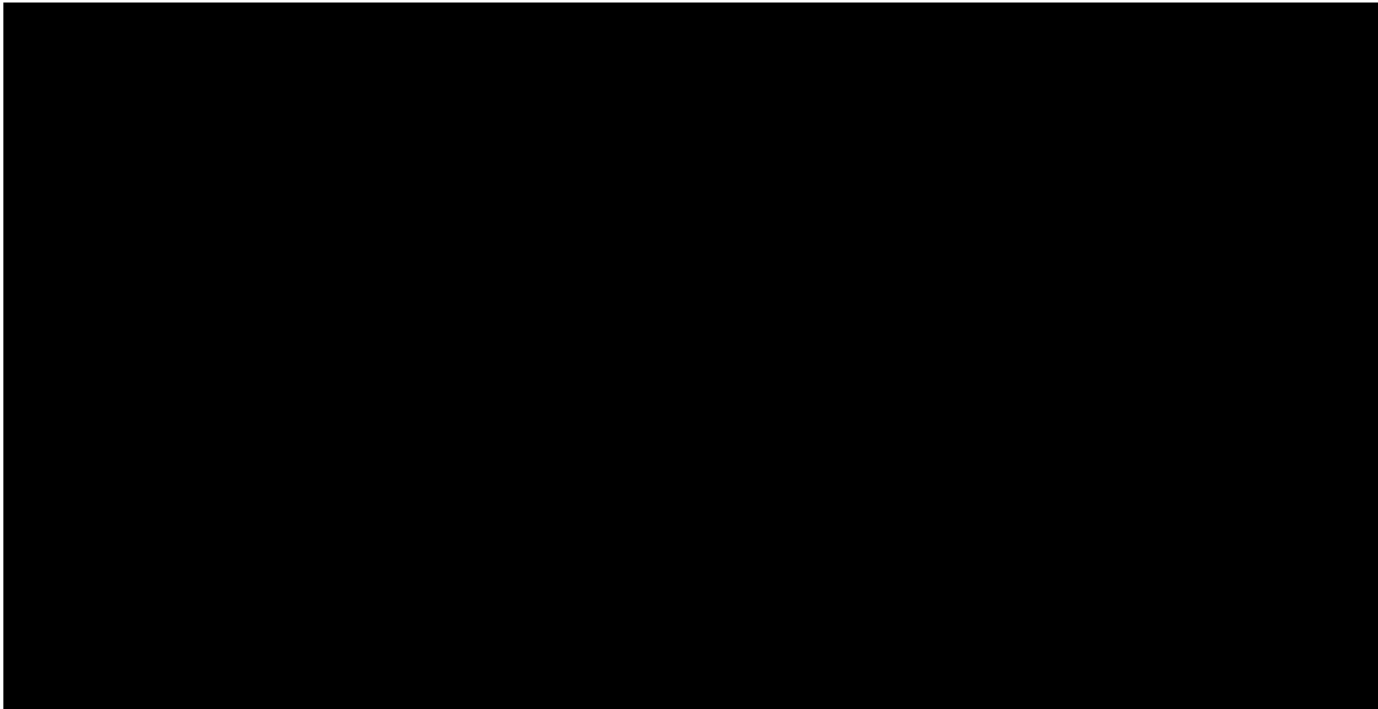
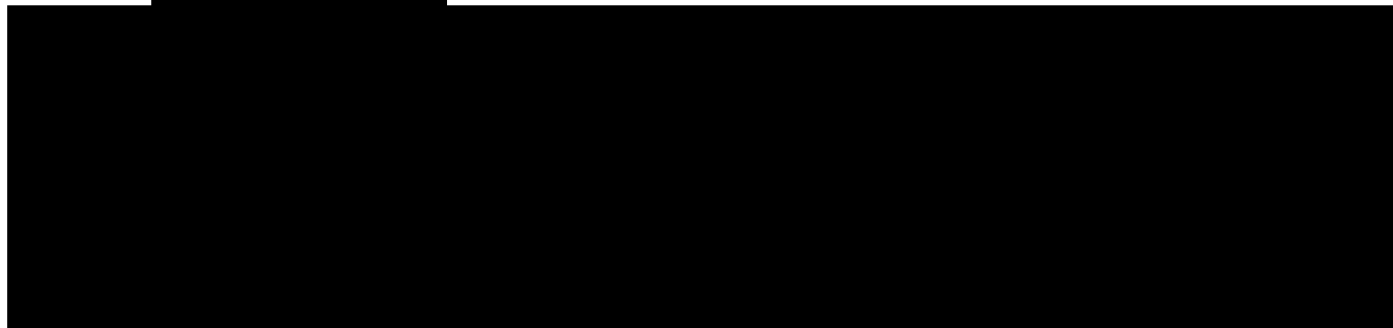
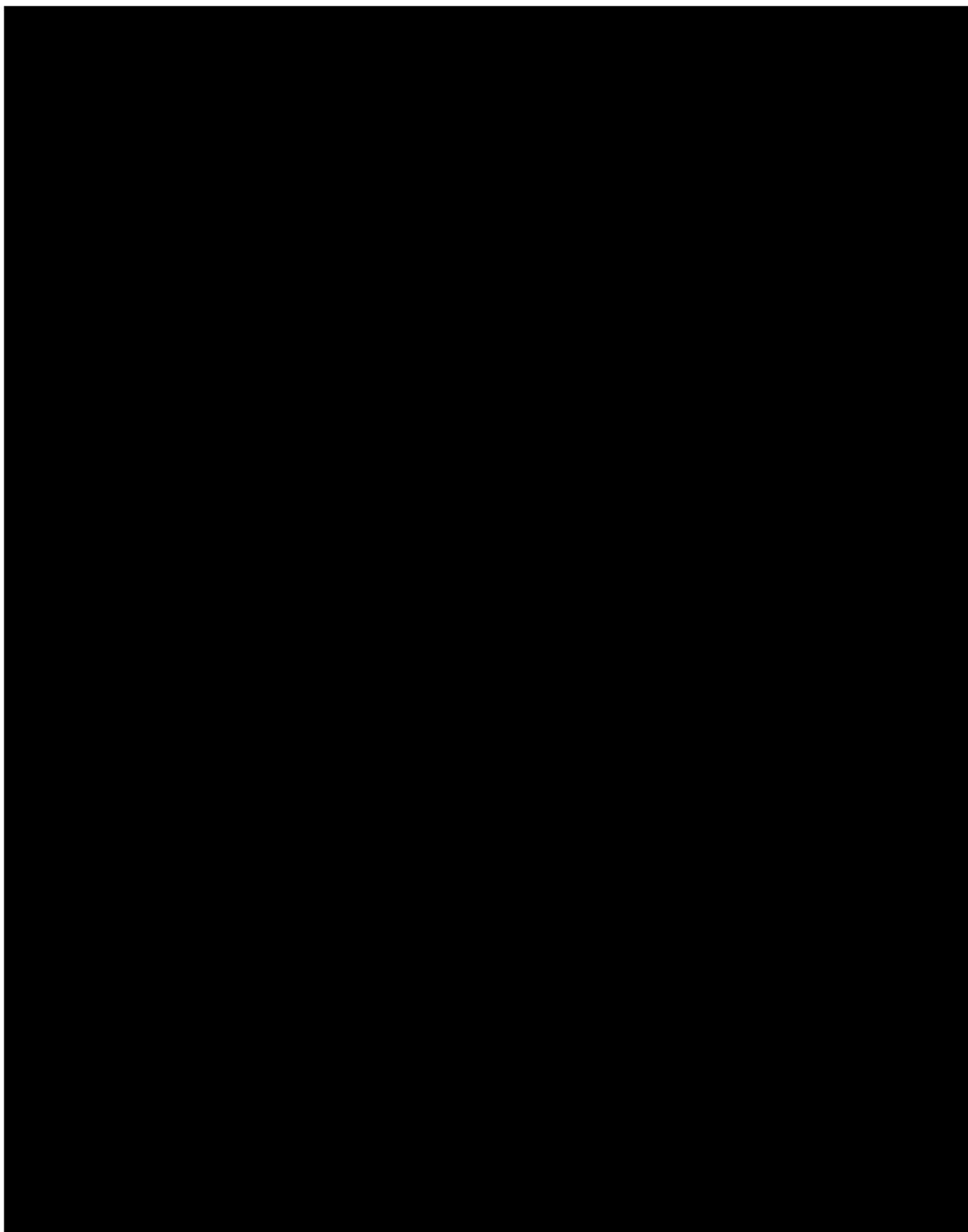


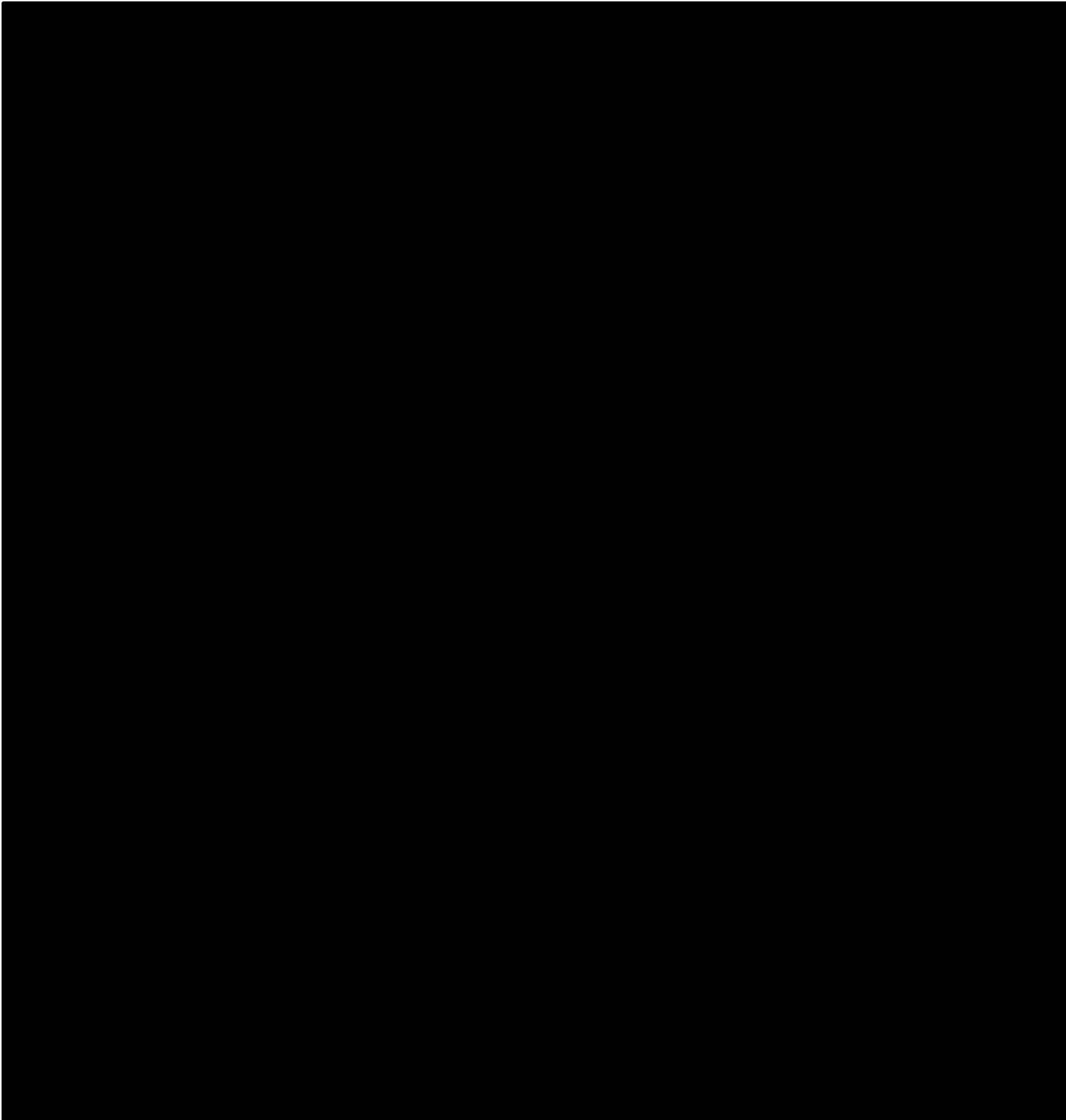
Table 28:



NaBISCOP
USCIS FDNS-HB 602-001

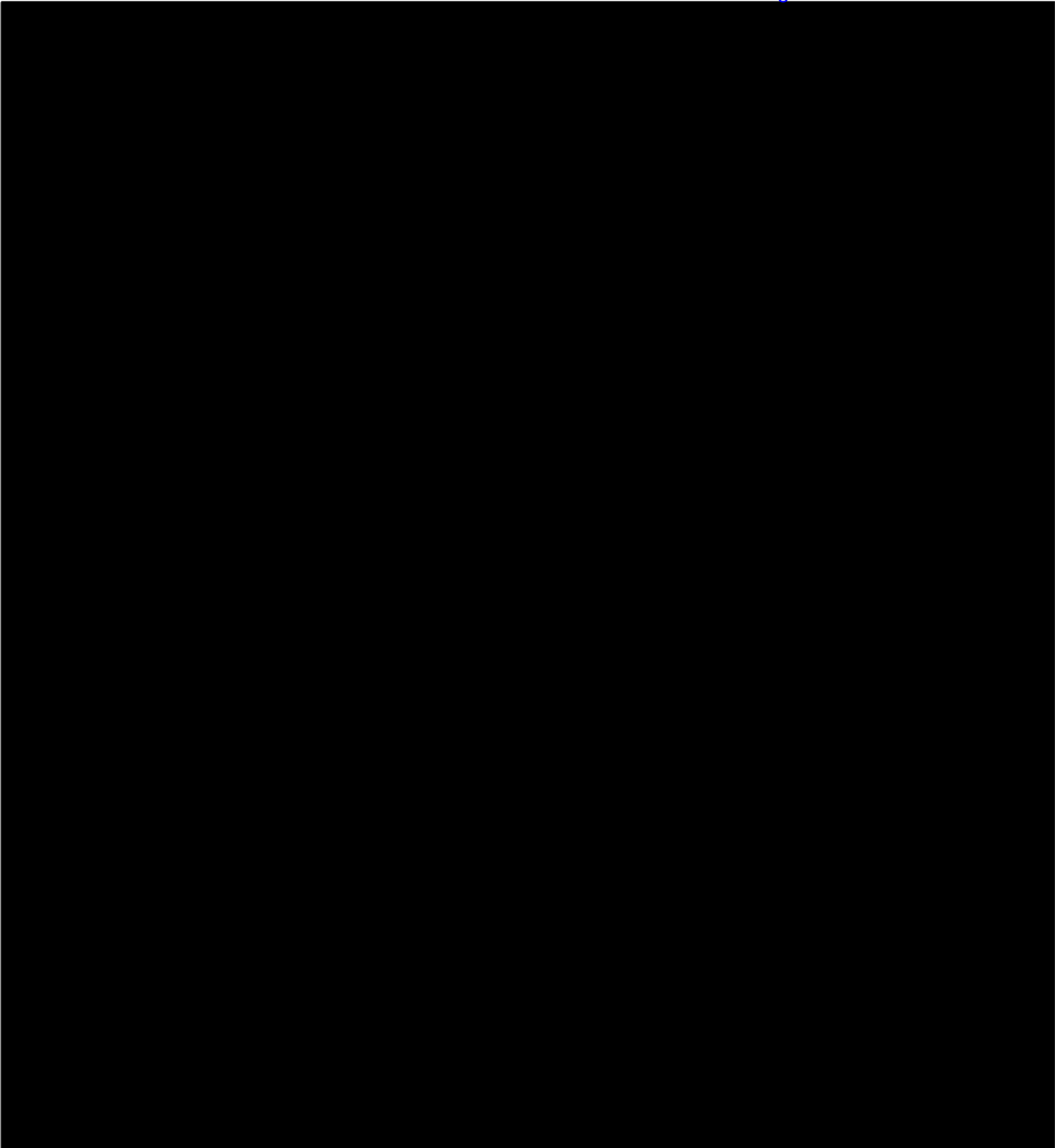


NaBISCOP
USCIS FDNS-HB 602-001



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES


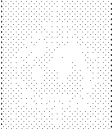








NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

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.

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:

	<p>Red Notice To seek the arrest or provisional arrest of wanted persons with a view to extradition.</p>		<p>Yellow Notice To help locate missing persons, often minors, or to help identify persons who are unable to identify themselves.</p>
	<p>Blue Notice To collect additional information about a person’s identity or activities in relation to a crime.</p>		<p>Black Notice To seek information on unidentified bodies.</p>
	<p>Green Notice To provide warnings and criminal intelligence about persons who have committed criminal offences and are likely to repeat these crimes in other countries.</p> <p><small>NOTE: Issued for persons who are the subjects of the United Nations Security Council Sanctions Regime, or persons who are the subjects of special notices and equipment seizures.</small></p>		<p>Orange Notice To warn police, public entities and other international organizations about potential threats from disguised weapons, parcel bombs and other dangerous materials.</p>
<div style="display: flex; align-items: center;">   <div> <p>INTERPOL-United Nations Special Notice Issued for groups and individuals who are the targets of UN sanctions against Al Qaeda and the Taliban.</p> </div> </div>			

Please access the INTERPOL website at <http://www.interpol.int/Public/Notices/default.asp> for more information on these notices.

Information about contacting INTERPOL for more information can be found in Appendix H, Notice to INTERPOL.

d. *All Other Hit types*

Examples include, but are not limited to the following:

- Agricultural violations;
- Visa overstays;
- Marriage fraud; or
- Absconders.

NaBISCOP
USCIS FDNS-HB 602-001

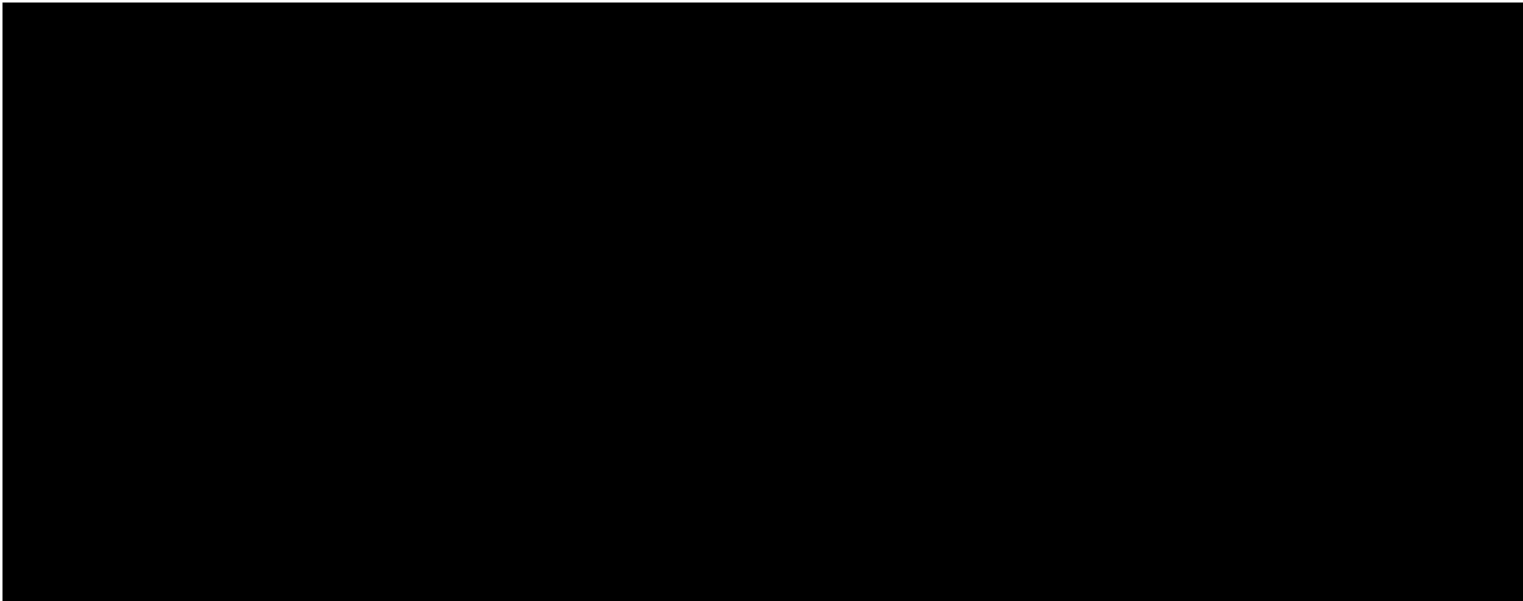
[Return to the Section Contents](#)

[Return to the Table of Contents](#)

H.



NaBISCOP
USCIS FDNS-HB 602-001



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

I.



NaBISCOP
USCIS FDNS-HB 602-001

For Official Use Only/Law Enforcement Sensitive

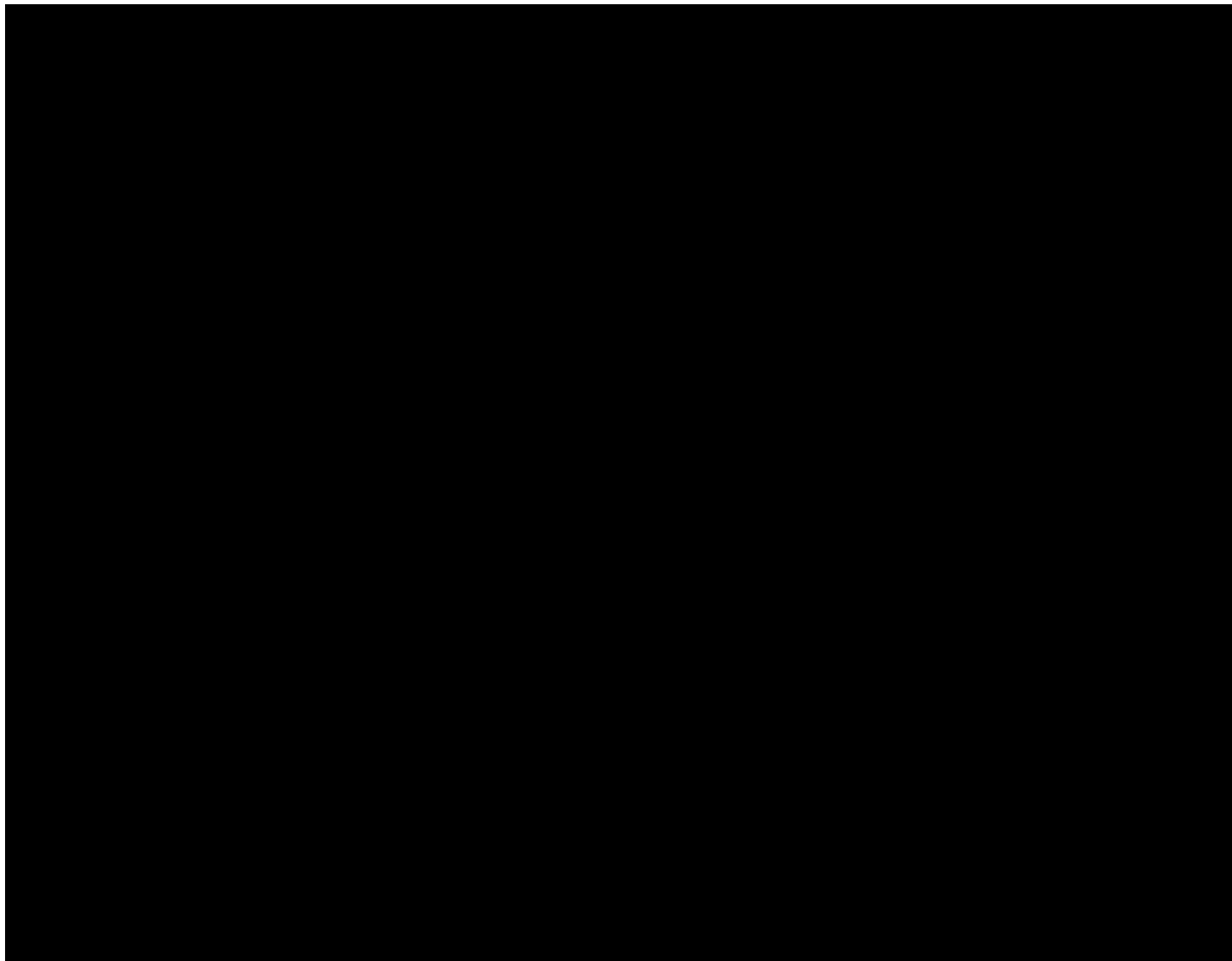


WARNING

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

**NaBISCOP
USCIS FDNS-HB 602-001**



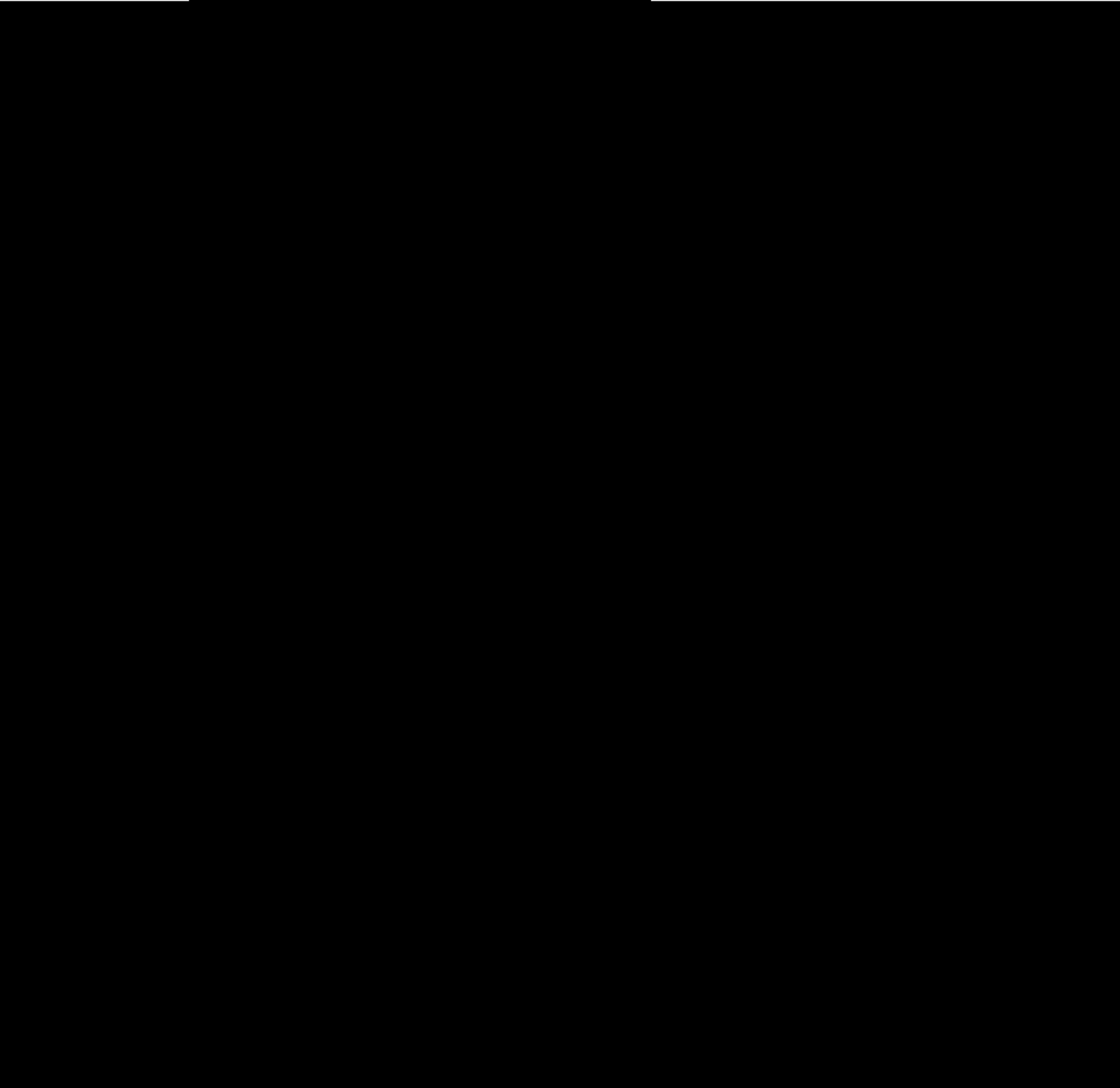
NaBISCOP
USCIS FDNS-HB 602-001

Figure 6:



NaBISCOP
USCIS FDNS-HB 602-001

Table 31:



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES



Figure 7: 

**NaBISCOP
USCIS FDNS-HB 602-001**

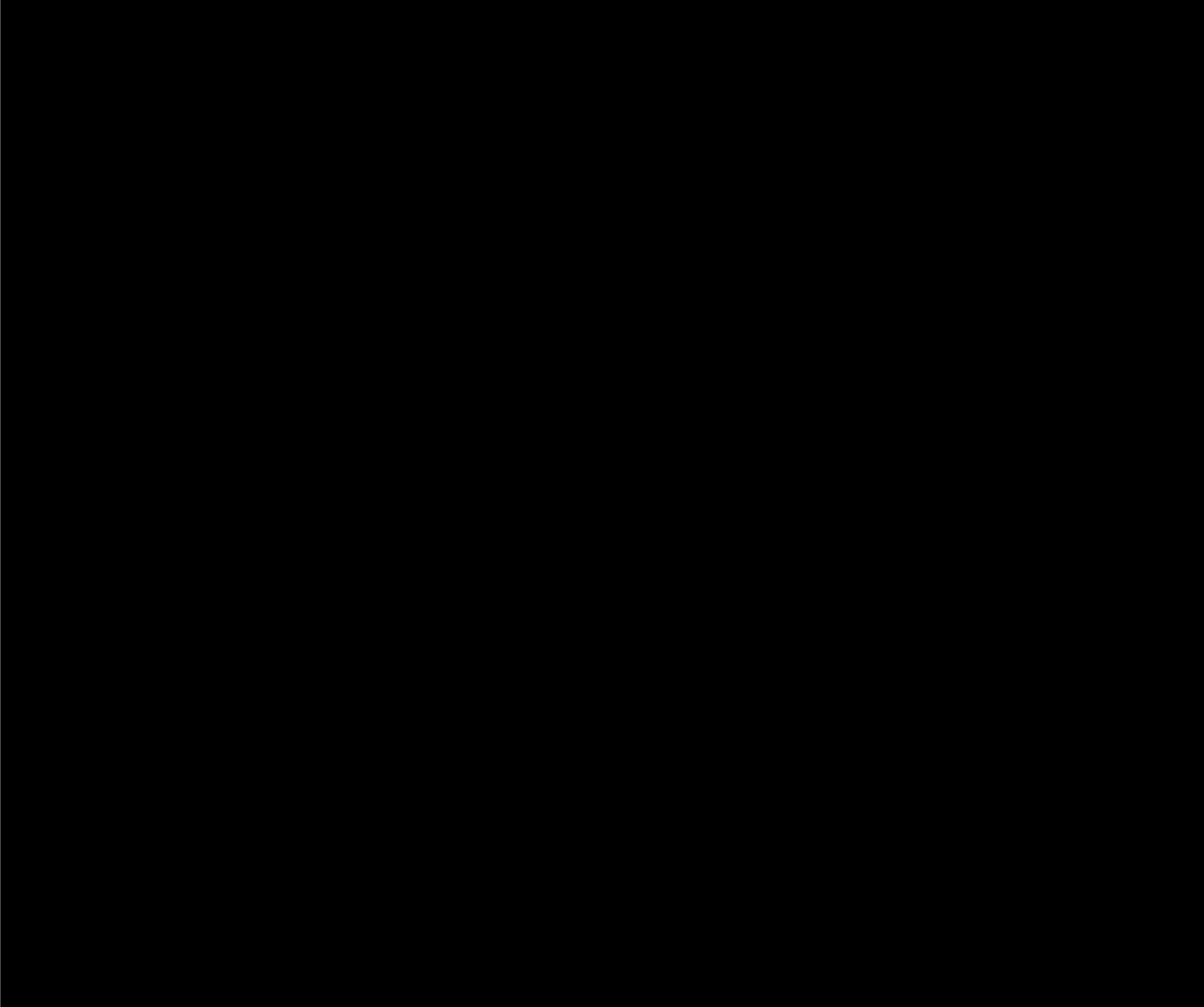
NaBISCOP
USCIS FDNS-HB 602-001

65

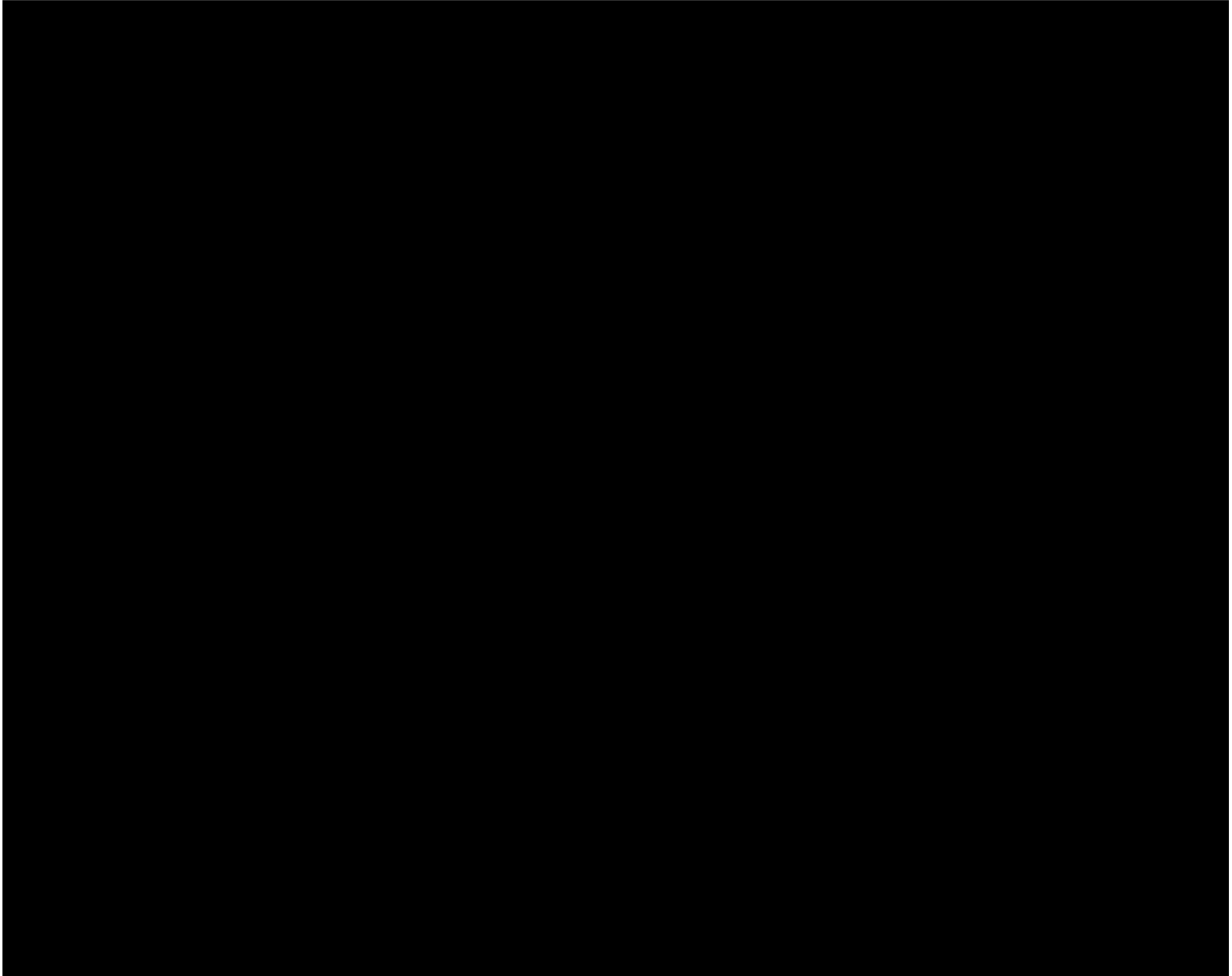
FOUO-LES

Figure 8:

[REDACTED]



NaBISCOP
USCIS FDNS-HB 602-001



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

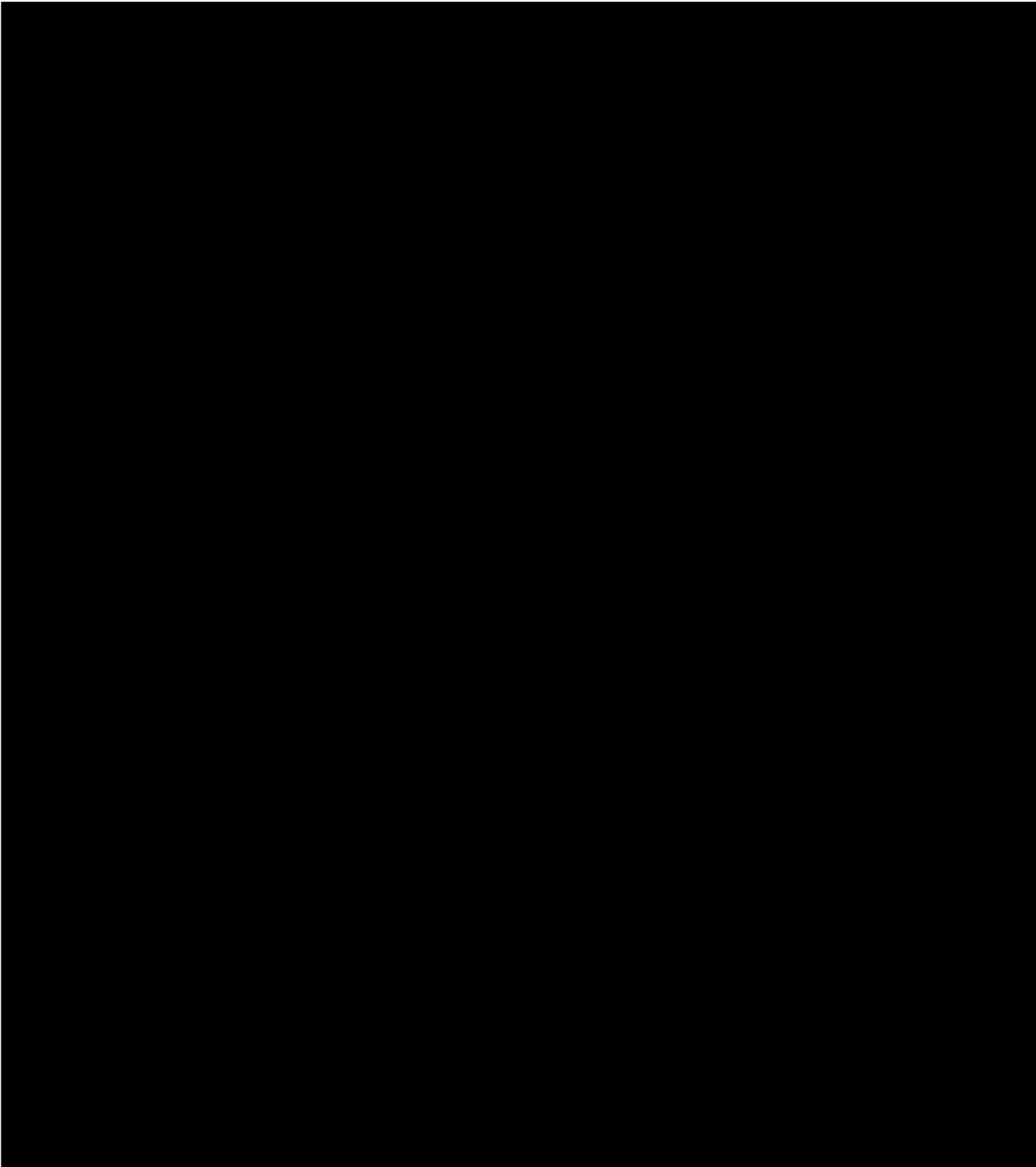
J.



NaBISCOP
USCIS FDNS-HB 602-001

68

FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

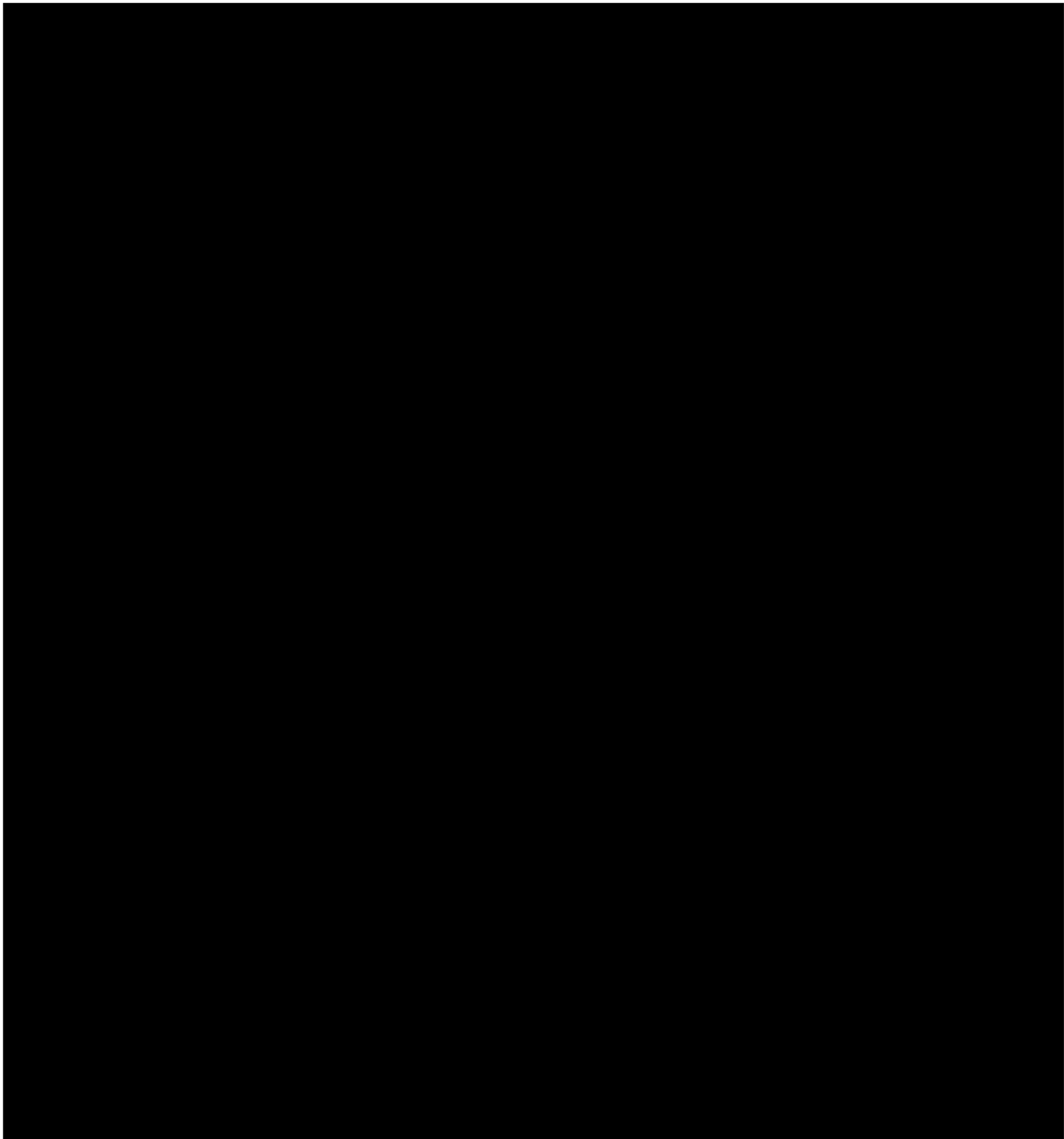
FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

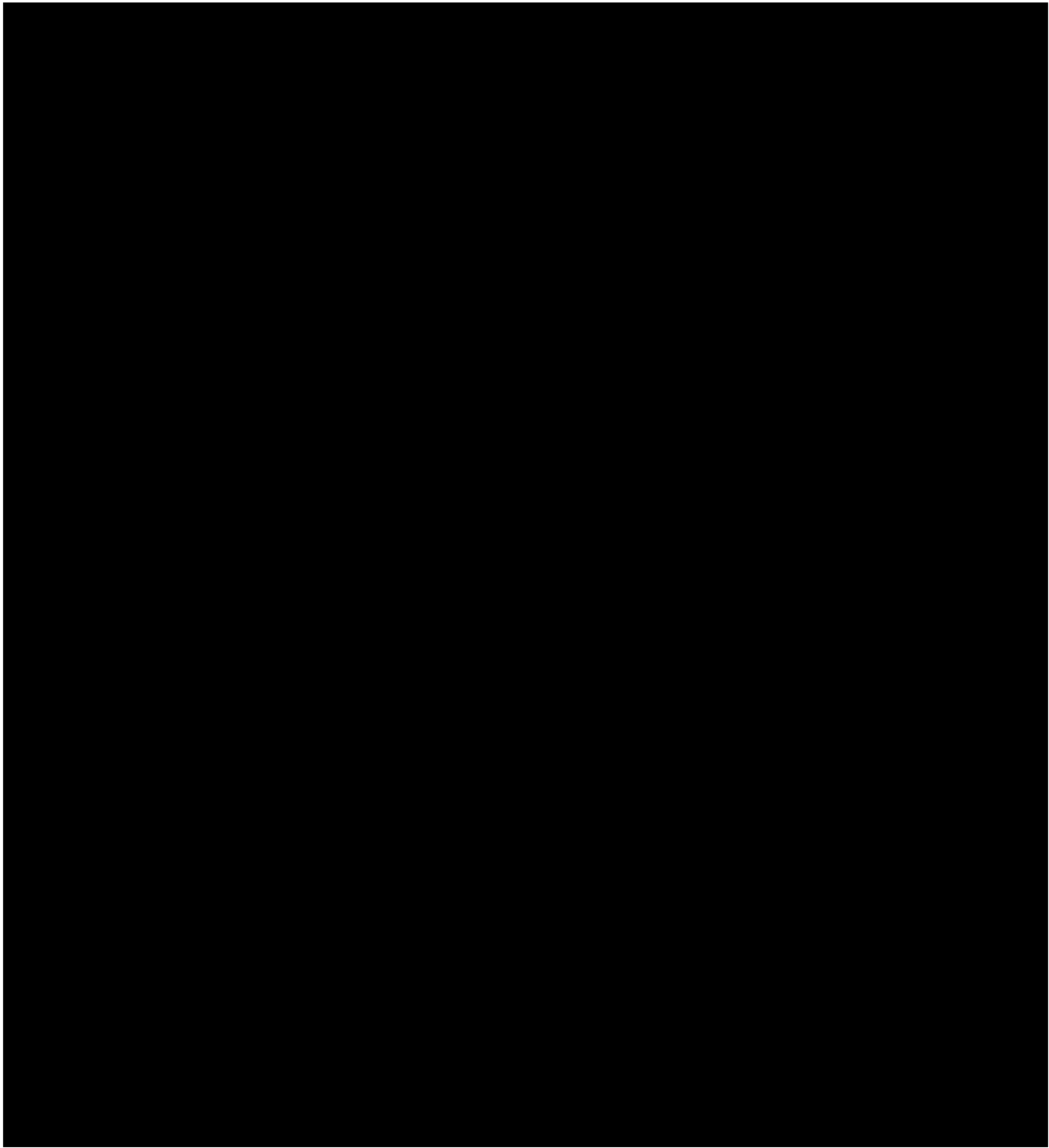
70

FOUO-LES



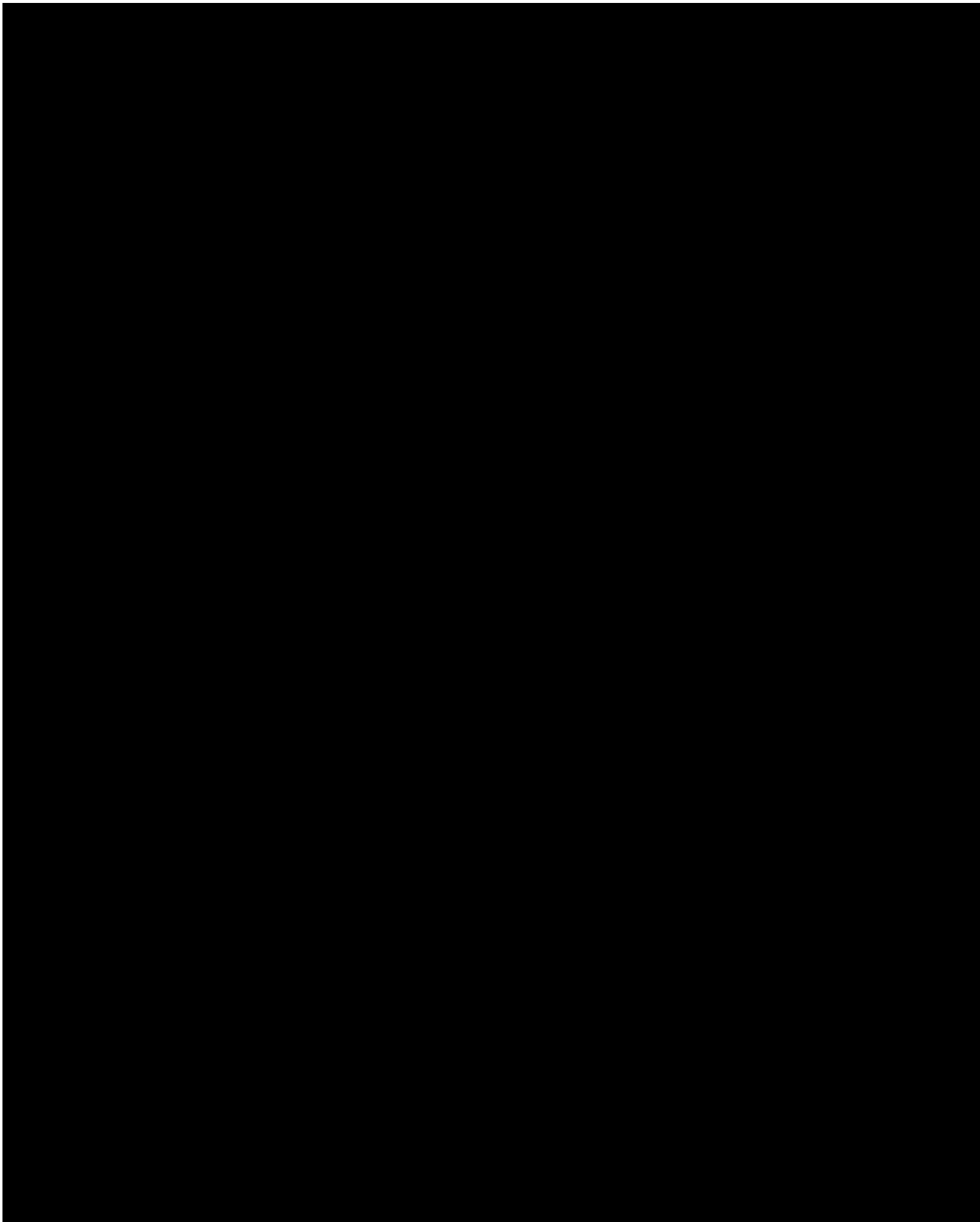
NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES



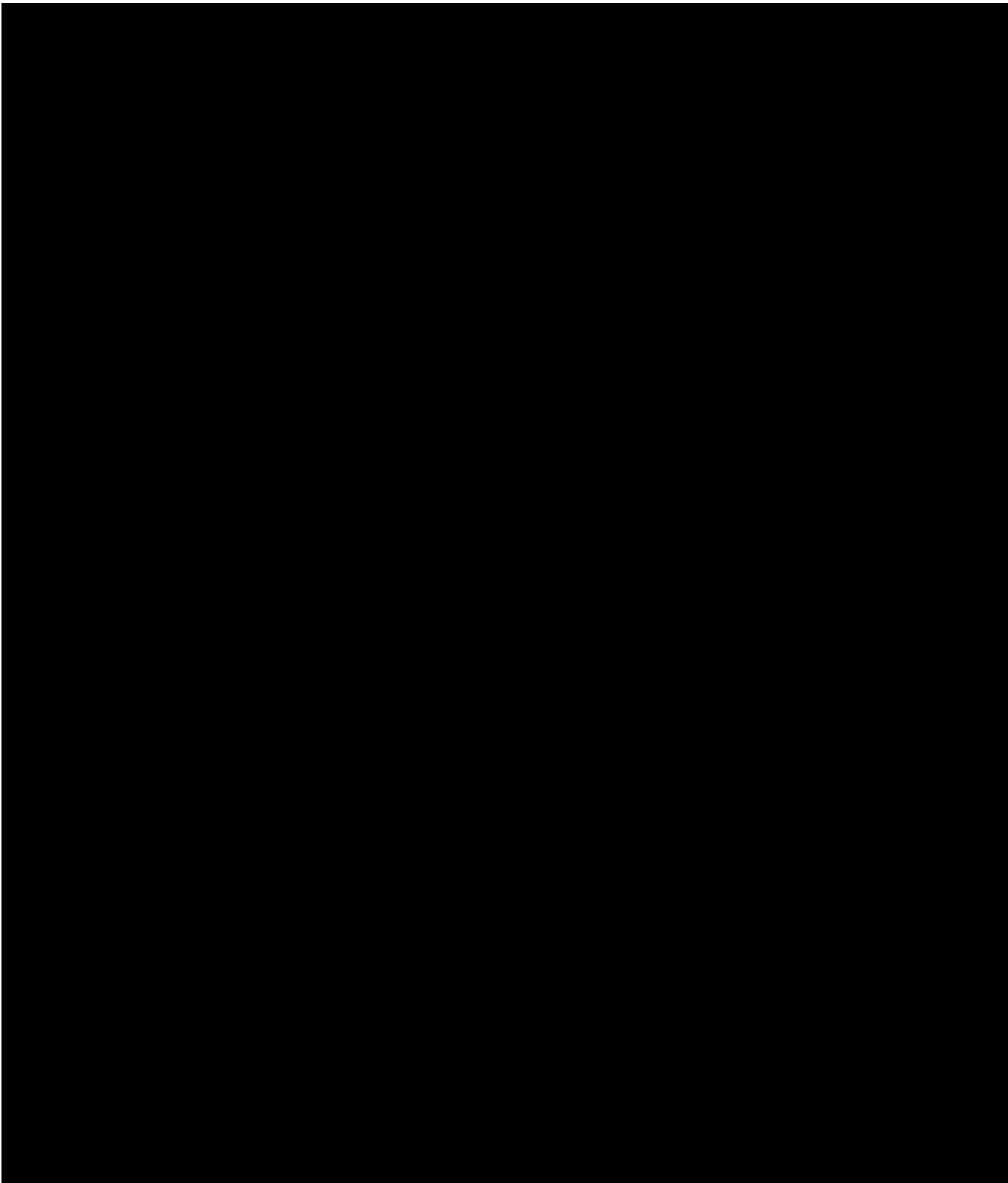
NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES



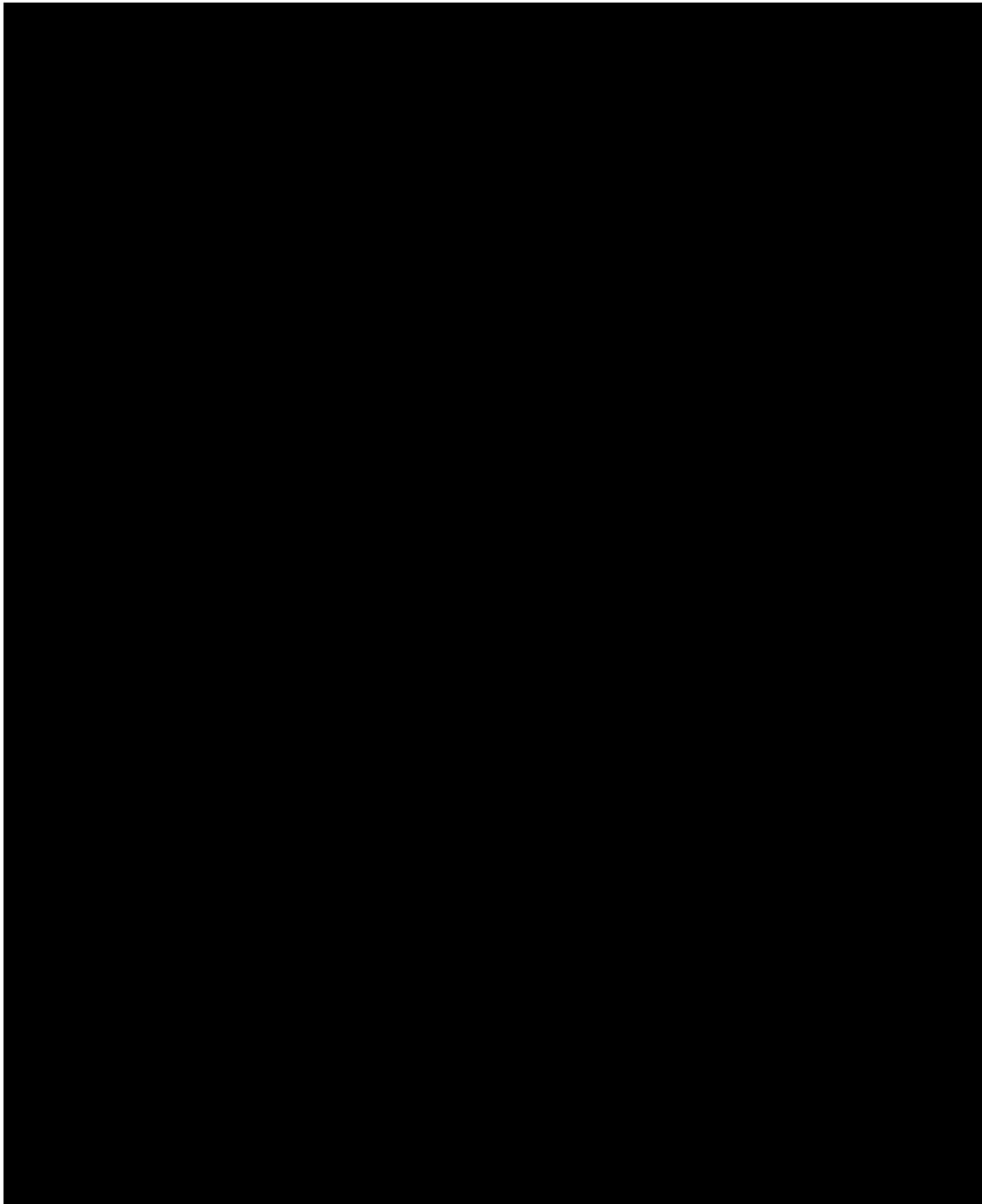
NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

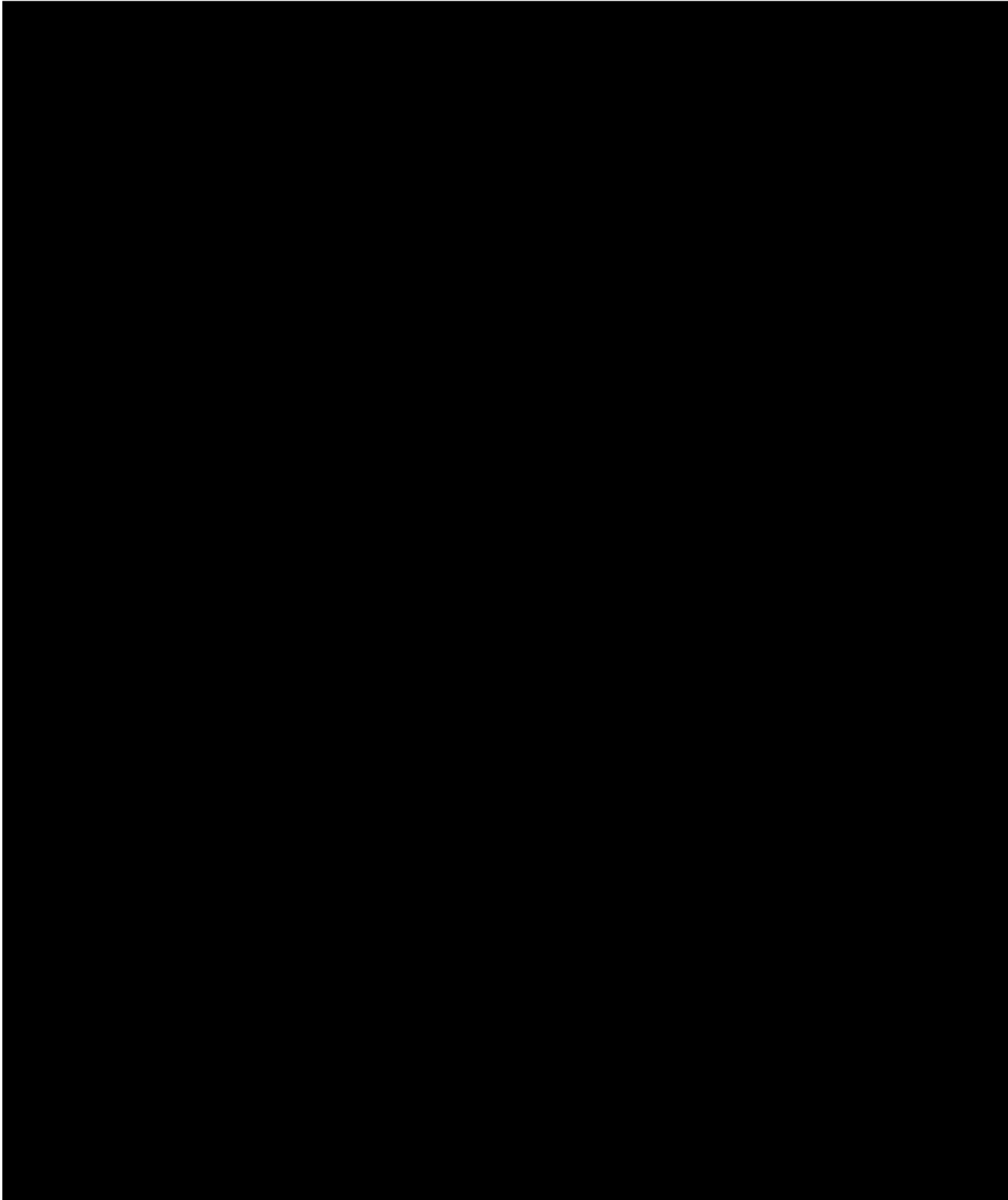


NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

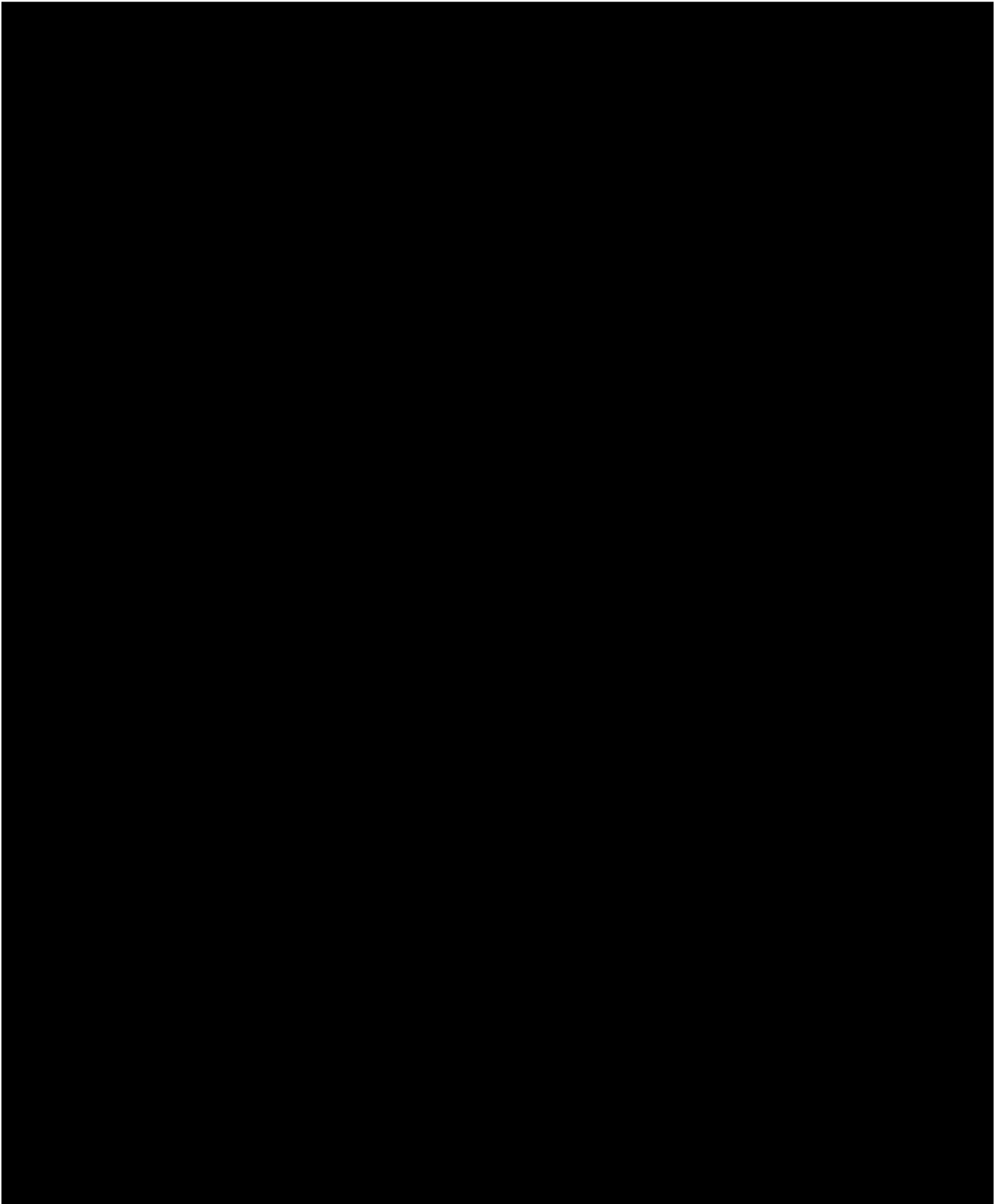


NaBISCOP
USCIS FDNS-HB 602-001

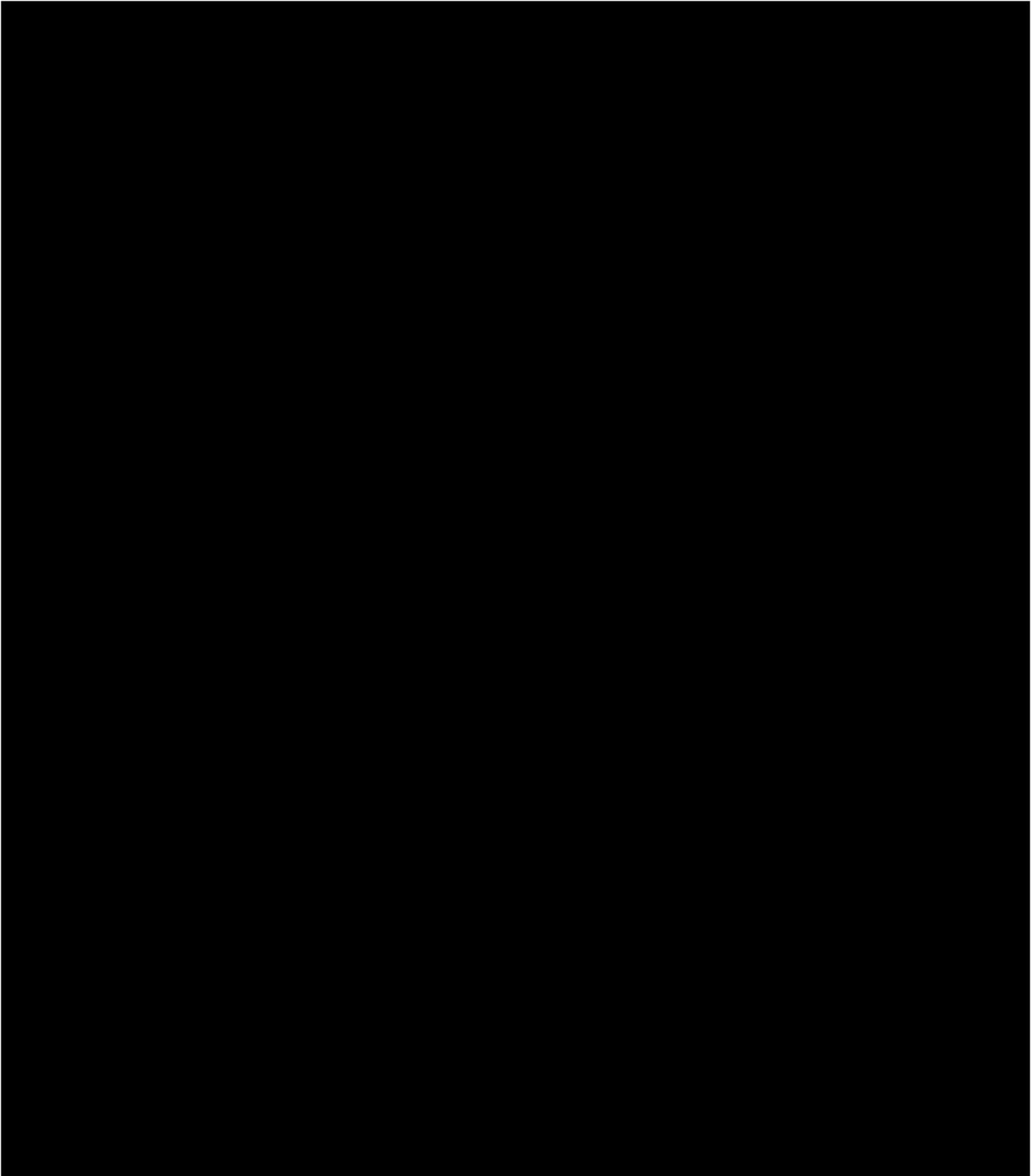


NaBISCOP
USCIS FDNS-HB 602-001

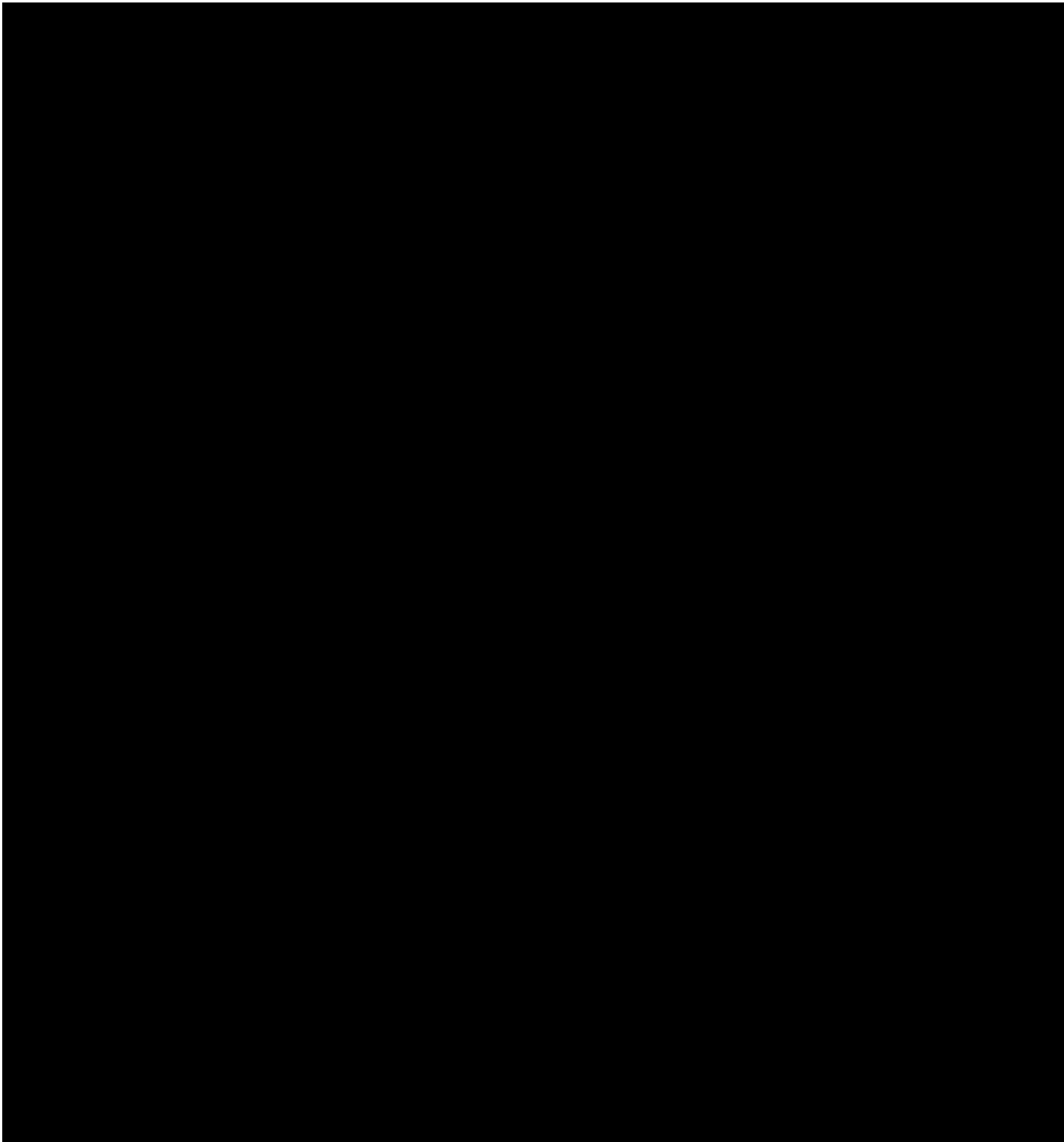
FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

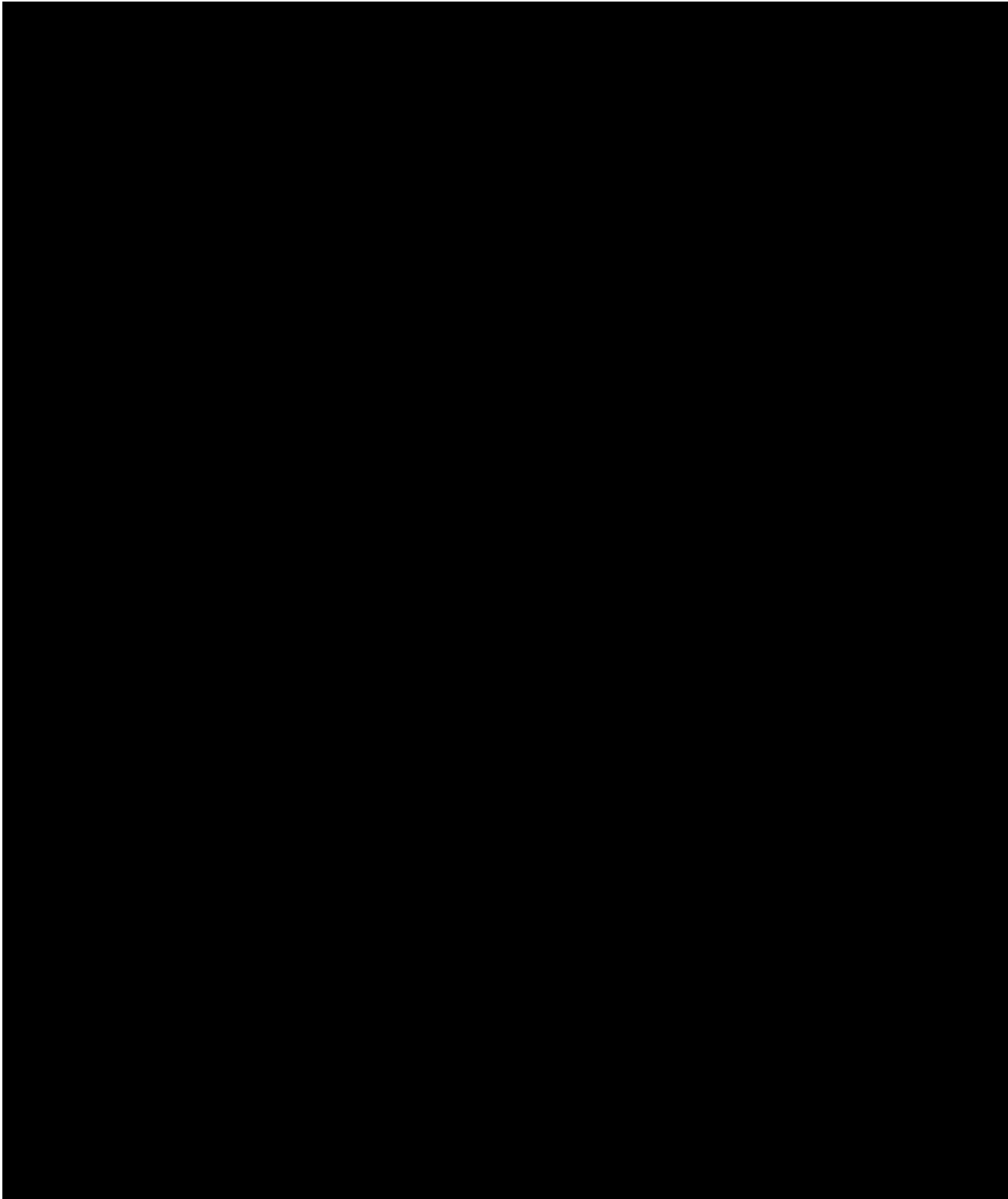


NaBISCOP
USCIS FDNS-HB 602-001



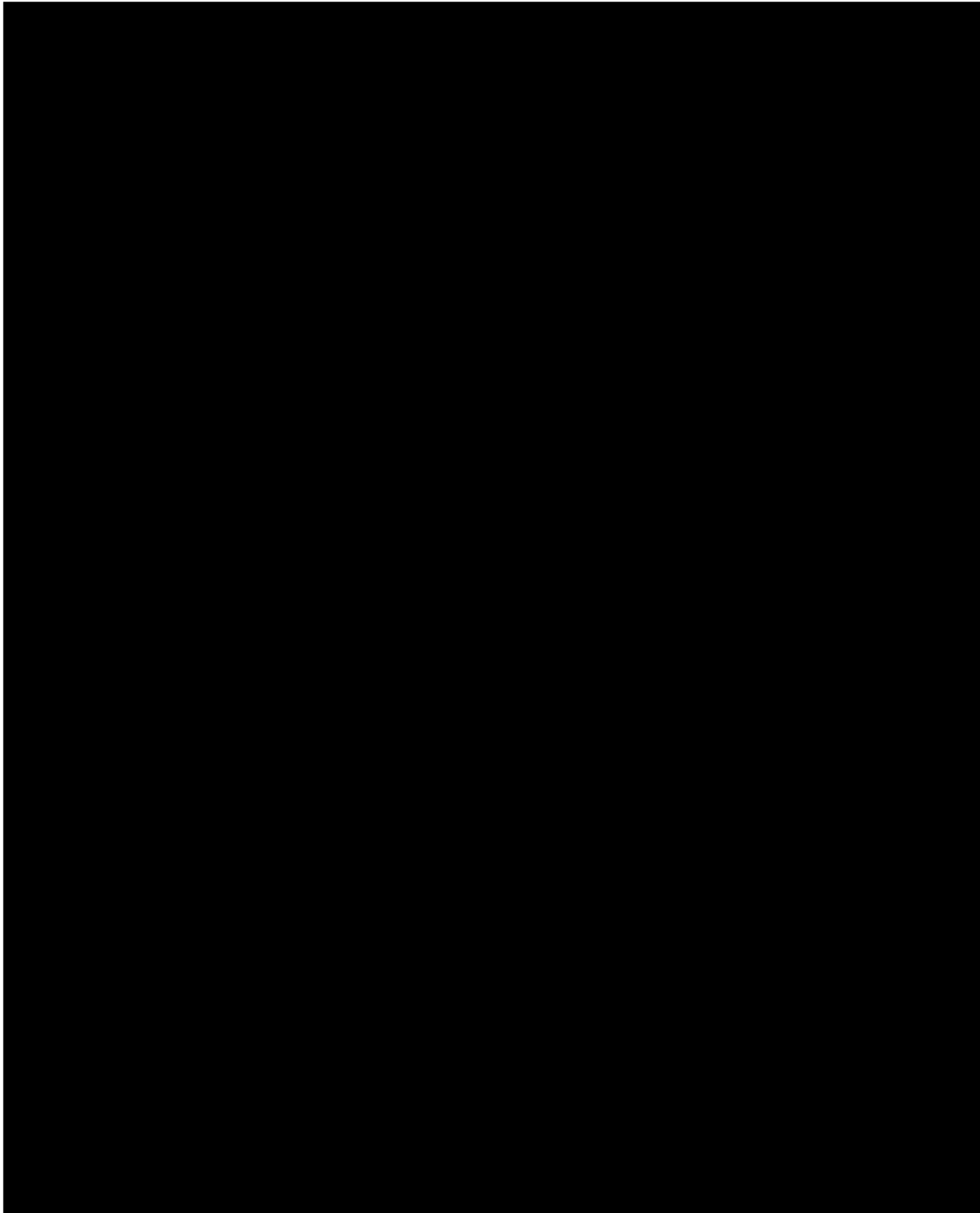
NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

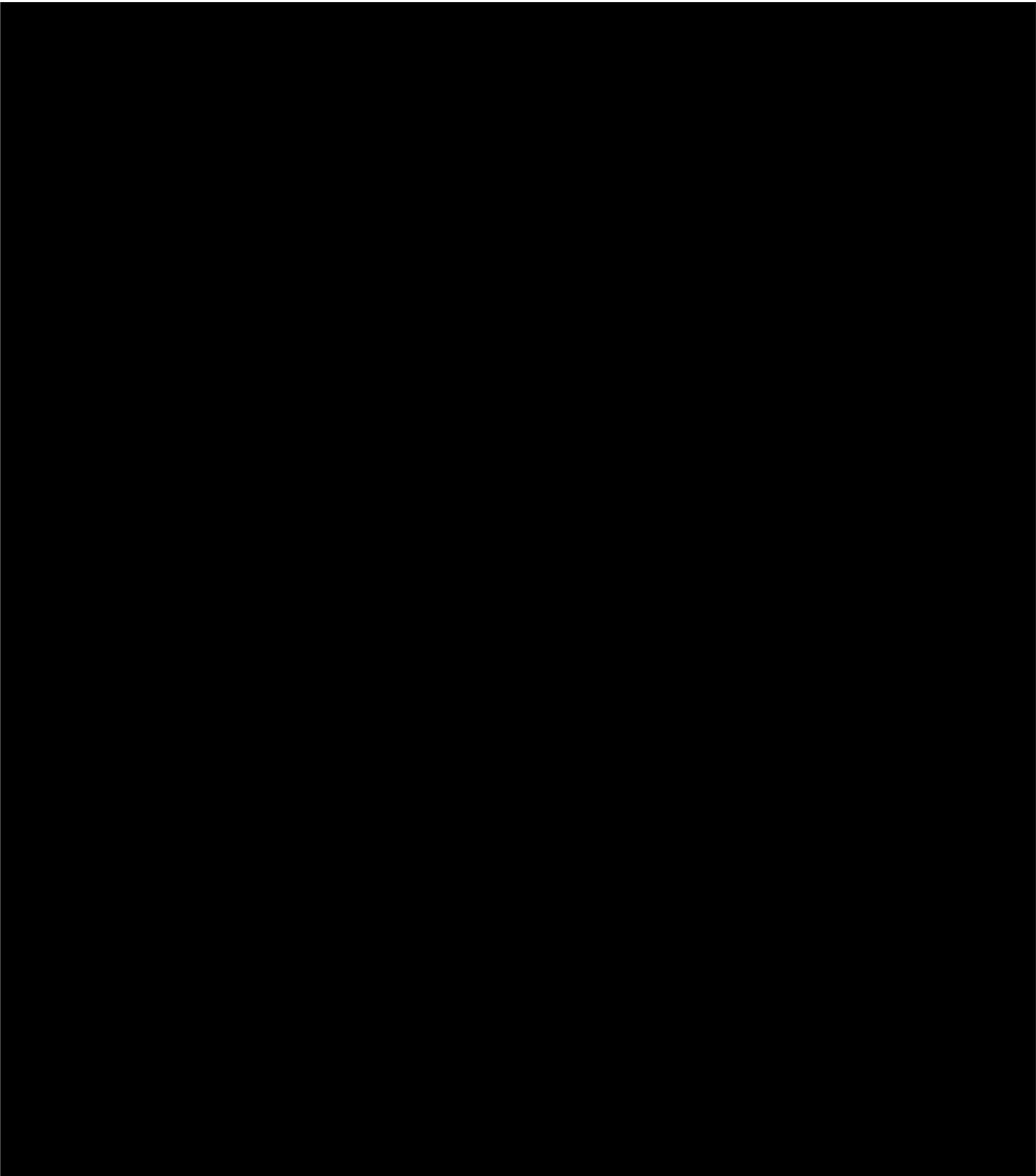


NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

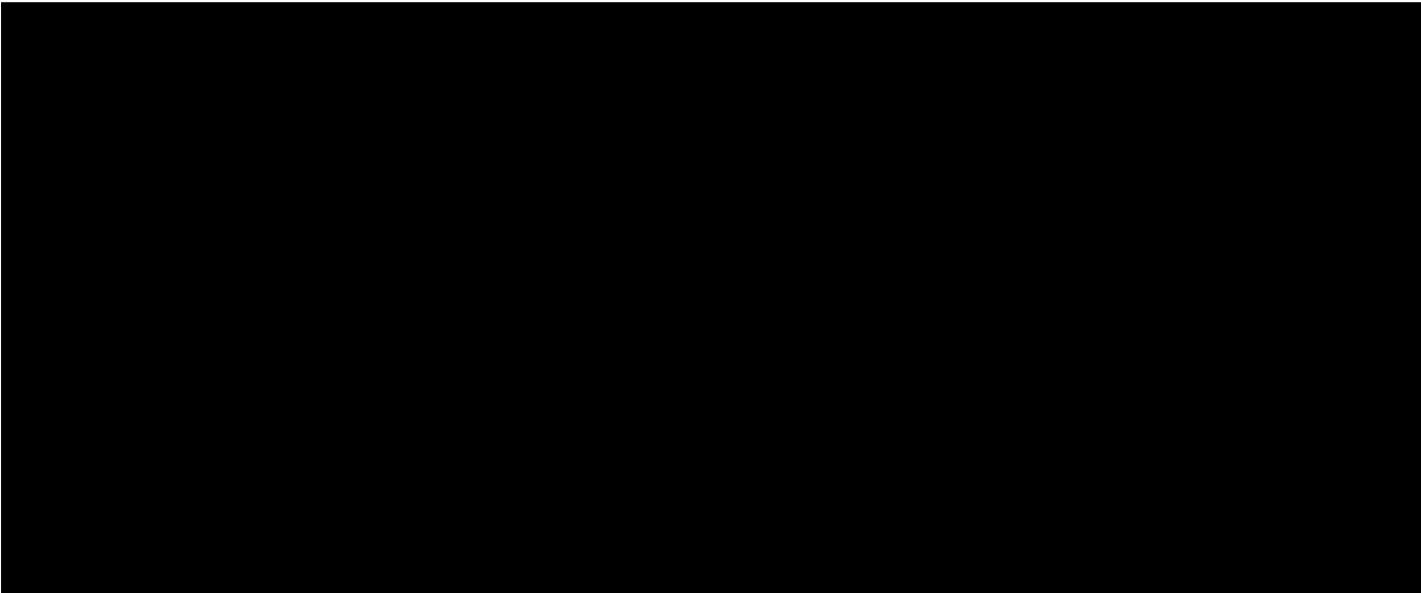


NaBISCOP
USCIS FDNS-HB 602-001



NaBISCOP
USCIS FDNS-HB 602-001

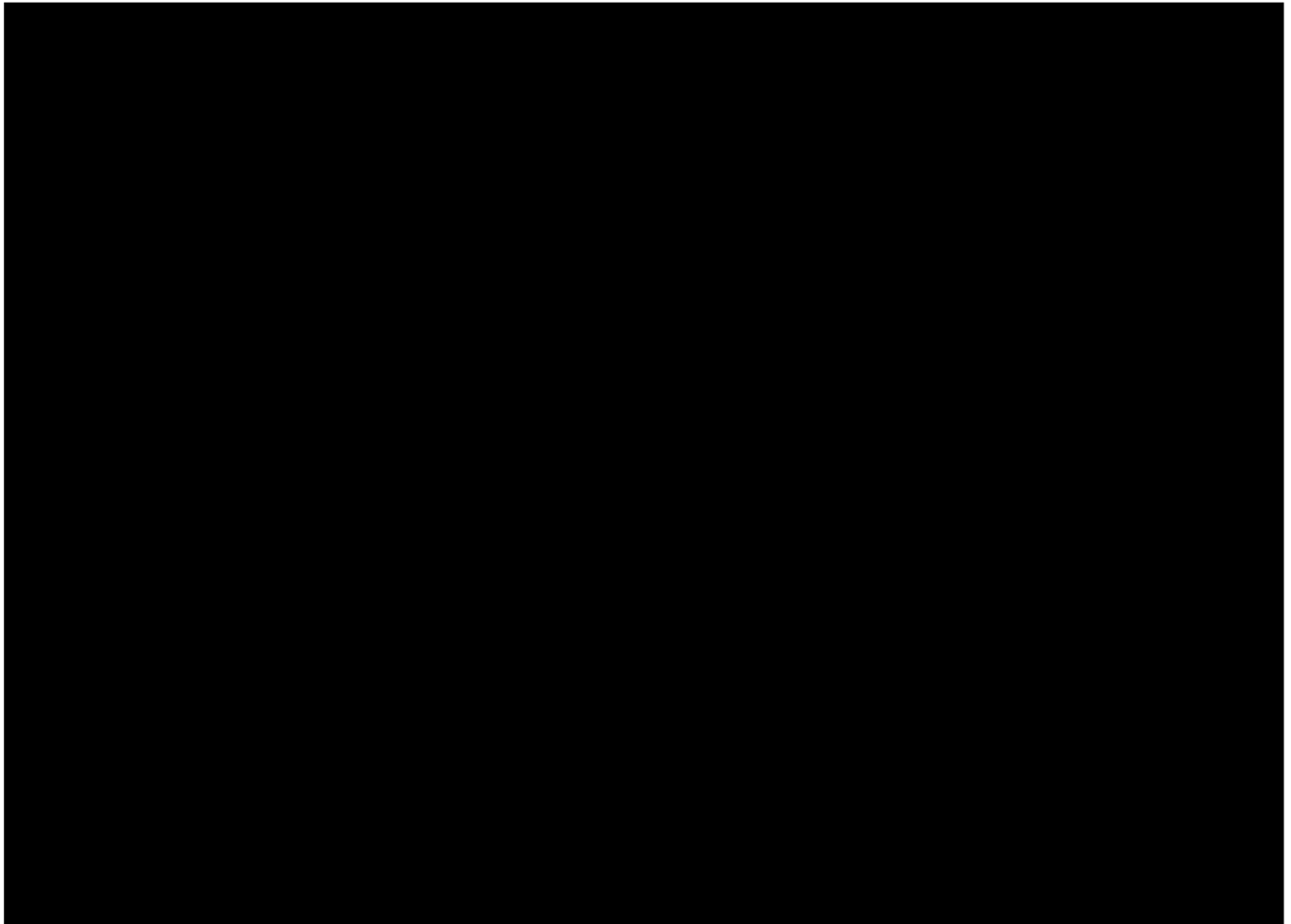
FOUO-LES



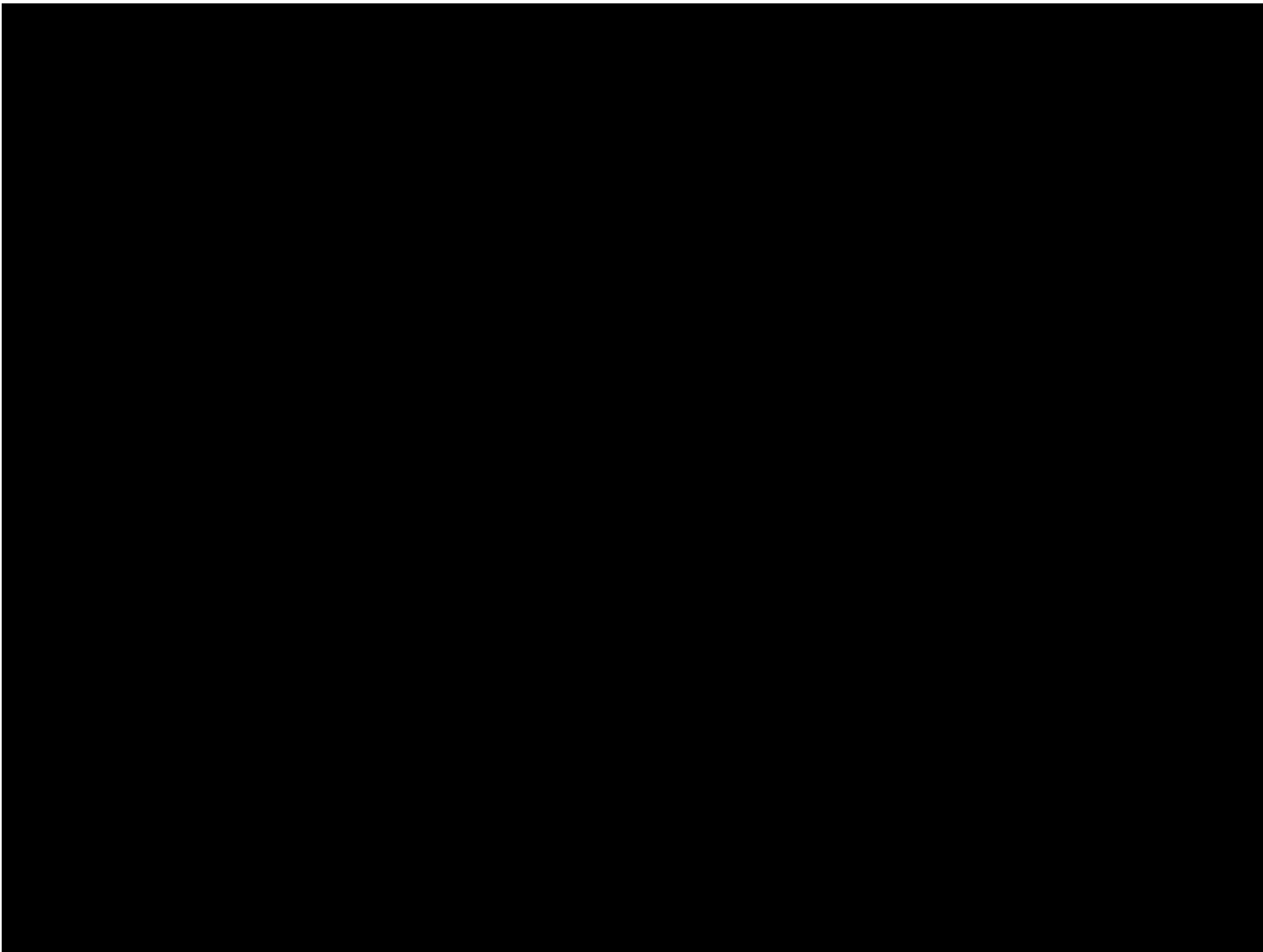
[Return to the Section Contents](#)

[Return to the Table of Contents](#)

K.



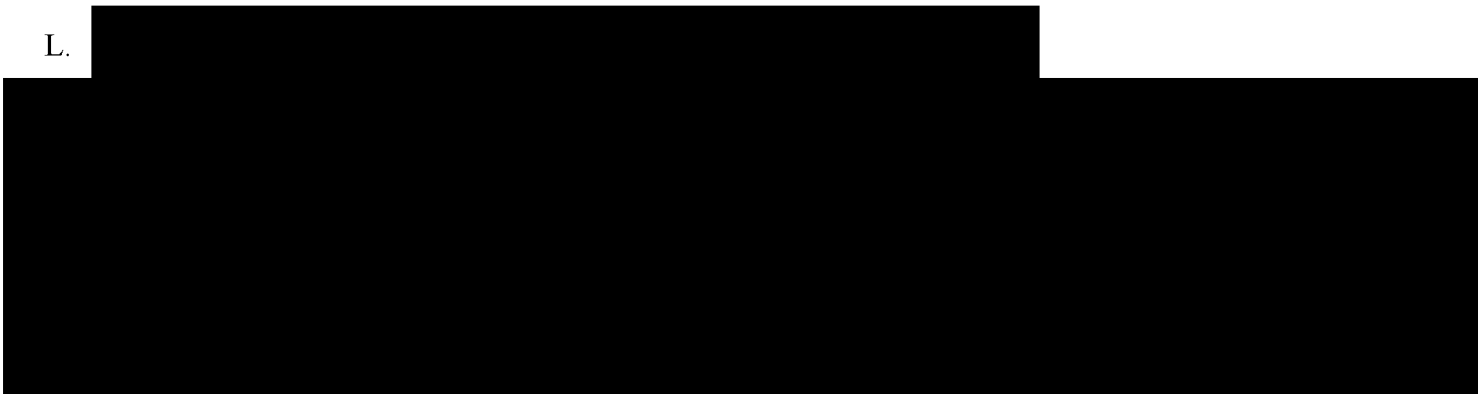
NaBISCOP
USCIS FDNS-HB 602-001



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

L.



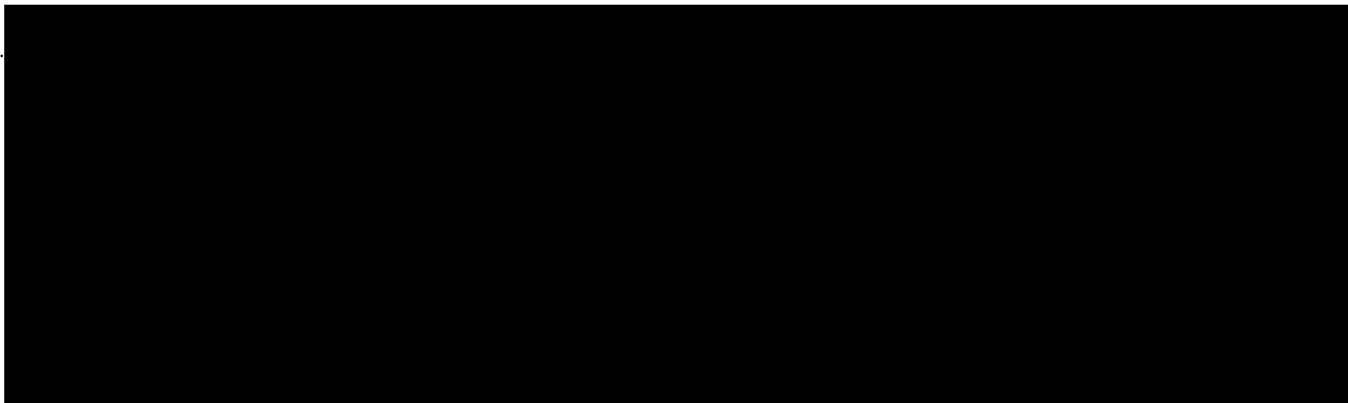
**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

M.



NaBISCOP
USCIS FDNS-HB 602-001

NaBISCOP
USCIS FDNS-HB 602-001

86

FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

87

FOUO-LES

5. *TECS Equipment and Technical Assistance*

Guidelines regarding TECS equipment and technical assistance include:

- 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 [REDACTED]
- 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.

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 (available in Appendix Q of this document:

[REDACTED] 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.

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:

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

NaBISCOP
USCIS FDNS-HB 602-001

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.

[Return to the Section Contents](#)
[Return to the Table of Contents](#)

N. [REDACTED]

[Return to the Section Contents](#)
[Return to the Table of Contents](#)

O. **Internal USCIS Policy Relating to TECS Queries**

- *“Issuance of Updated IBIS and USVISIT Procedures and Security Checklist,”* dated January 26, 2007, and signed by Joseph E. Langlois,

- *“IBIS Naming Conventions,”* dated December 30, 2005, and signed by Michael Aytes,
- *“Interagency Border Inspection System Processing Completed at the National Benefits Center,”* dated December 7, 2005, and signed by Michael Aytes,
- *“Accessing National Crime Information Center Interstate Identification Index (NCIC III) Data,”* dated June 3, 2005, and signed by William R. Yates and Joseph Cuddihy,

Attachment: *“IBIS NN16 User Agreement,”*

NaBISCOP
USCIS FDNS-HB 602-001

- “Revised Enhanced Processing Instructions,” dated April 5, 2005, and signed by William R. Yates, [REDACTED]
Attachment: “Enhanced Processing Instructions,”
[REDACTED]
- “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, [REDACTED]
- [REDACTED]
- “New Resolution Process for IBIS National Security/Terrorism-Related Positive Results,” dated November 29, 2004, and signed by William R. Yates,
[REDACTED]
- “New National Security-Related IBIS Procedures,” dated May 21, 2004, and signed by William R. Yates, [REDACTED]
- [REDACTED]
- “National Security Unit Case Closures,” dated February 19, 2004, and signed by William R. Yates, [REDACTED]
- “Interagency Border Inspection System Records Check Requirements,” dated January 20, 2004, and signed by William R. Yates,
[REDACTED]
- “Responsibilities of Adjudicators,” dated November 13, 2002, and signed by Johnny N. Williams, [REDACTED]

NaBISCOP
USCIS FDNS-HB 602-001

- “*Interagency Border Inspection System Records Check*,” dated July 2, 2002, and signed by Johnny N. Williams and Thomas Schiltgen,

- “*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,

- “*INS Policy on the Usage of the Interagency Border Inspection System*,” dated July 31, 2001, and signed by Michael D. Cronin,

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

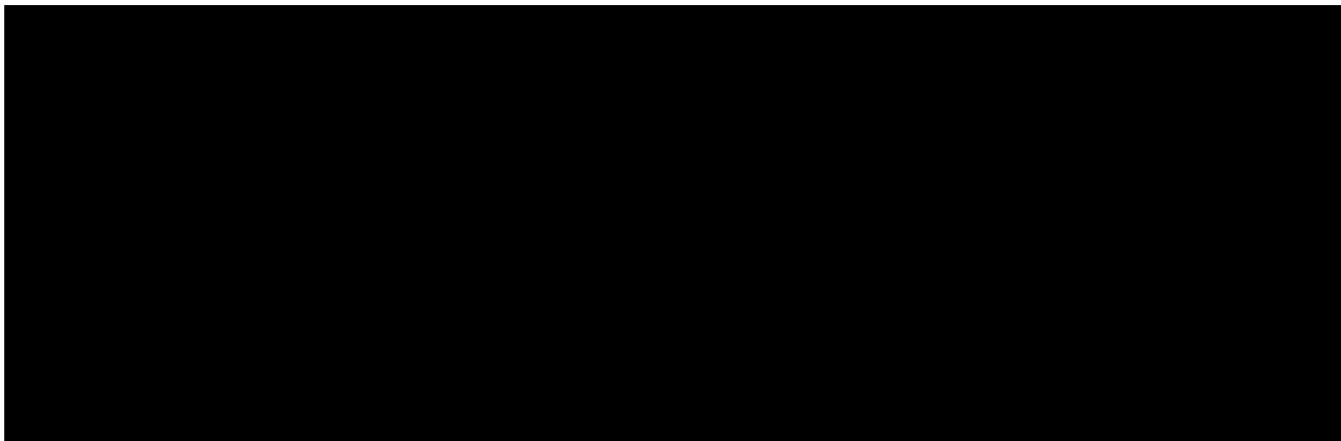
**NaBISCOP
USCIS FDNS-HB 602-001**

VI. Security Check: FBI Name Check

Section Contents

A.
B.
C.
D.

E.
F.
G.
H.



A.



NaBISCOP
USCIS FDNS-HB 602-001

Figure 9:



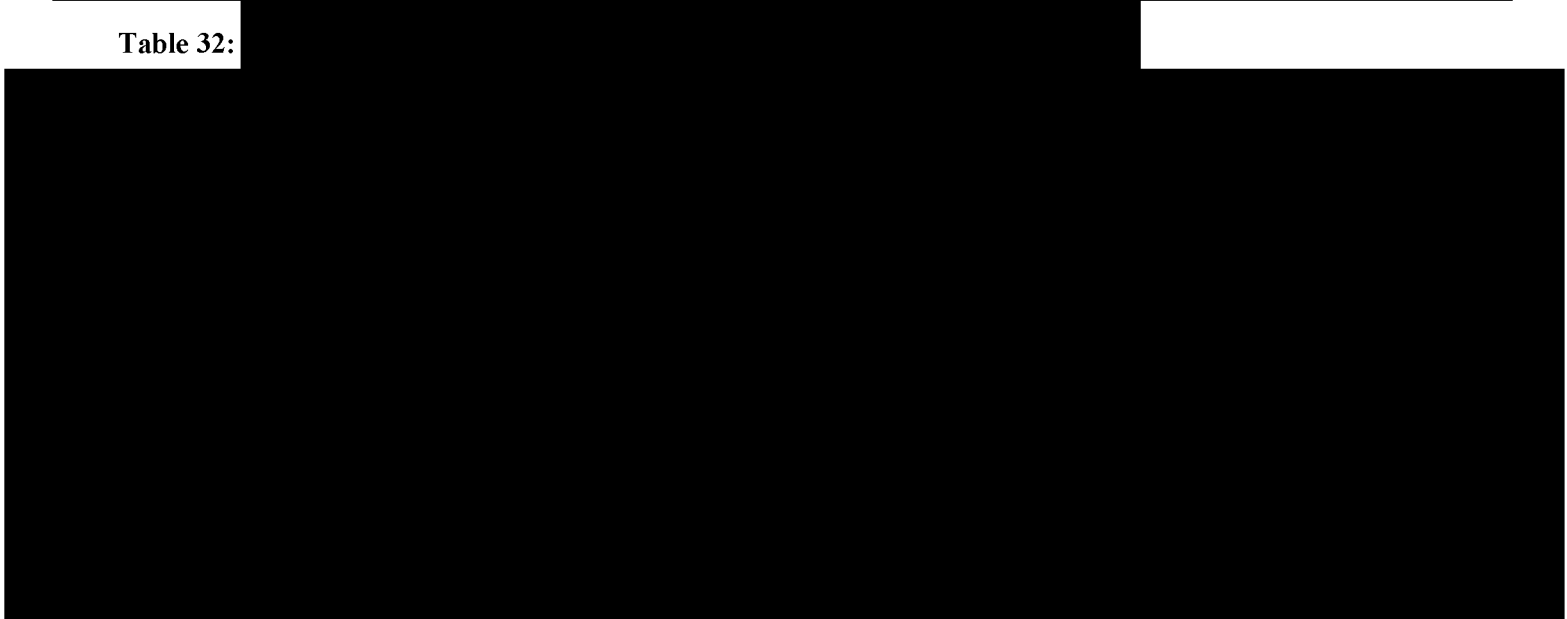
[Return to the Section Contents](#)

[Return to the Table of Contents](#)

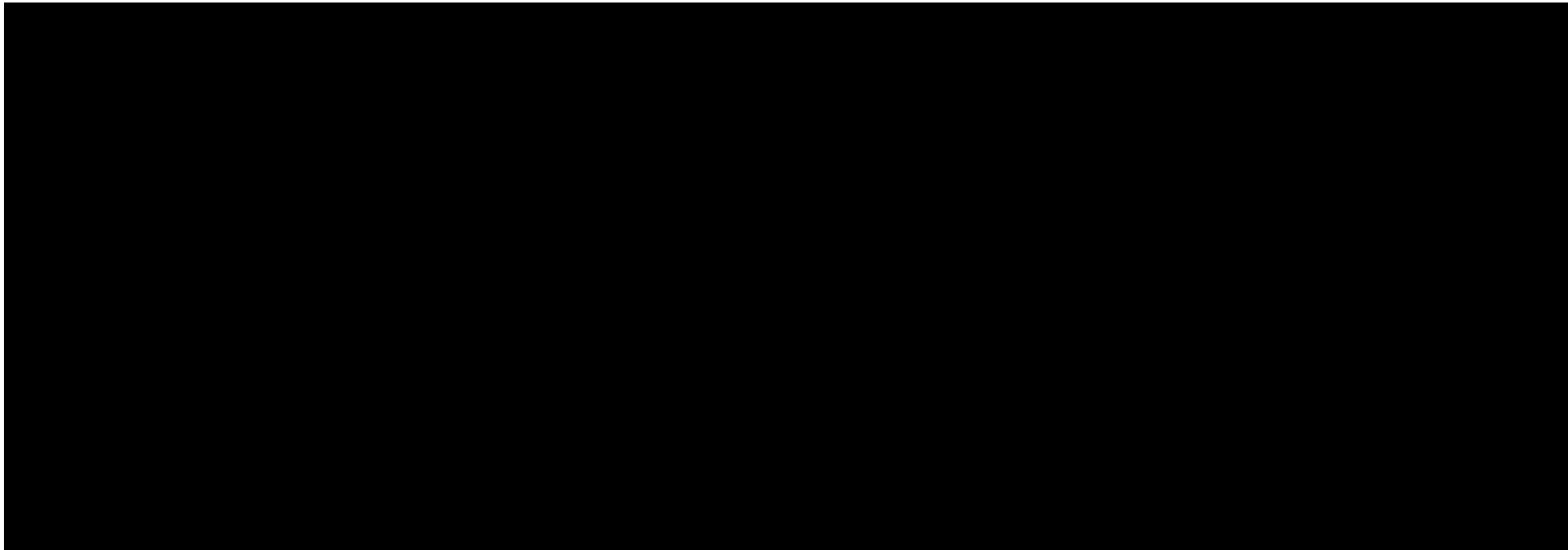
B.



Table 32:



**NaBISCOP
USCIS FDNS-HB 602-001**



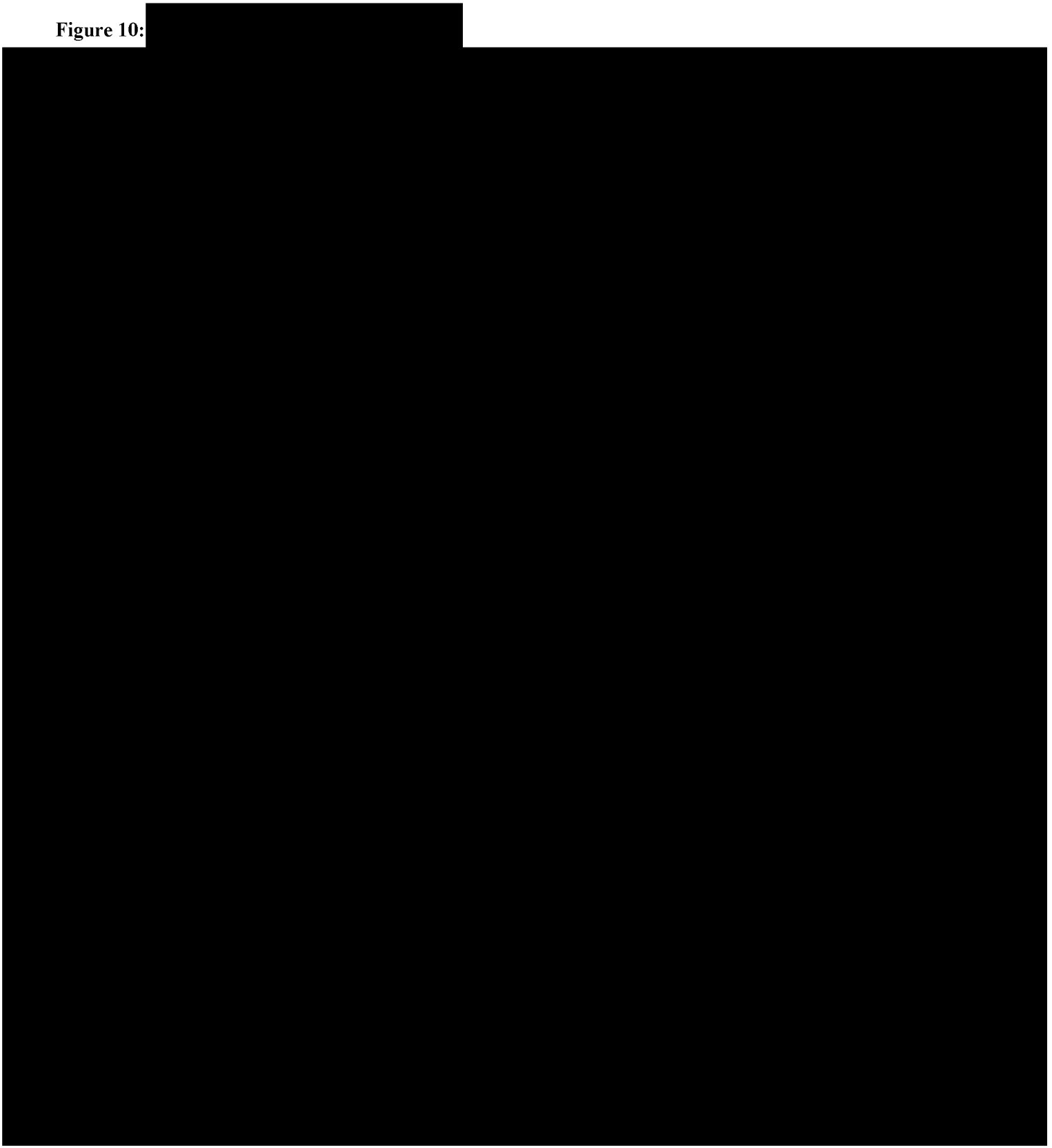
[Return to the Section Contents](#)
[Return to the Table of Contents](#)

C.



NaBISCOP
USCIS FDNS-HB 602-001

Figure 10:



**NaBISCOP
USCIS FDNS-HB 602-001**

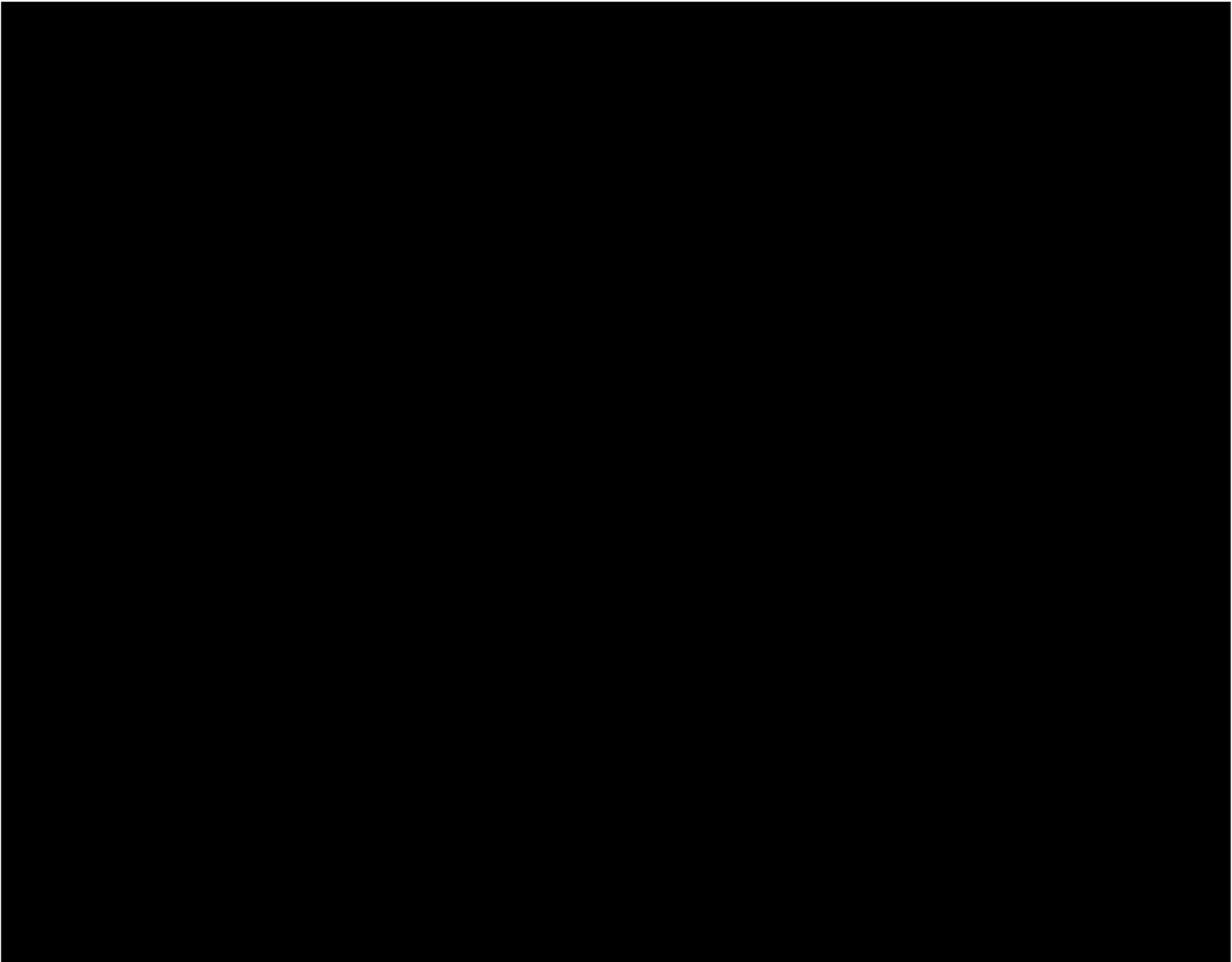
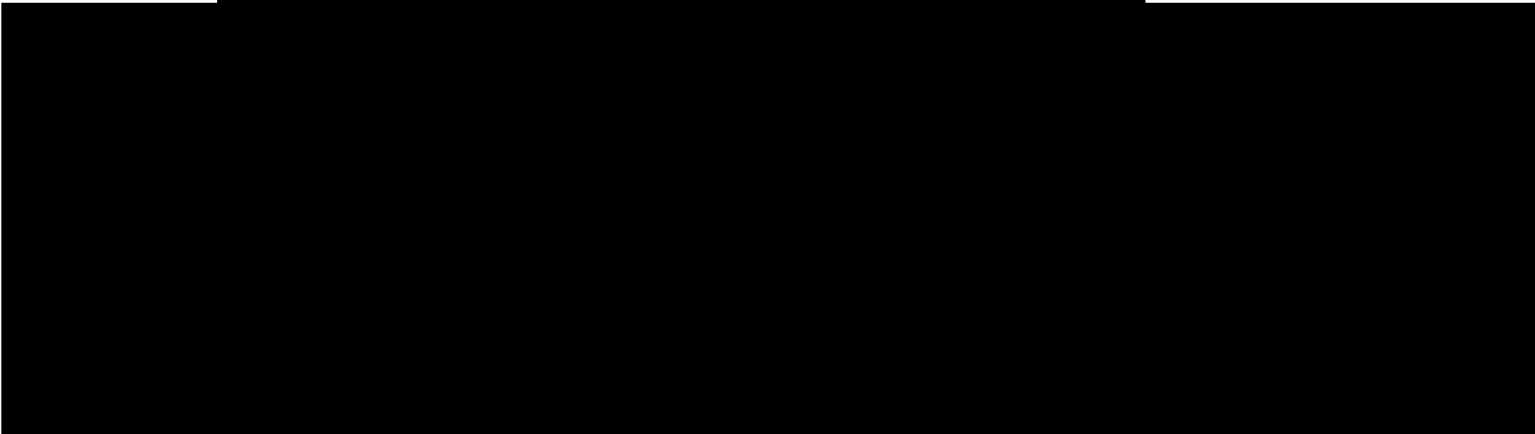
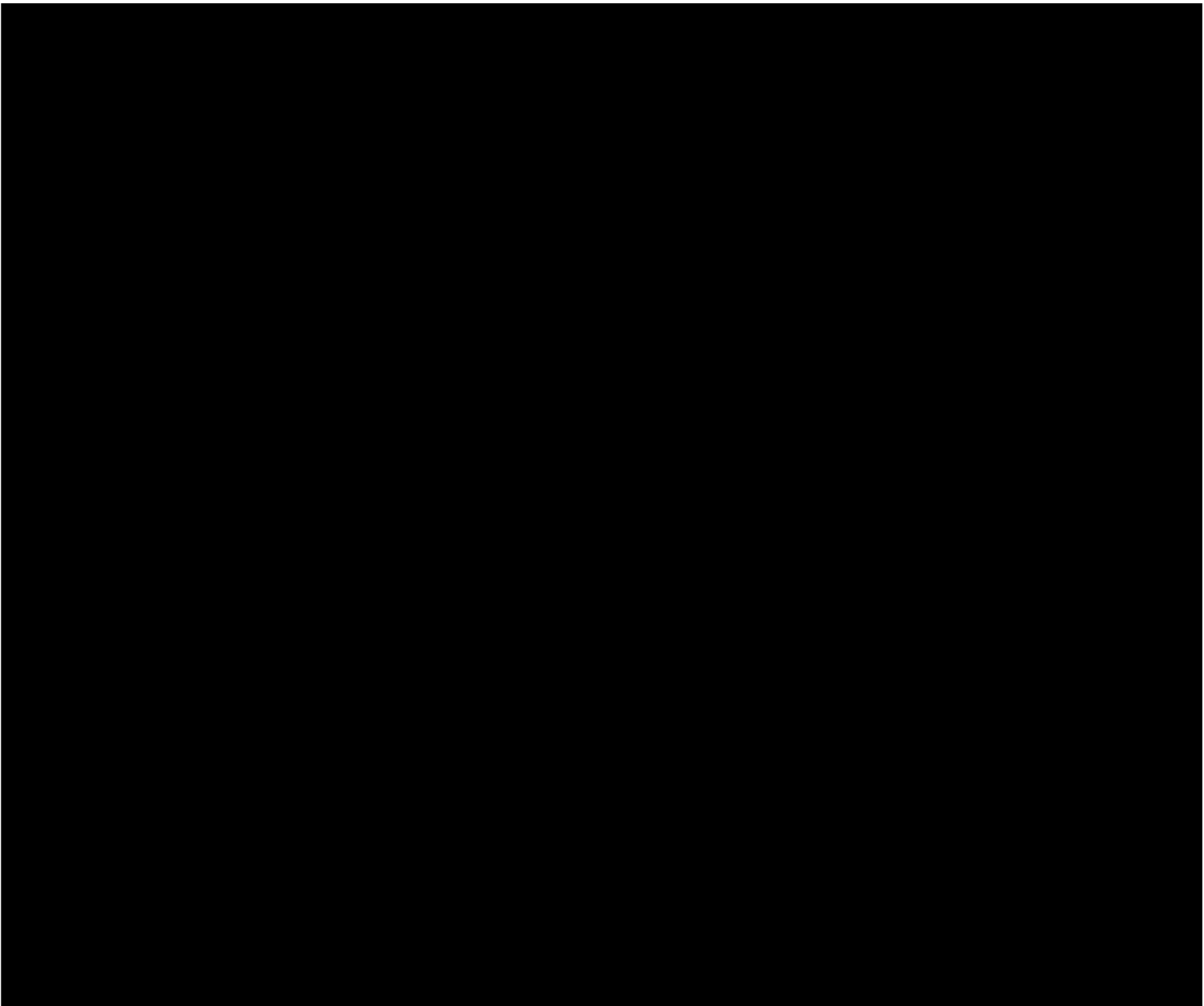


Table 33:



**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)
[Return to the Table of Contents](#)

D.

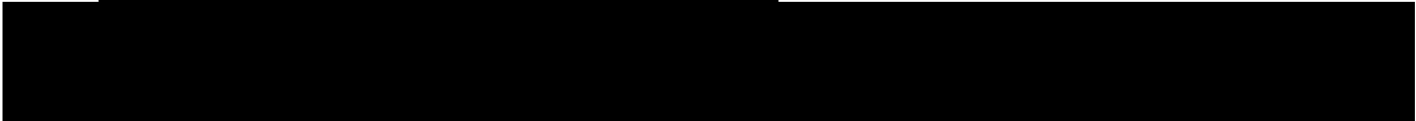
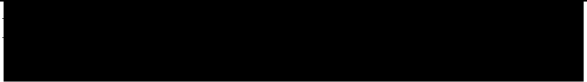


Figure 11:



NaBISCOP
USCIS FDNS-HB 602-001

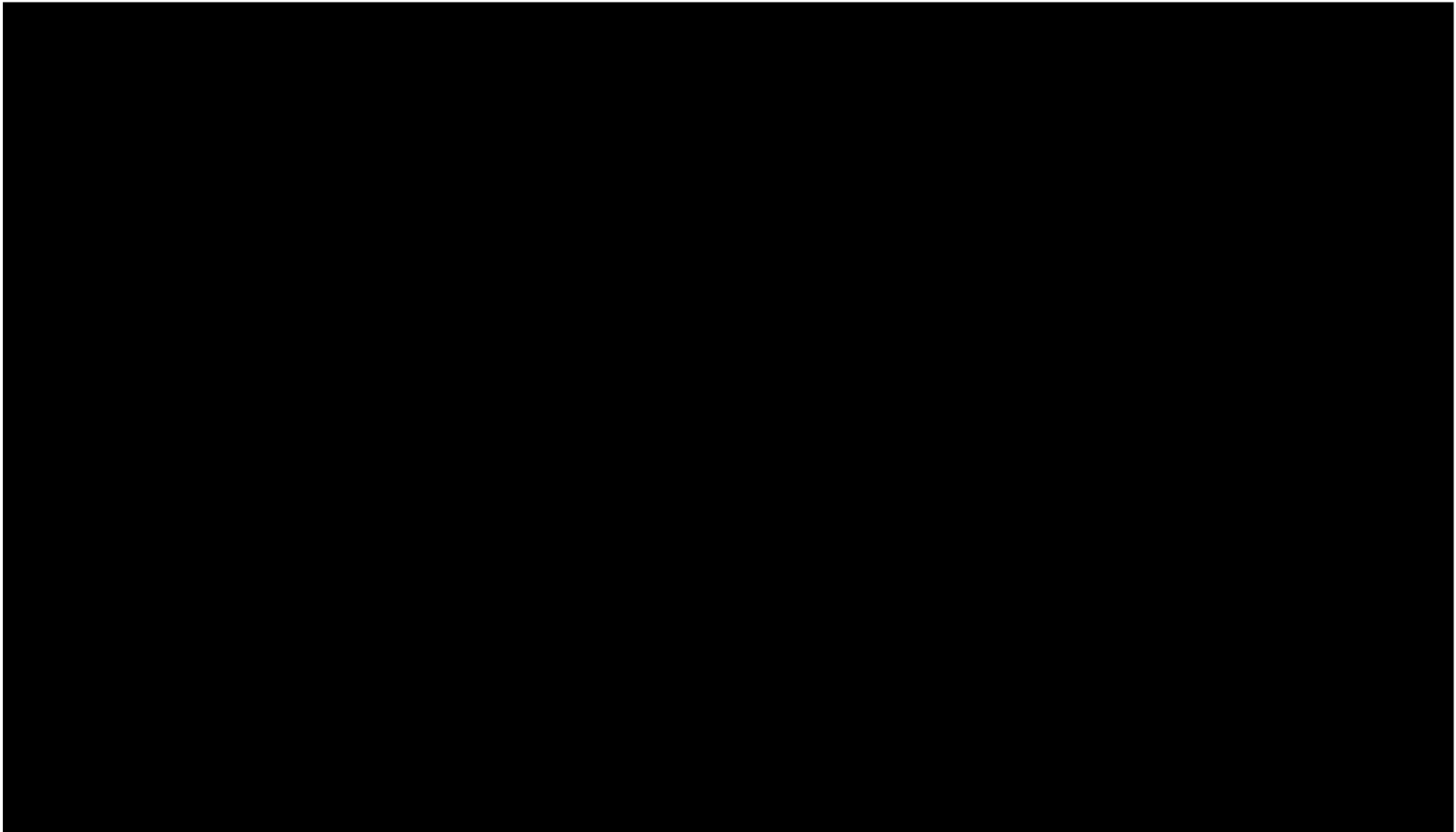
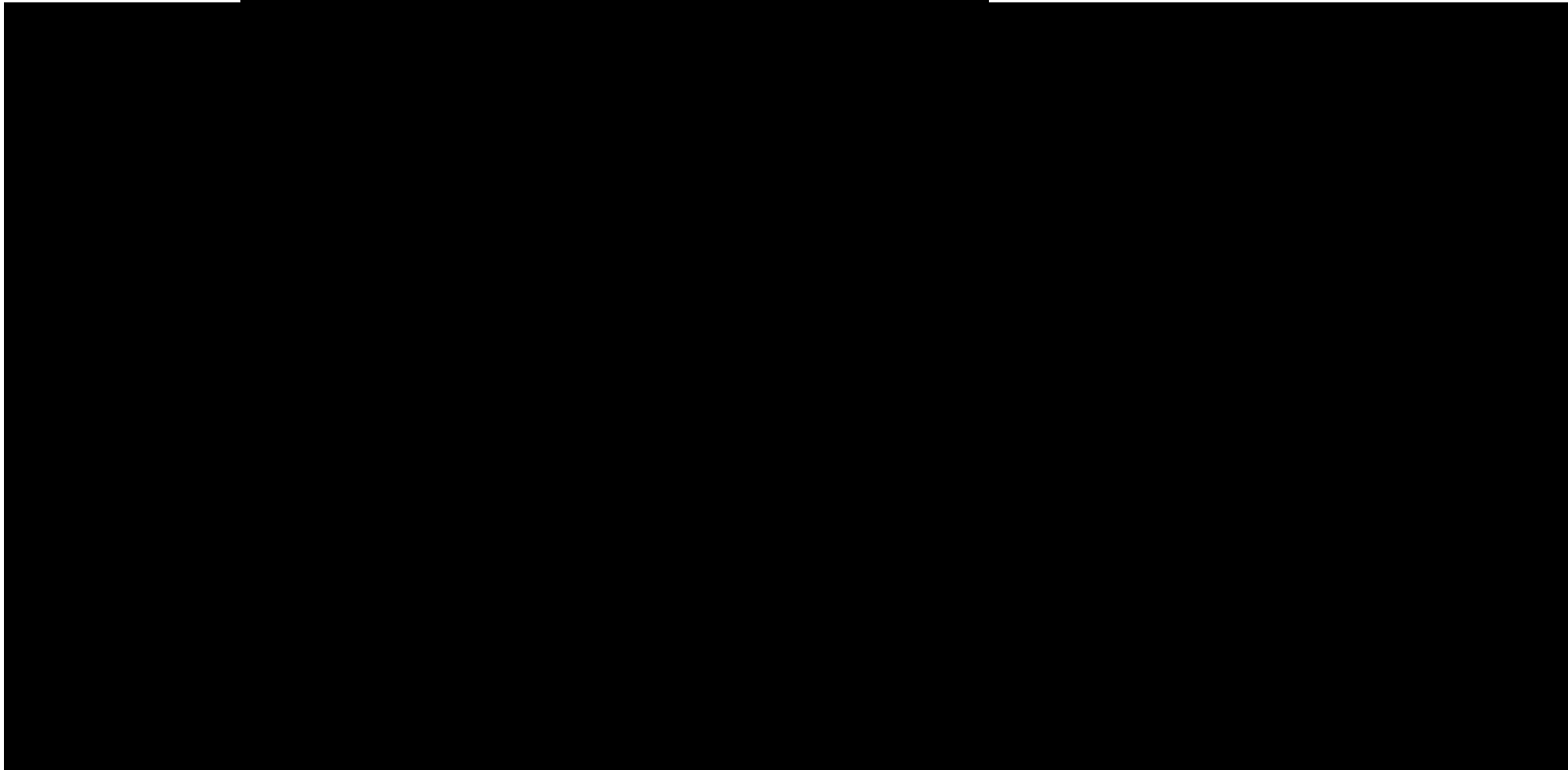
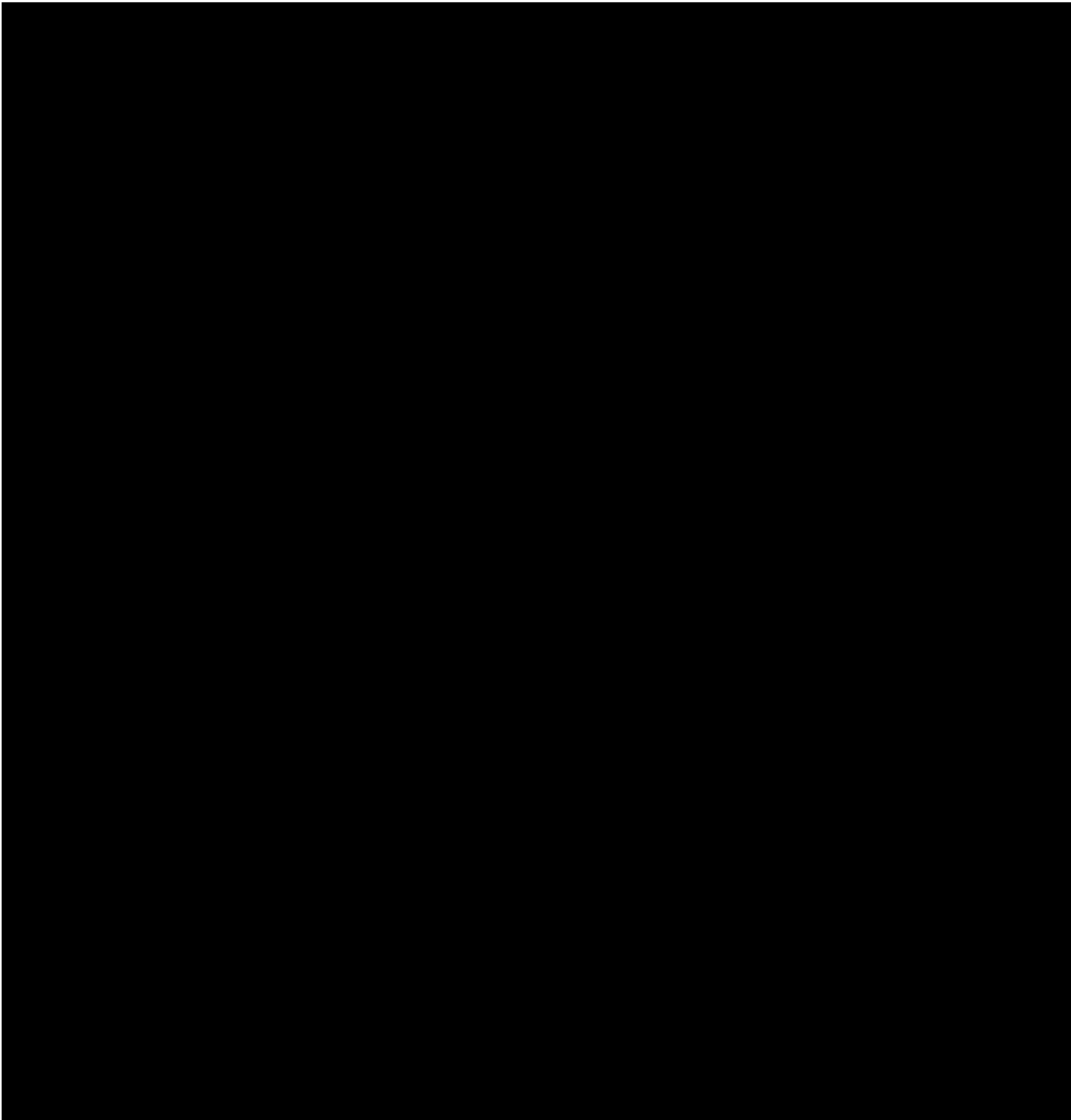


Table 34:



**NaBISCOP
USCIS FDNS-HB 602-001**



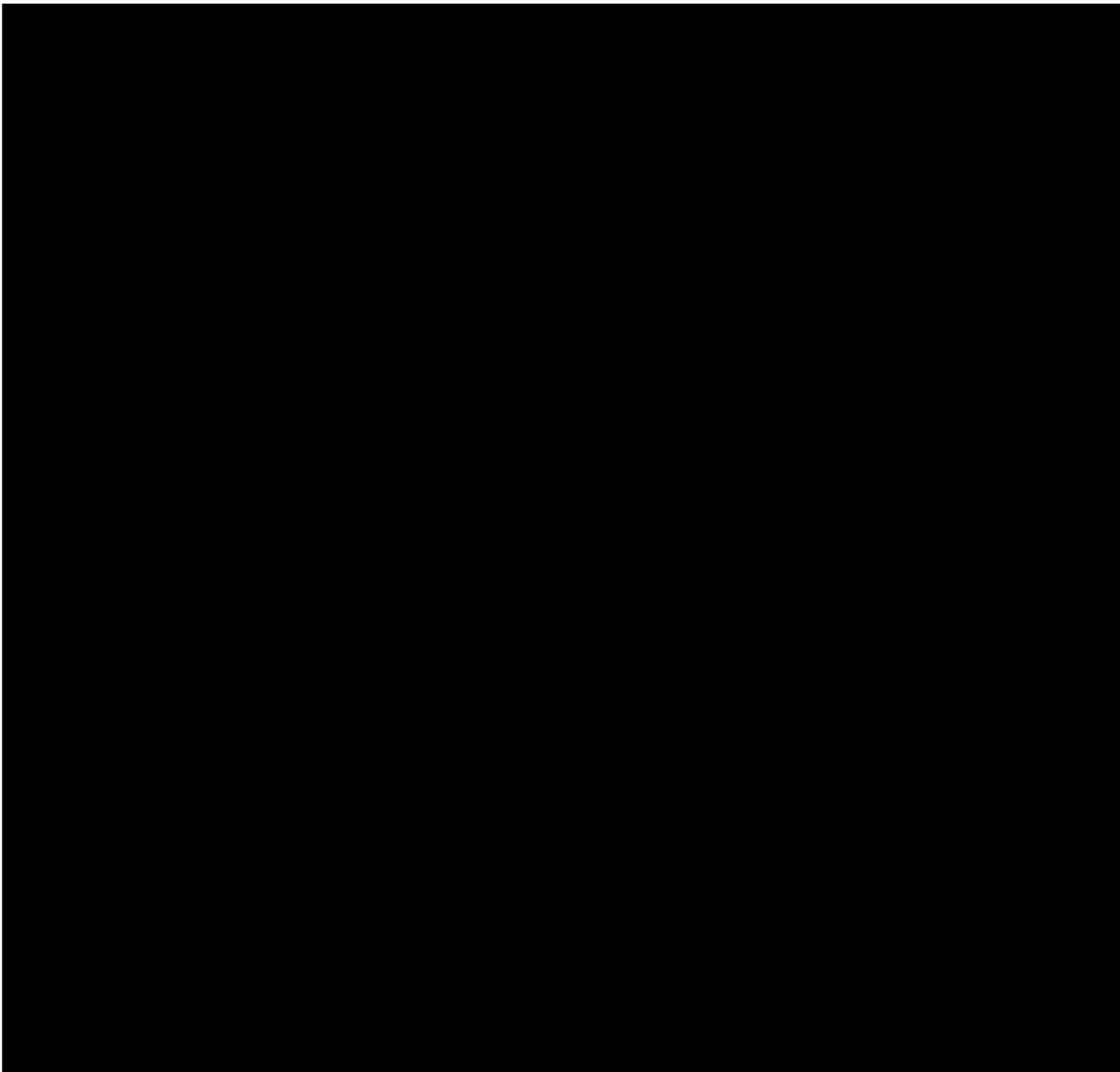
NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

NaBISCOP
USCIS FDNS-HB 602-001

100

FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

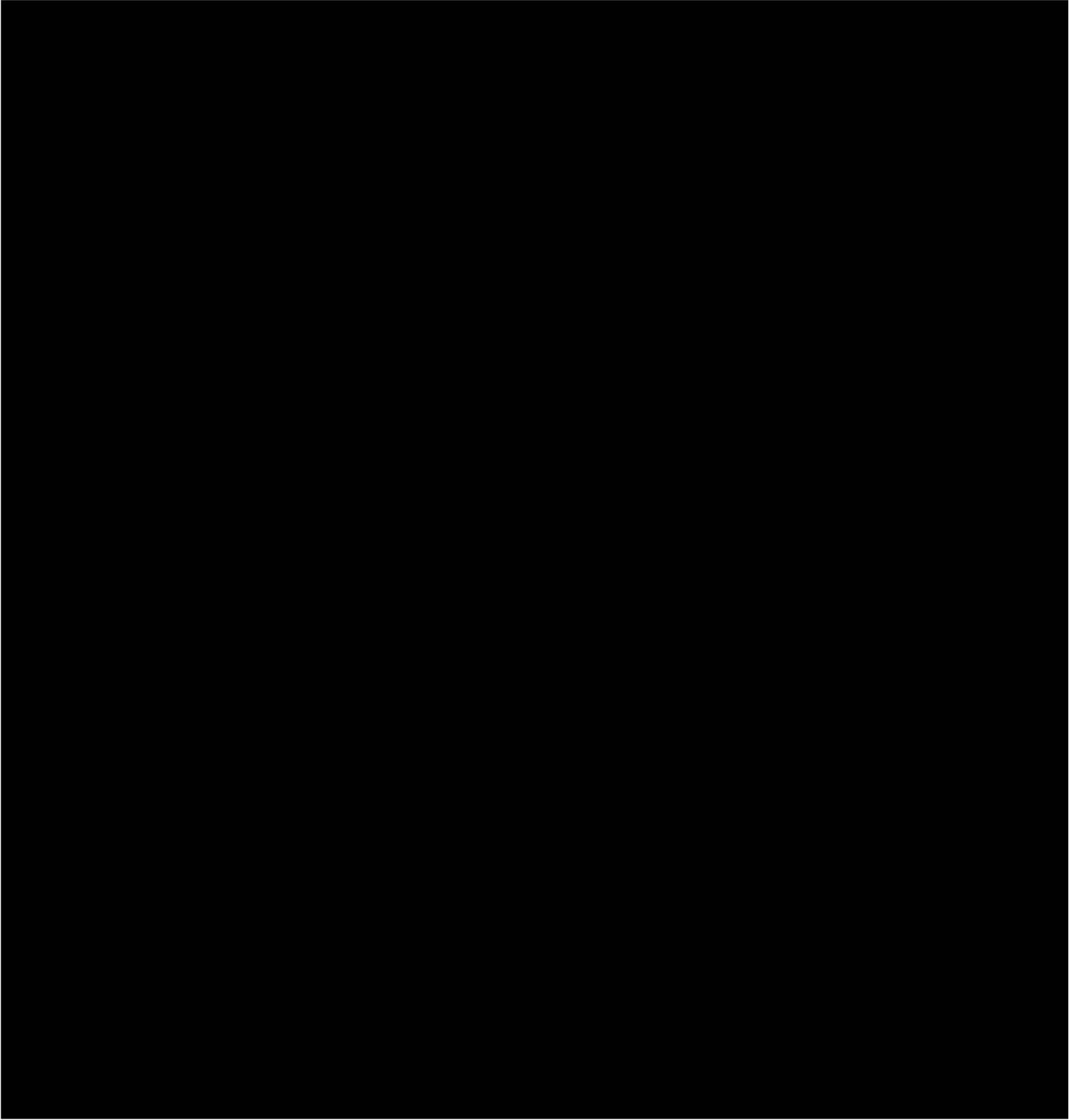
Figure 12:



Table 35:

A large black rectangular redaction box covers the entire content area of Table 35, obscuring any data or text that might have been present.

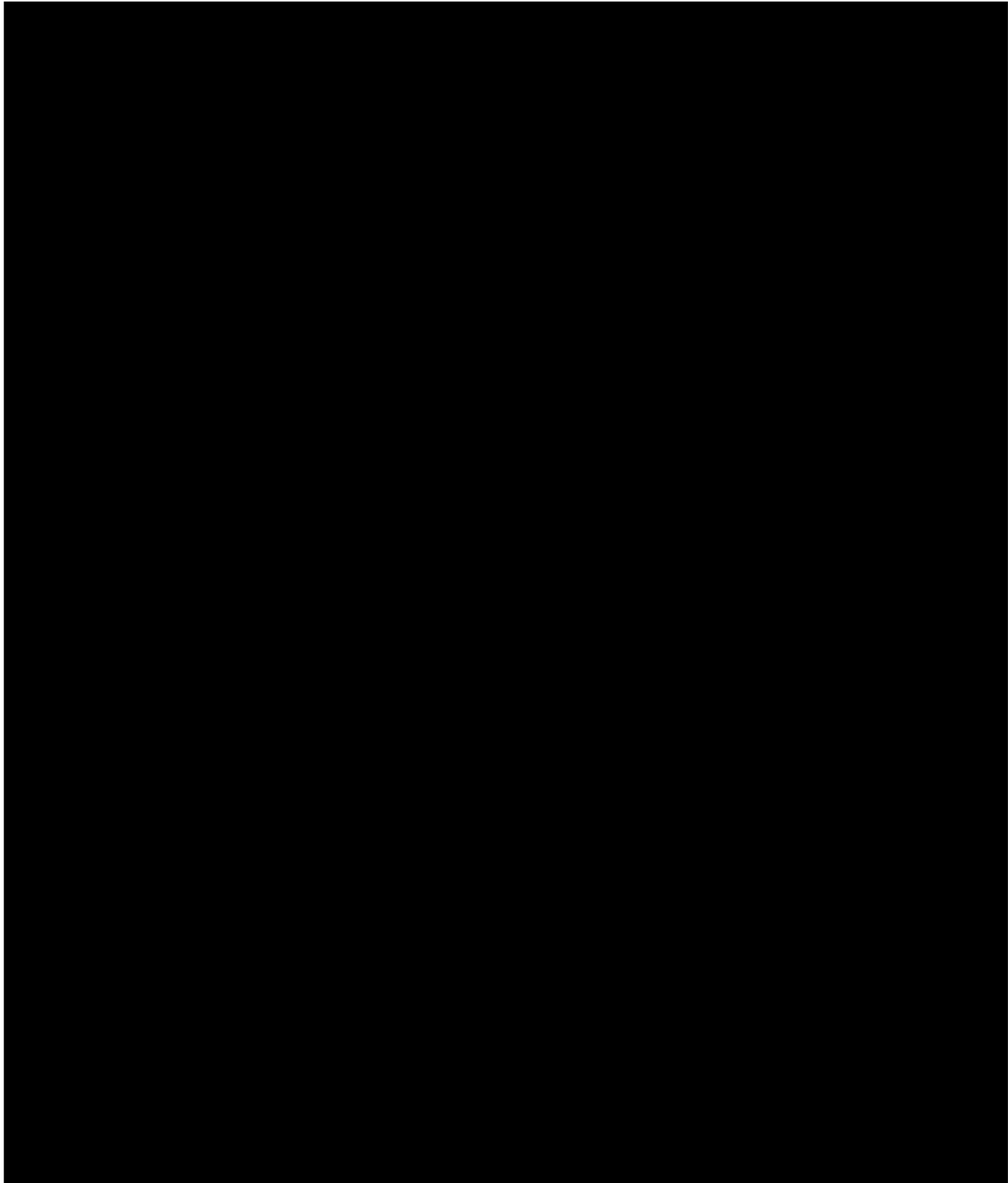
**NaBISCOP
USCIS FDNS-HB 602-001**



NaBISCOP
USCIS FDNS-HB 602-001

103

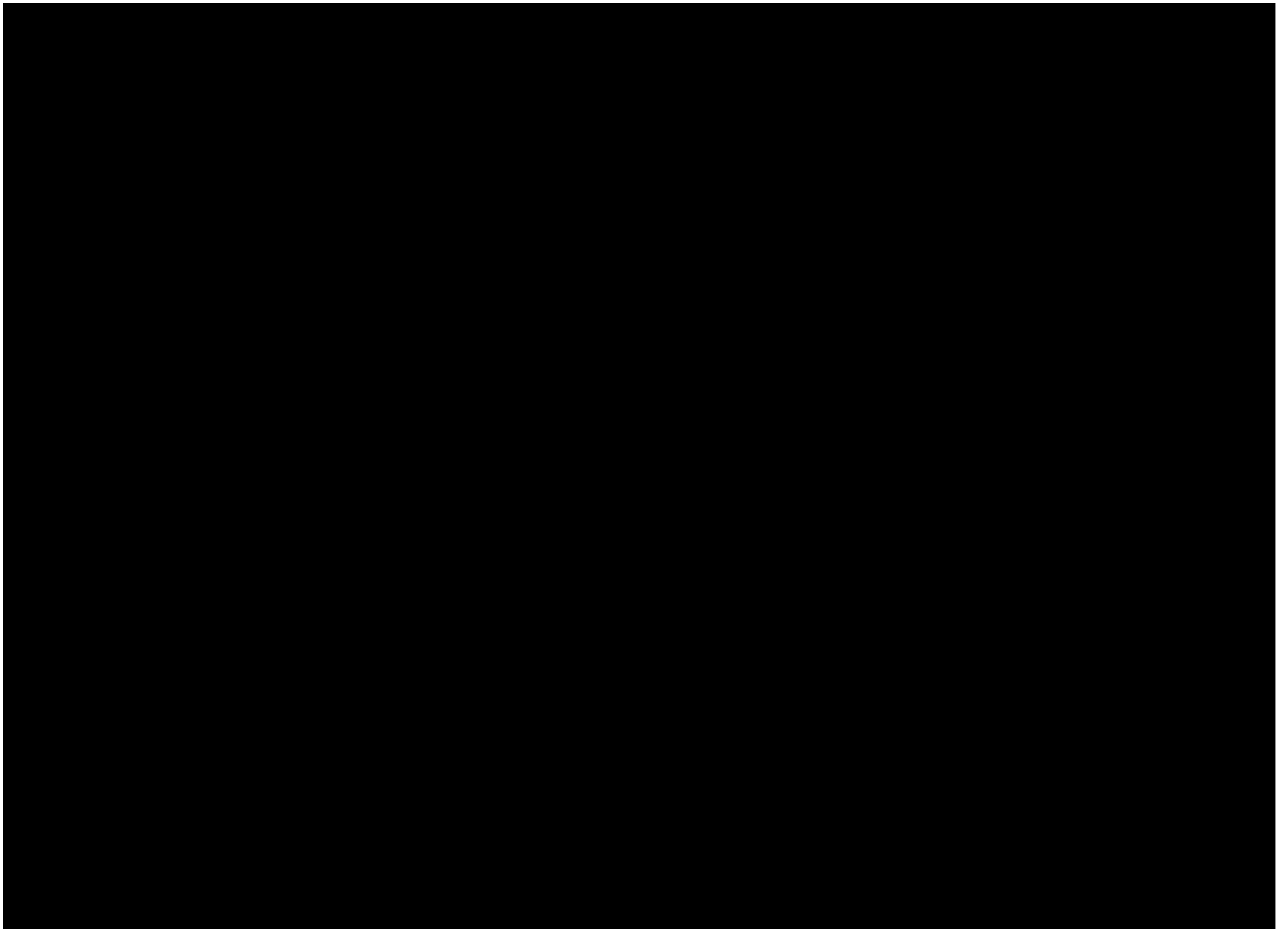
FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

104

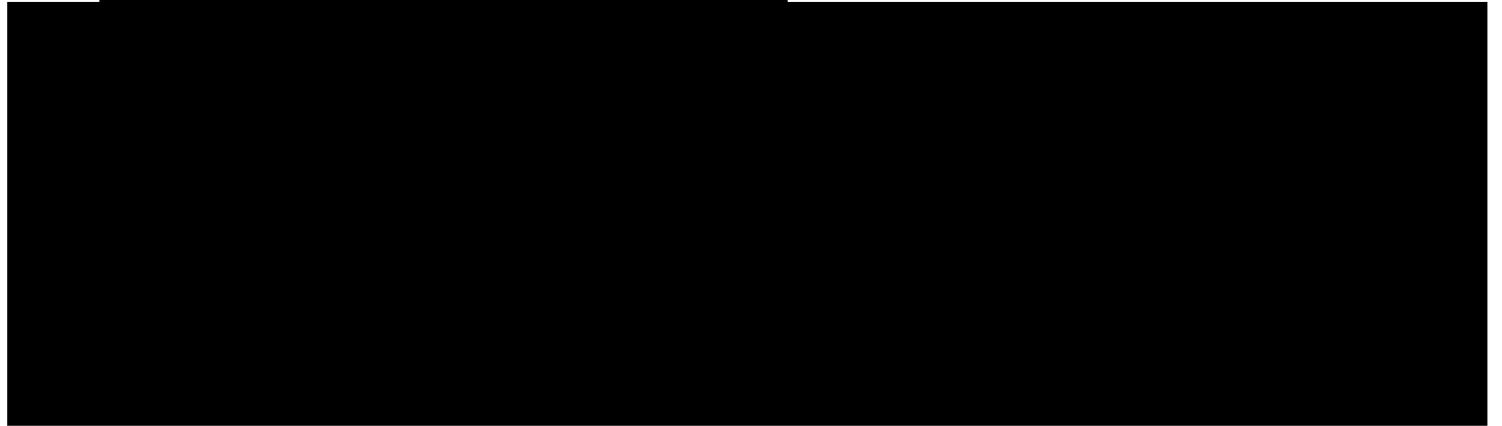
FOUO-LES



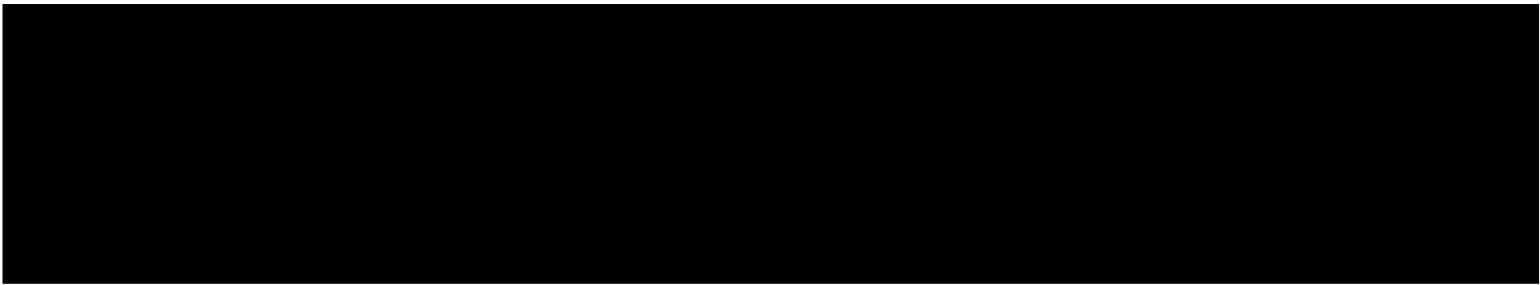
[Return to the Section Contents](#)

[Return to the Table of Contents](#)

E.



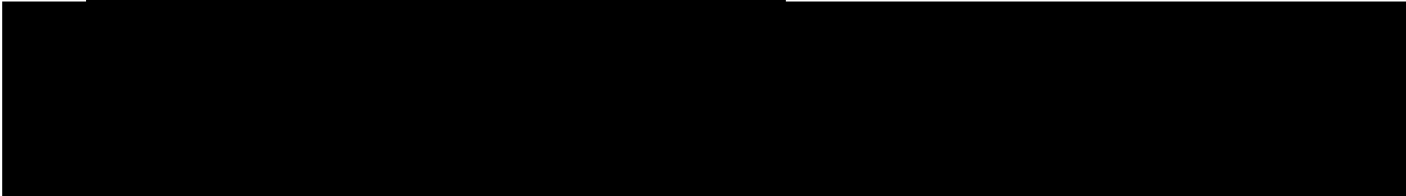
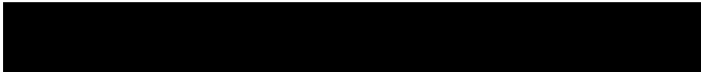
NaBISCOP
USCIS FDNS-HB 602-001



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

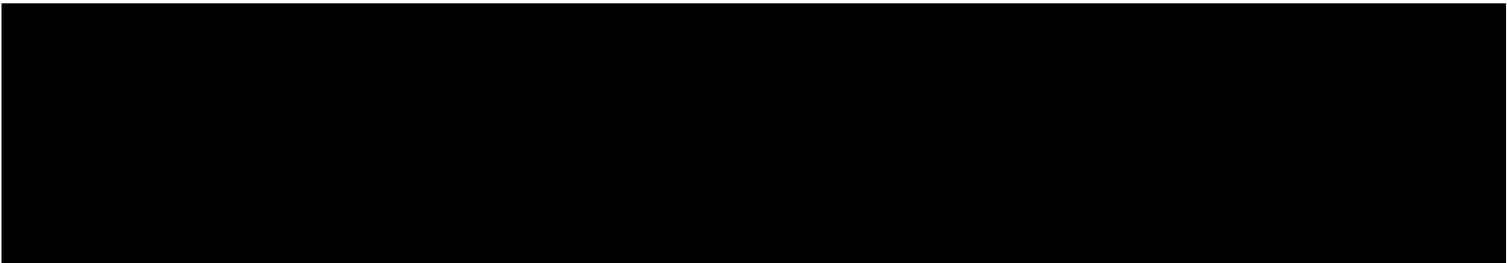
F.



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

G.



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

H.



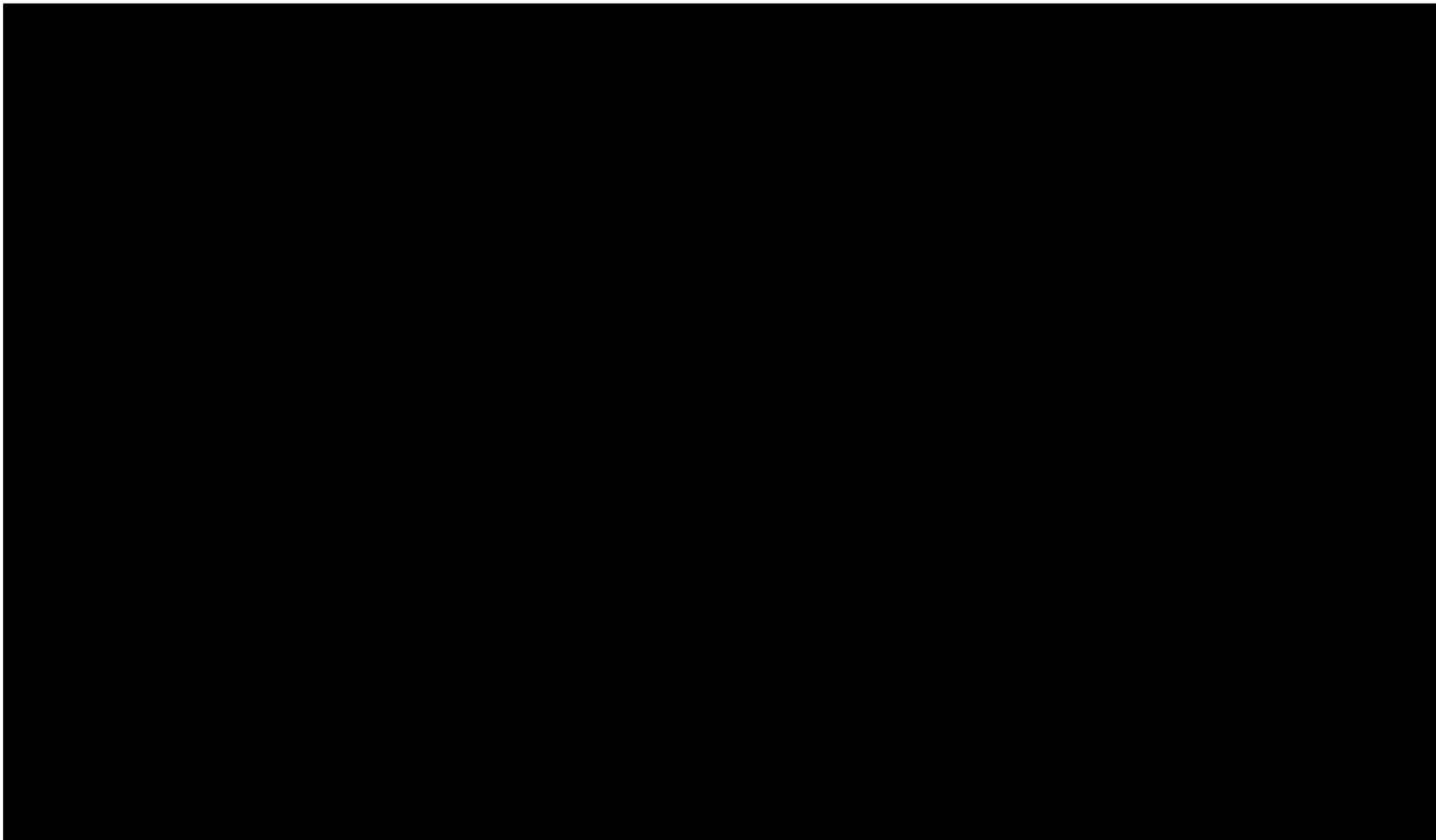
- “*National Security Adjudication and Reporting Requirements Update*,” dated February 9, 2009, and signed by Donald Neufeld,



- “*Revised National Security Adjudication and Reporting Requirements*,” dated February 4, 2008, and signed by Michael Aytes,



**NaBISCOP
USCIS FDNS-HB 602-001**



- Johnny Williams memorandum entitled “*Enhanced Processing Instructions*,” dated March, 18, 2002, [REDACTED] and William Yates memorandum entitled “*Revised Enhanced Processing Instructions*,” dated April 5, 2005, [REDACTED]

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

VII. Security Check: FBI Fingerprint Check

Section Contents

- A. FBI Fingerprint Check
- B. Who Requires FBI Fingerprint Checks

- C.
- D.
- E.
- F.
- G.
- H.
- I.

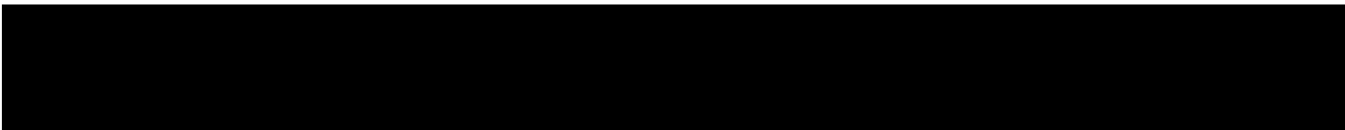


A. FBI Fingerprint Check

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 Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS is a national fingerprint and criminal history system maintained by the FBI's CJIS Division.

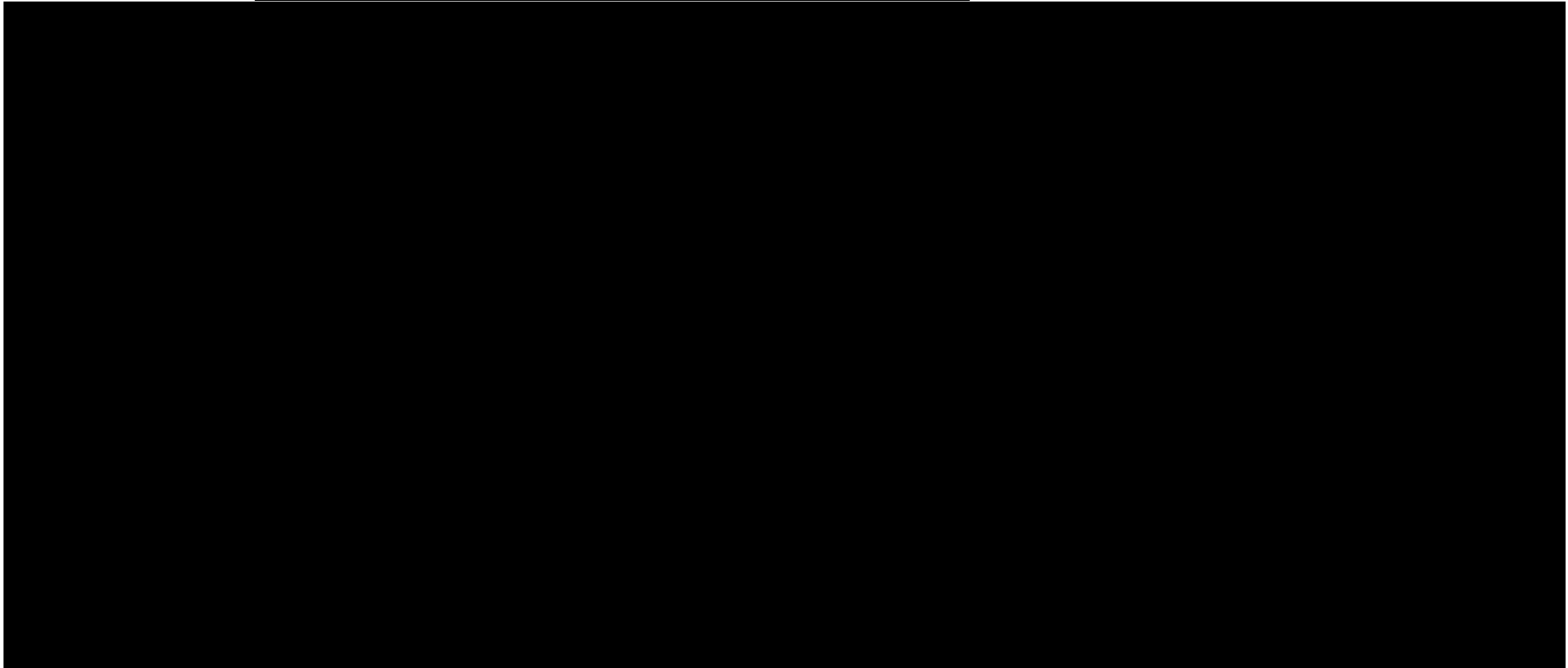
State, local, and federal law enforcement agencies submit fingerprints and corresponding administrative or criminal history information to the IAFIS. Participation by state and local agencies is not mandatory, so the FBI Fingerprint check does not contain records from every jurisdiction. The information 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.

The application support center (ASC) captures fingerprints for required individuals that come into the ASC for that purpose.⁹ This data is transmitted daily to the FBI's database. This query submits fingerprints, without any names associated with the prints. Results of this query are all the names of individuals that match the prints in the FBI's system. These results are loaded into FD-258.



**NaBISCOP
USCIS FDNS-HB 602-001**

Figure 13:



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

B.

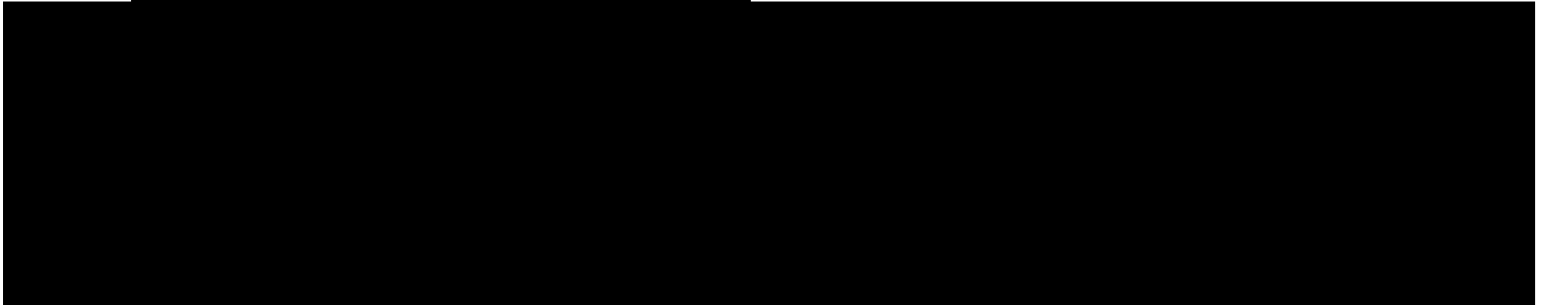
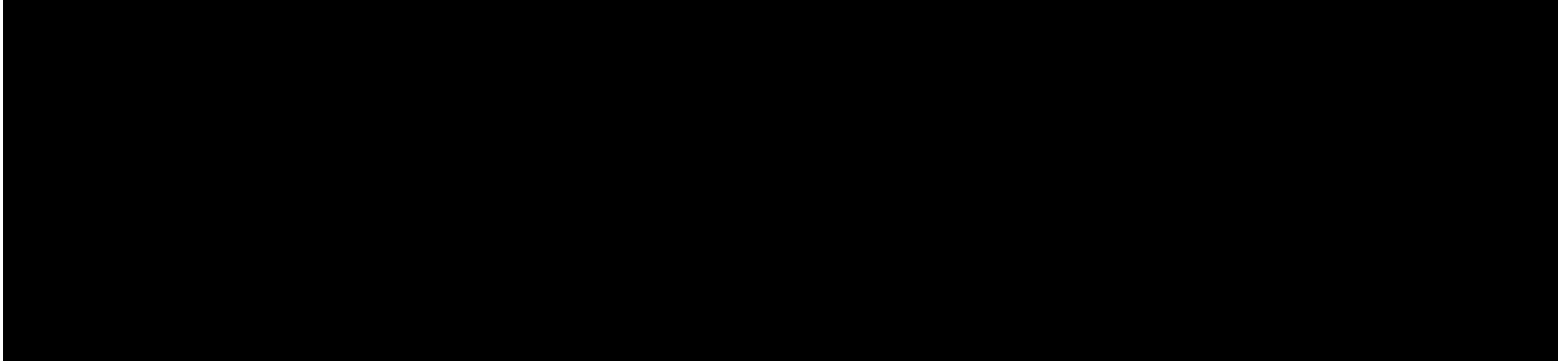
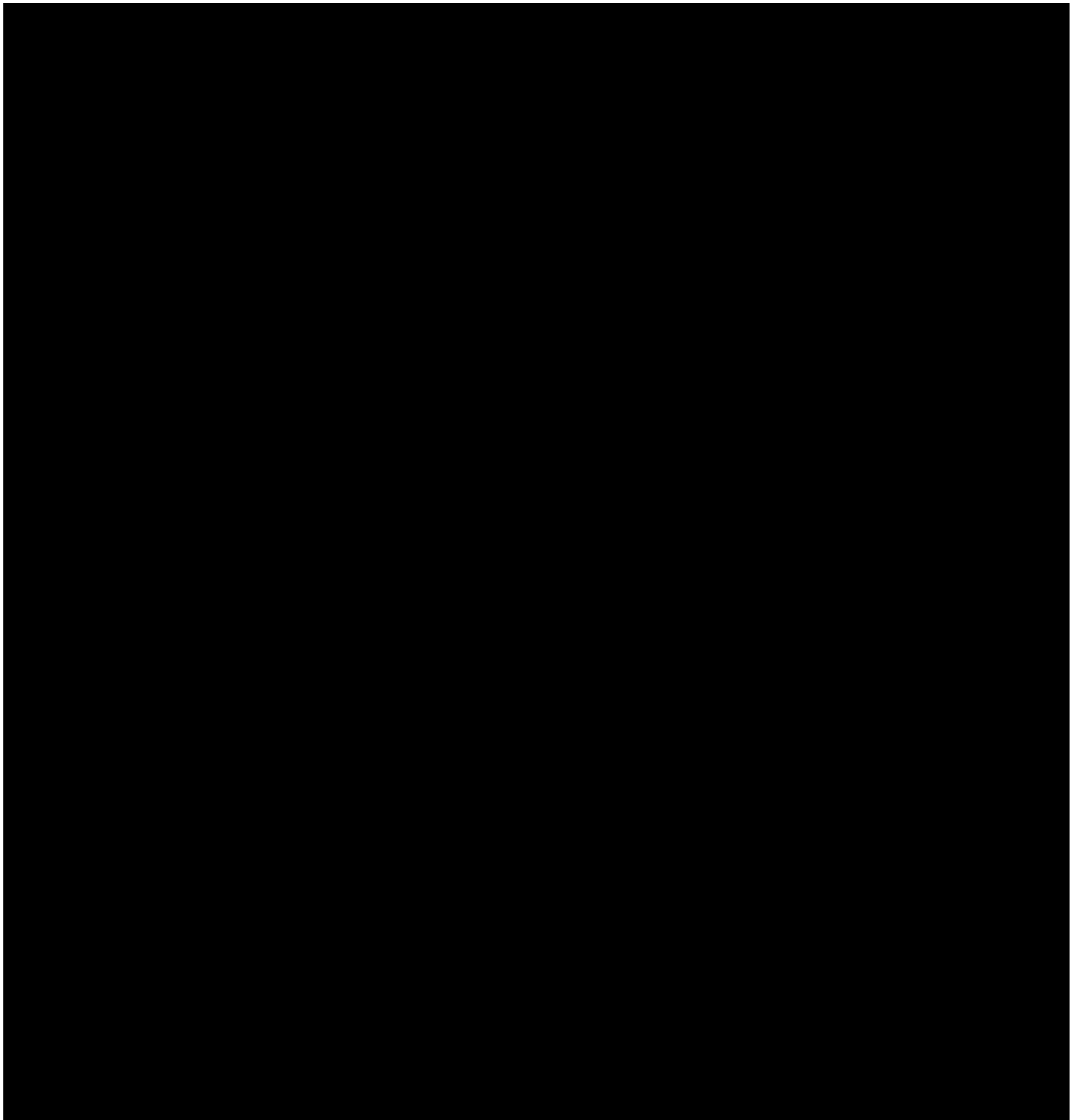


Table 36:

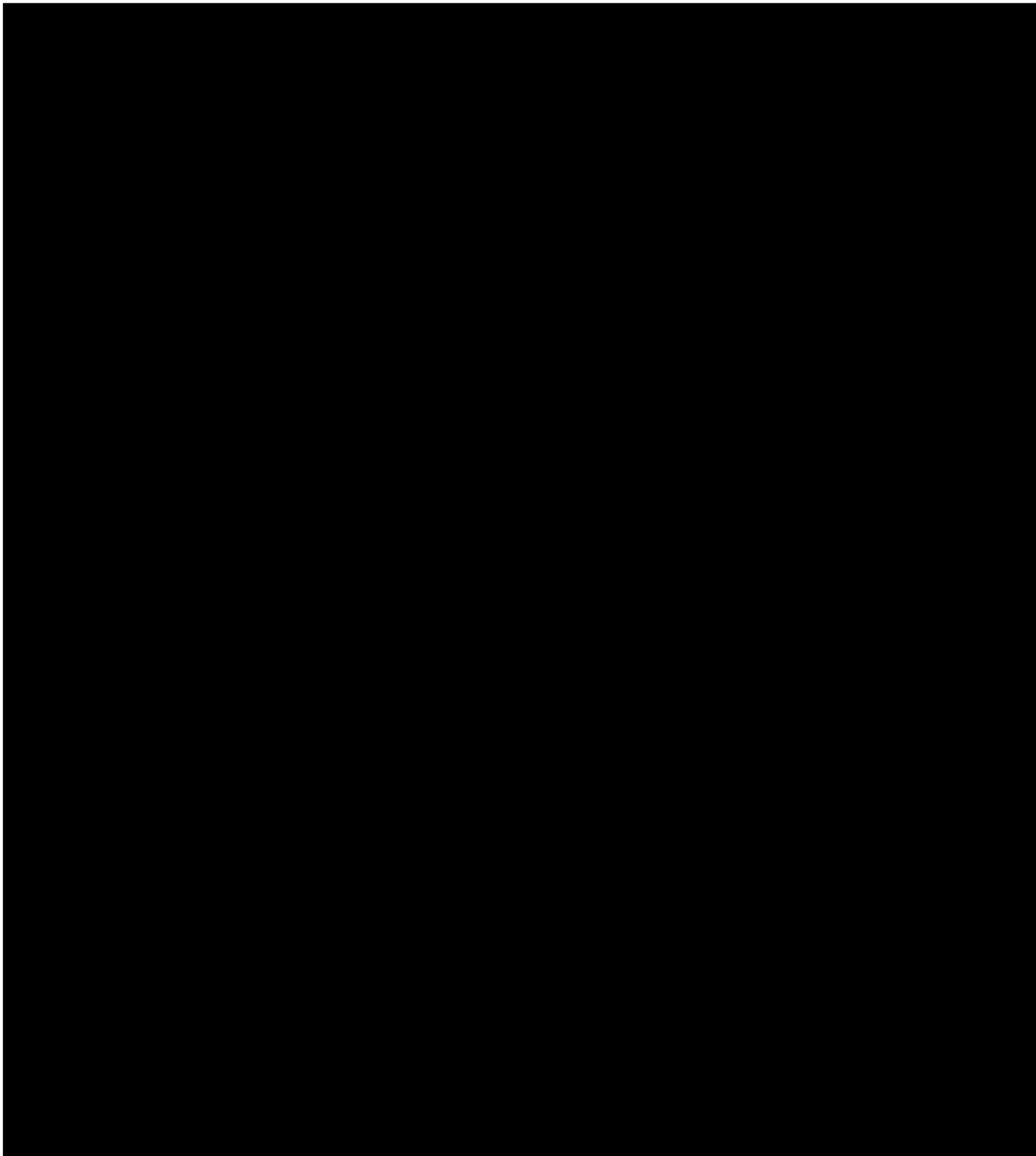


NaBISCOP
USCIS FDNS-HB 602-001



NaBISCOP
USCIS FDNS-HB 602-001

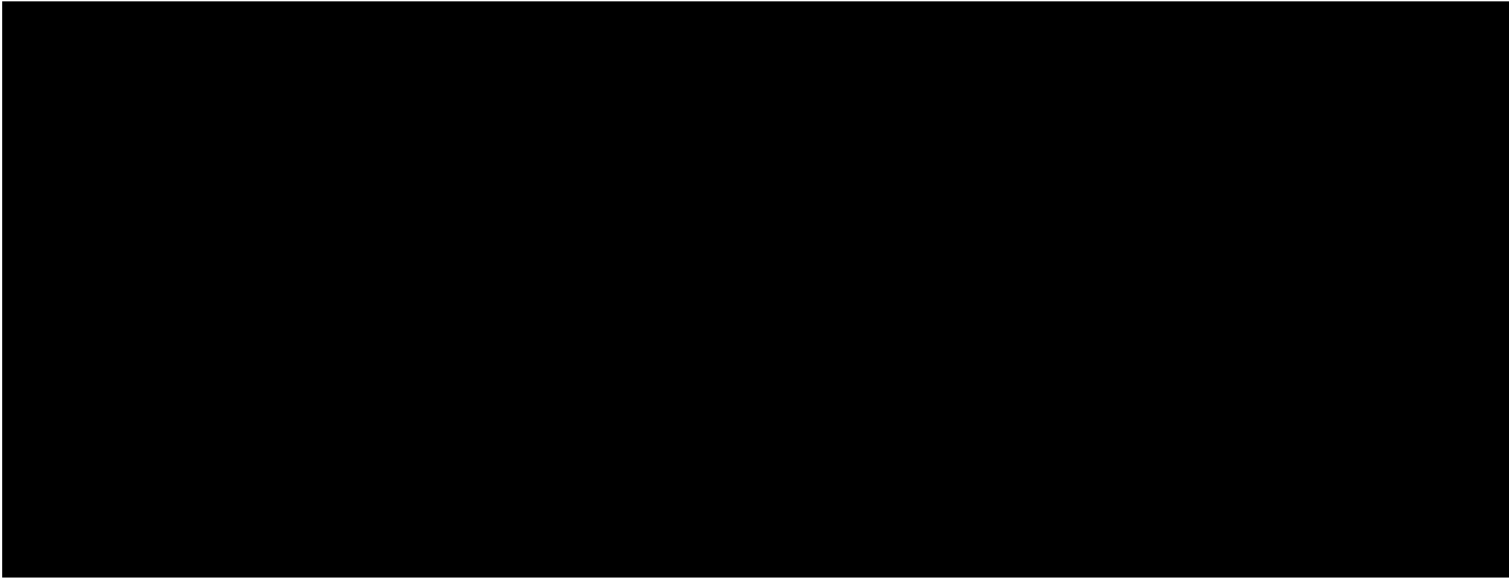
FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

111

FOUO-LES



[Return to the Section Contents](#)
[Return to the Table of Contents](#)

C.



NaBISCOP
USCIS FDNS-HB 602-001

Figure 14:



[Return to the Section Contents](#)
[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

D.

Figure 15:

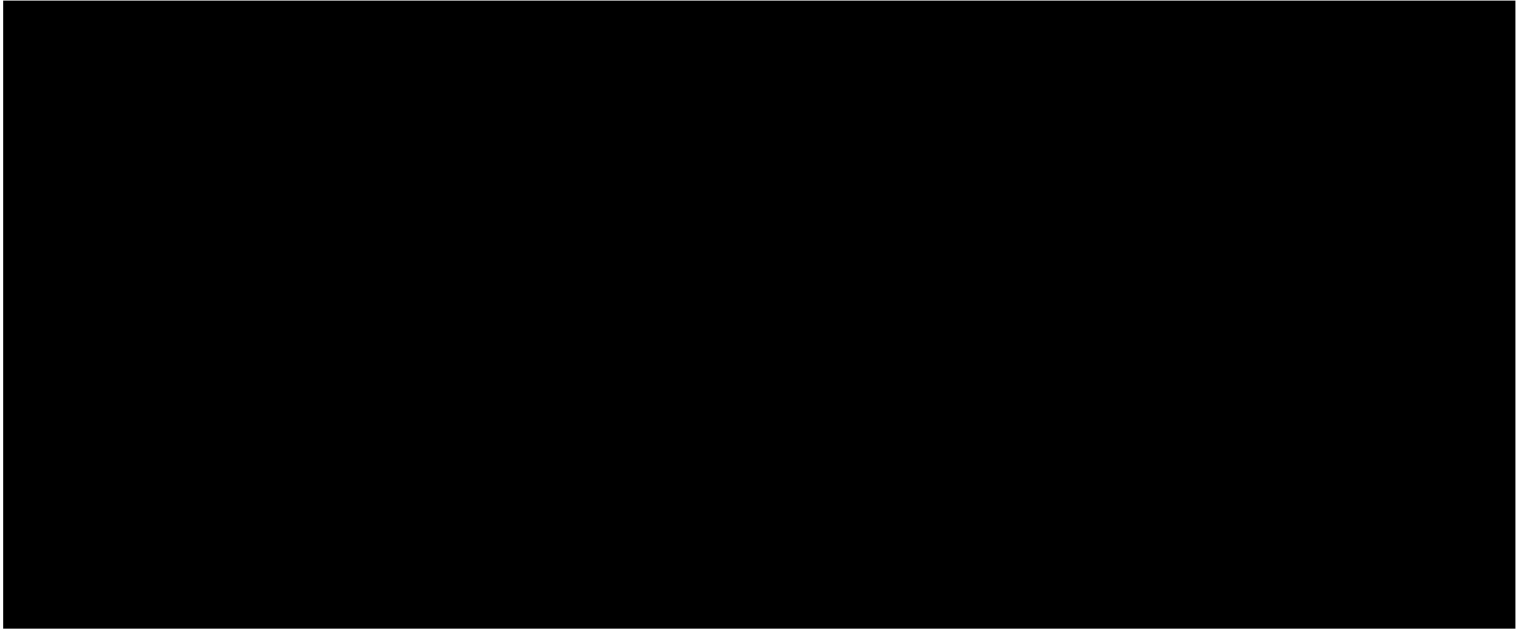
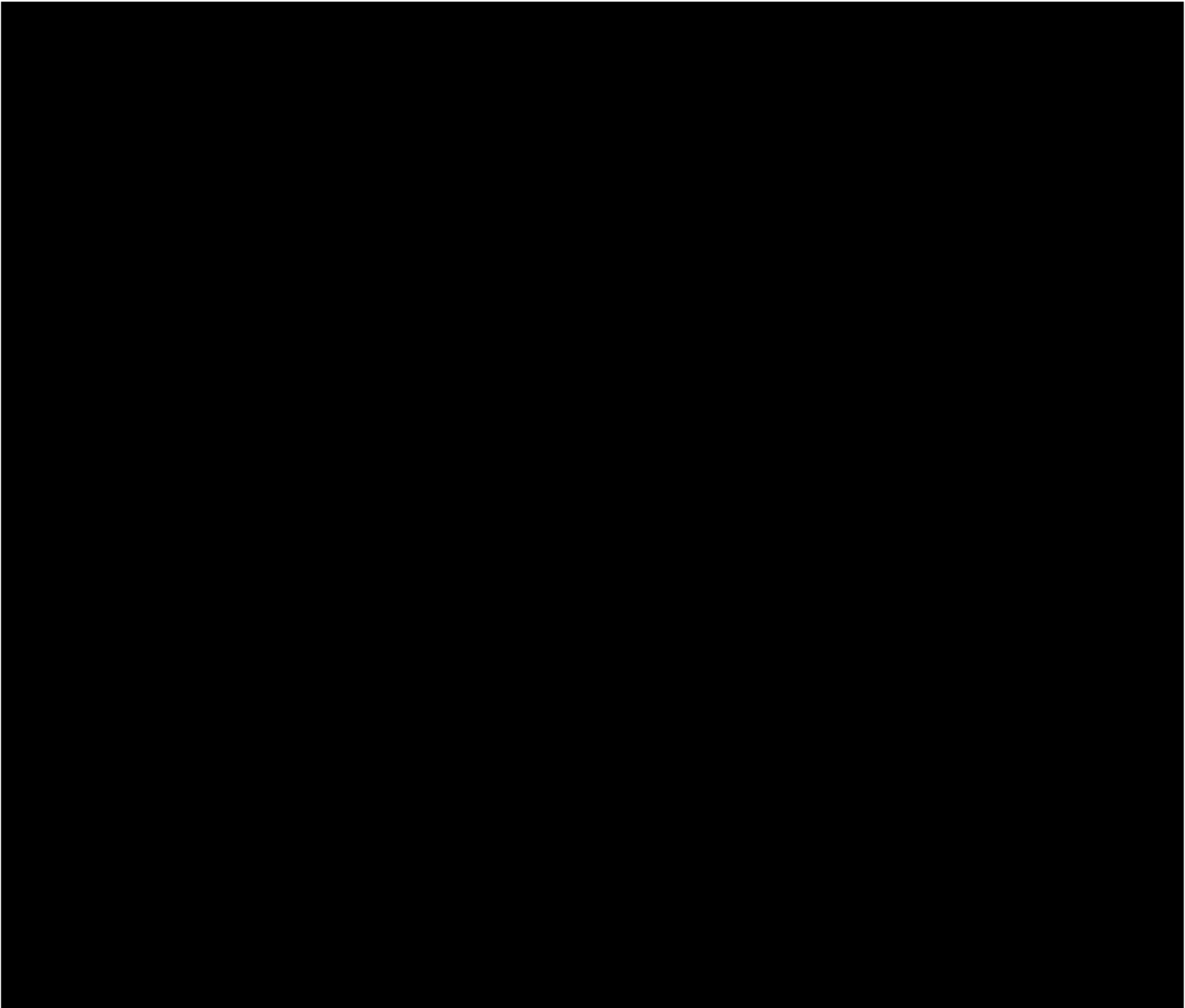


Table 37:

A large rectangular area of the page is completely blacked out, indicating redaction of the content associated with Table 37.

**NaBISCOP
USCIS FDNS-HB 602-001**



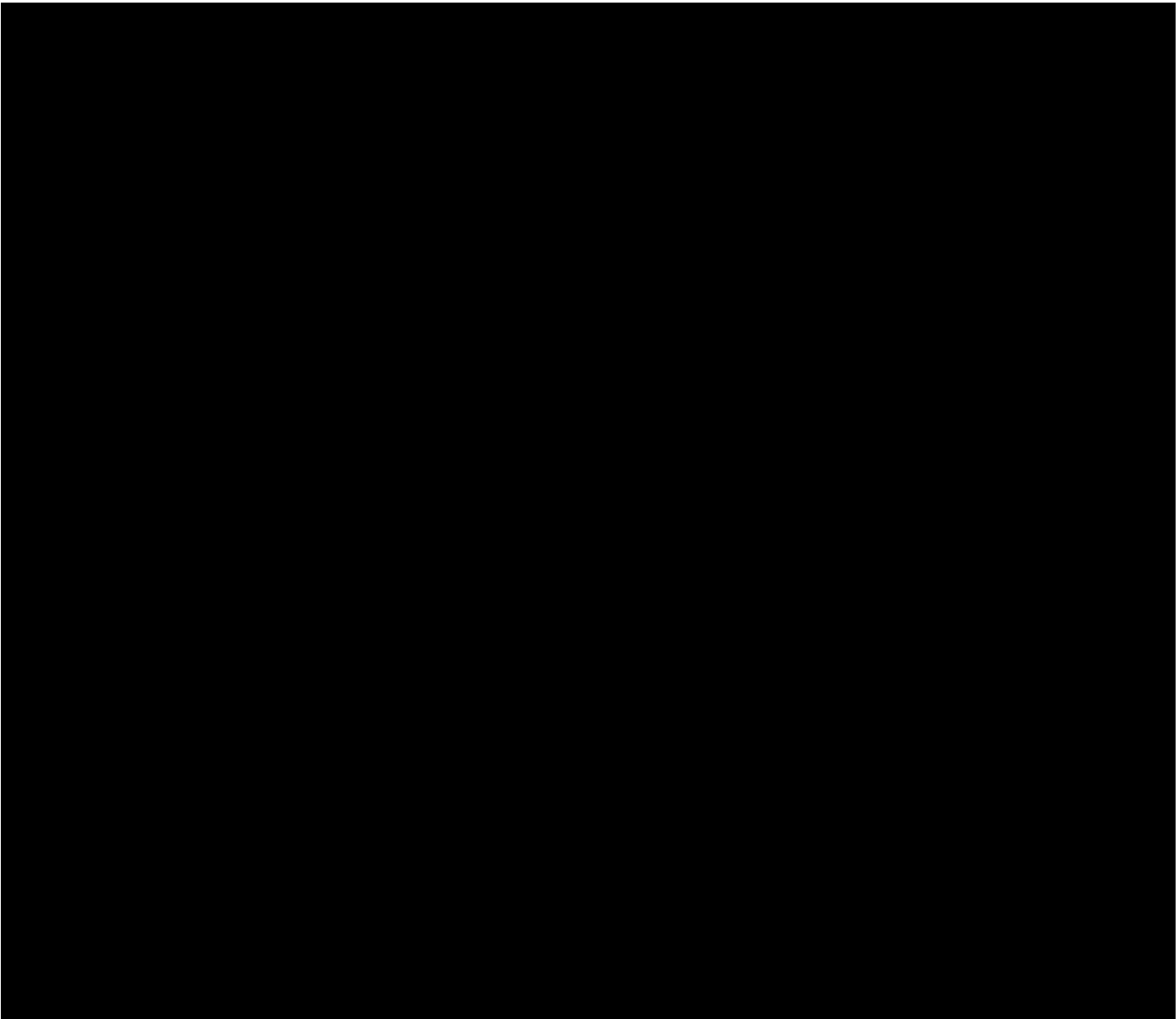
[Return to the Section Contents](#)

[Return to the Table of Contents](#)

E. 

A large black rectangular redaction covers the text following the letter 'E.', extending across the width of the page.

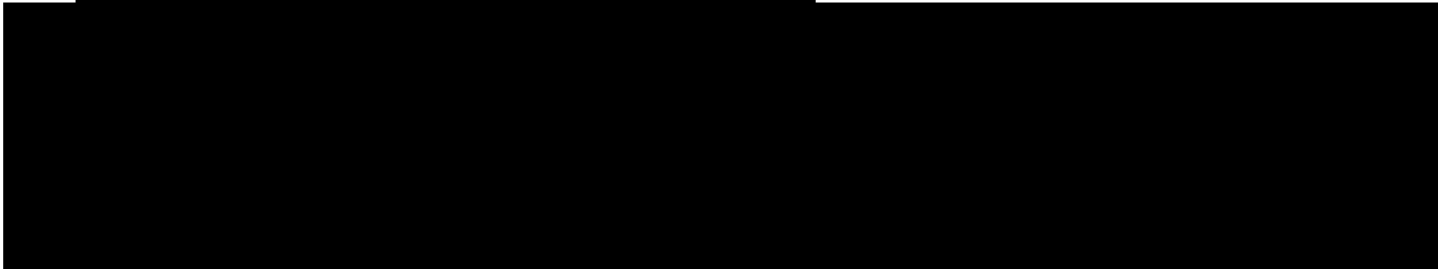
NaBISCOP
USCIS FDNS-HB 602-001



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

F.



NaBISCOP
USCIS FDNS-HB 602-001



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

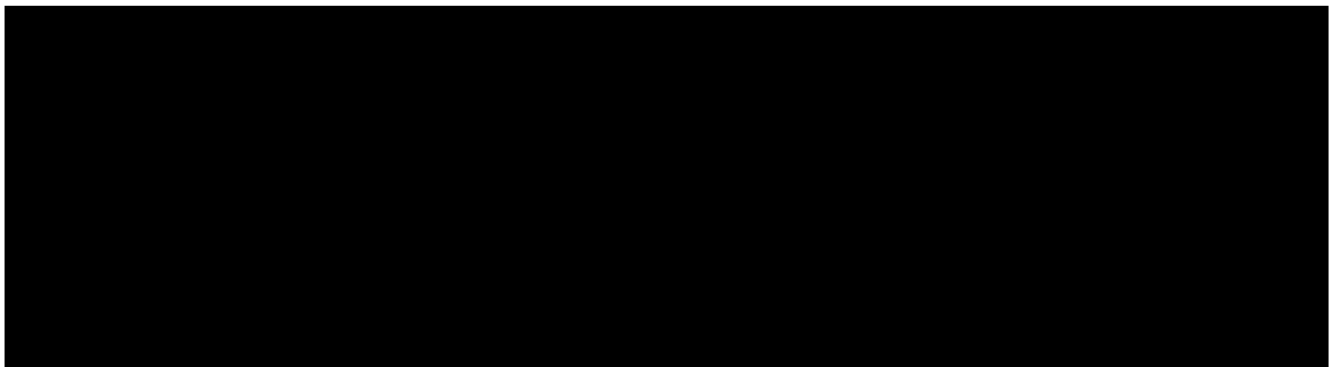
G.



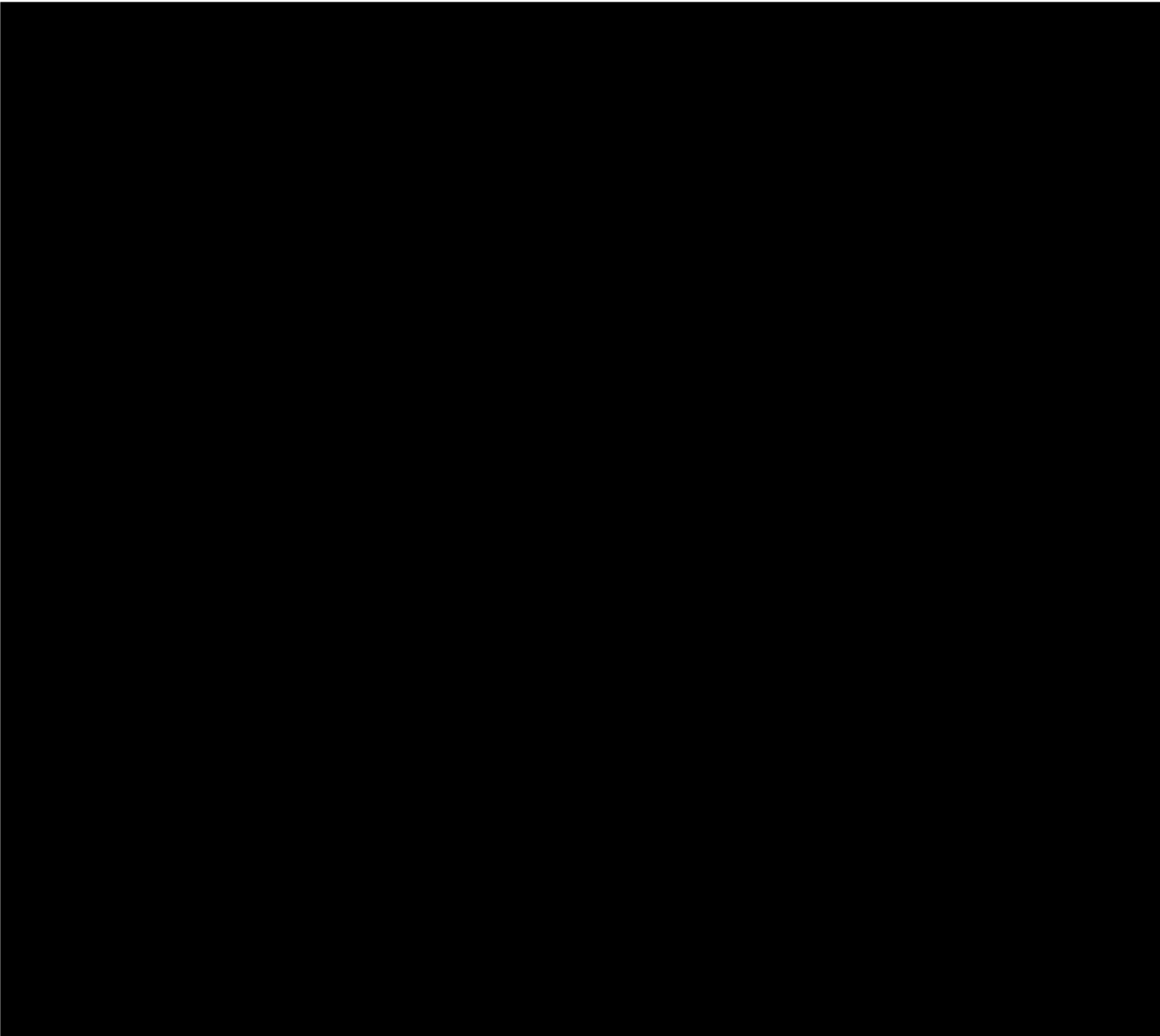
[Return to the Section Contents](#)

[Return to the Table of Contents](#)

H.



NaBISCOP
USCIS FDNS-HB 602-001



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

I. Internal USCIS Policy Relating to FBI Fingerprint Checks

The below internal policy memoranda relate to the FBI Fingerprint Check:

**NaBISCOP
USCIS FDNS-HB 602-001**

- “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,
[REDACTED]
- “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, [REDACTED]
- “Additional Guidance: Processing Fingerprint Checks Prior to the Filing of Form I-600 Abroad,” dated May 13, 2003, and signed by William R. Yates,
[REDACTED]
- “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,
[REDACTED]
- “Fingerprint Check Integrity When Adjudicating Orphan Petitions,” dated February 14, 2003, and signed by Johnny N. Williams,
[REDACTED]
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,”
[REDACTED]
Attachment Two - Beginning on page 6: “National Quality Procedures, Part III, Fingerprint Check Integrity,”
[REDACTED]
- “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, [REDACTED]
- “Request for Duplicate Rap Sheets and Inquiries”, dated February 22, 2001, and signed by William R. Yates
- “Policy for Requesting Updated Rap Sheets for Expired Fingerprint Results”, dated December 27, 2001, and signed by William R. Yates
- “Expeditious Processing of Civil Fingerprint Cards, Forms FD-258,” dated May 18, 2000, and signed by William R. Yates,
[REDACTED]
- “Fingerprint Waiver Policy for Naturalization Applicants who are Unable to be Fingerprinted (NOP Policy Memorandum No. 60),” dated November 15, 1999, and signed by William R. Yates,
[REDACTED]

**NaBISCOP
USCIS FDNS-HB 602-001**

- “*Guidance on the Acceptance and Handling of FD-258 Fingerprint Cards (NOP Policy Memorandum No. 32)*,” dated March 27, 1998, and signed by James S. Angus, [REDACTED]
- “*Benefits-Related Fingerprint Clearance Policy*,” dated April 2, 1997, and signed by Paul W. Virtue HQPGM, [REDACTED]

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

VIII. Security Check: US-VISIT/IDENT

Section Contents

A.

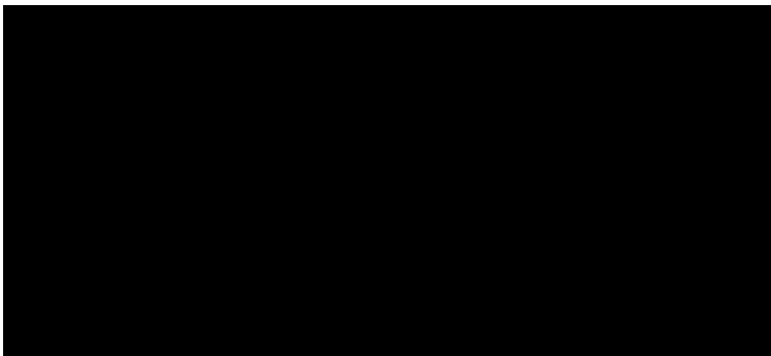
B.

C.

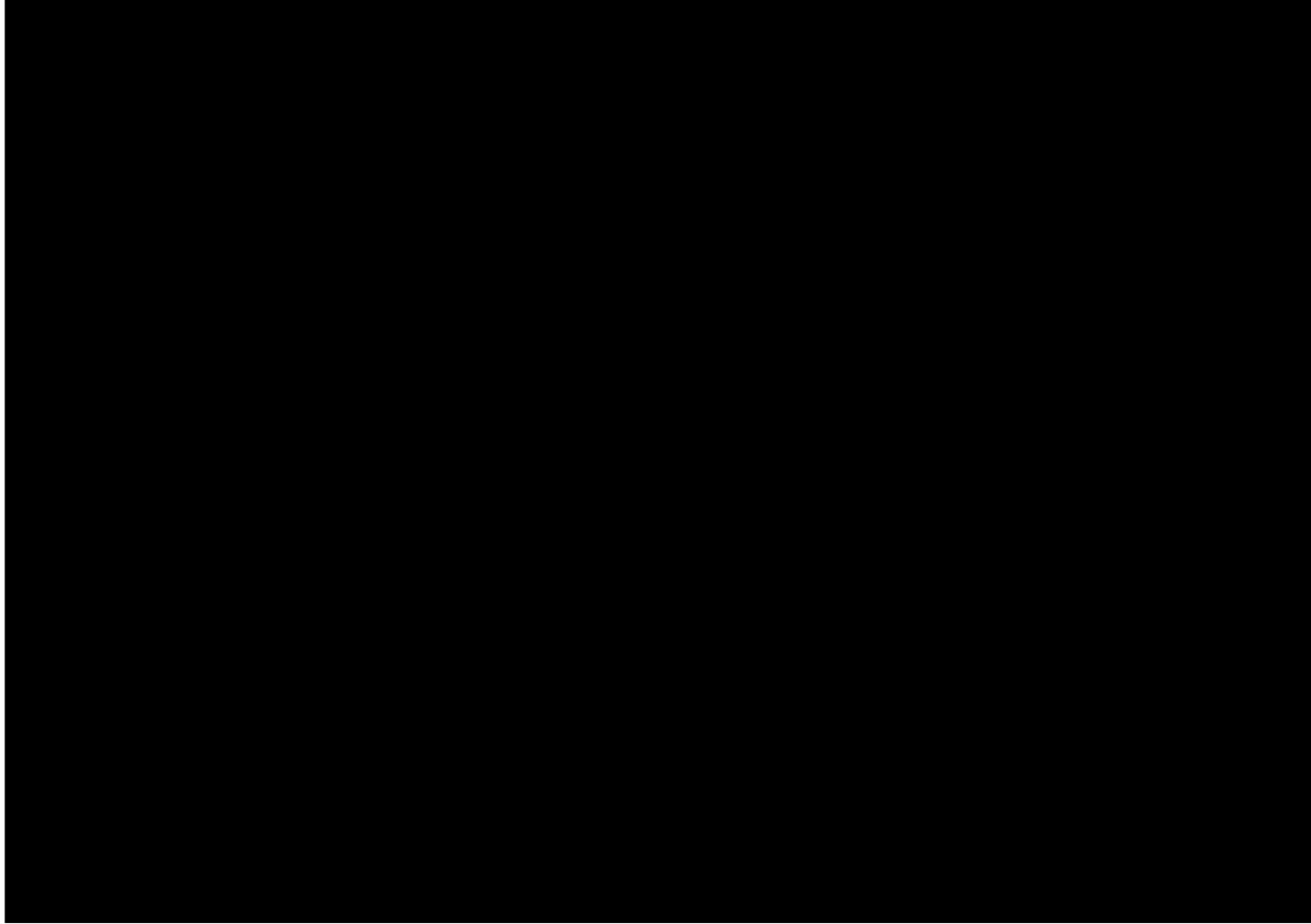
D.

E.

F.



A.



**NaBISCOP
USCIS FDNS-HB 602-001**

NaBISCOP
USCIS FDNS-HB 602-001

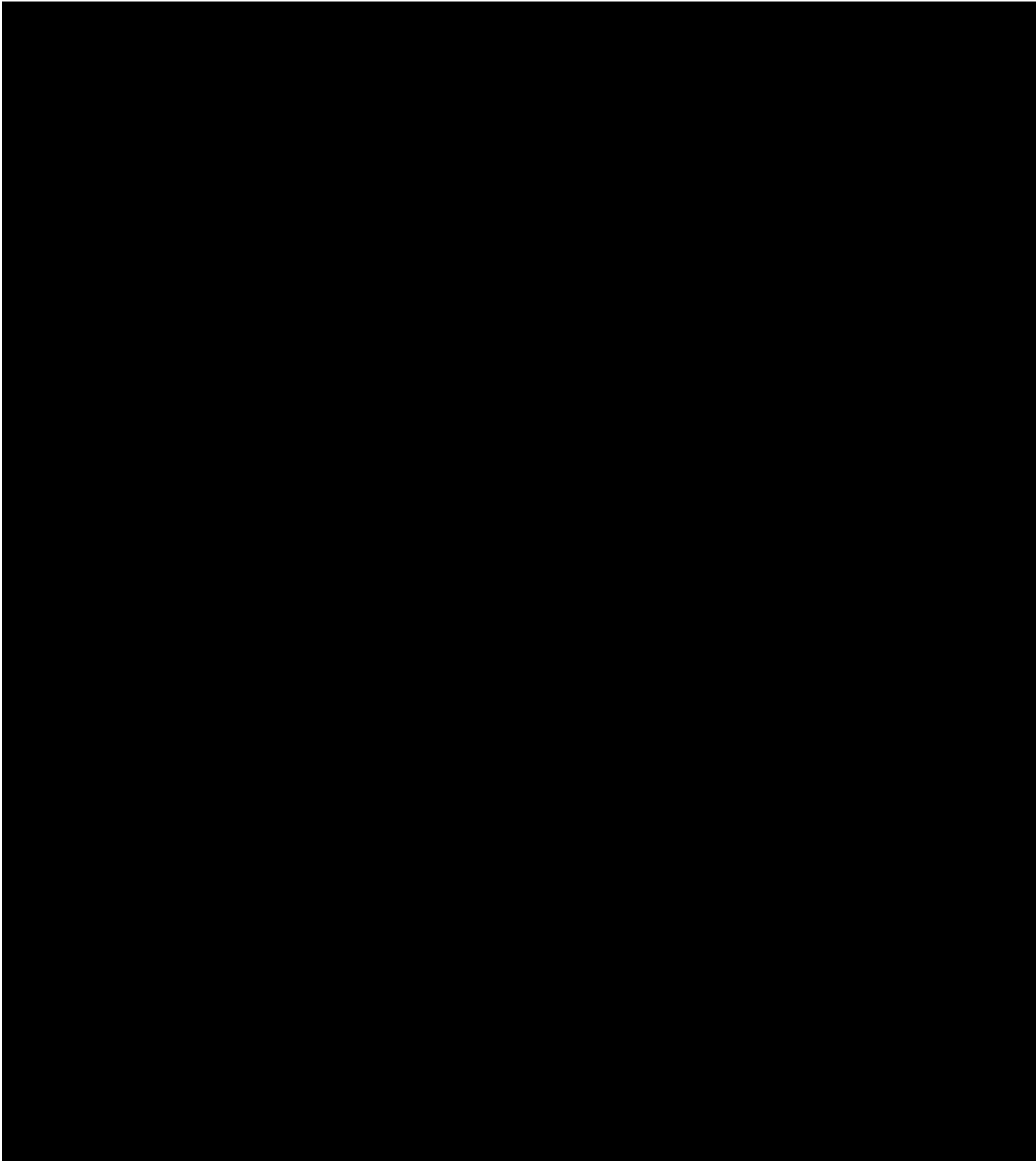
122

FOUO-LES

Table 38:

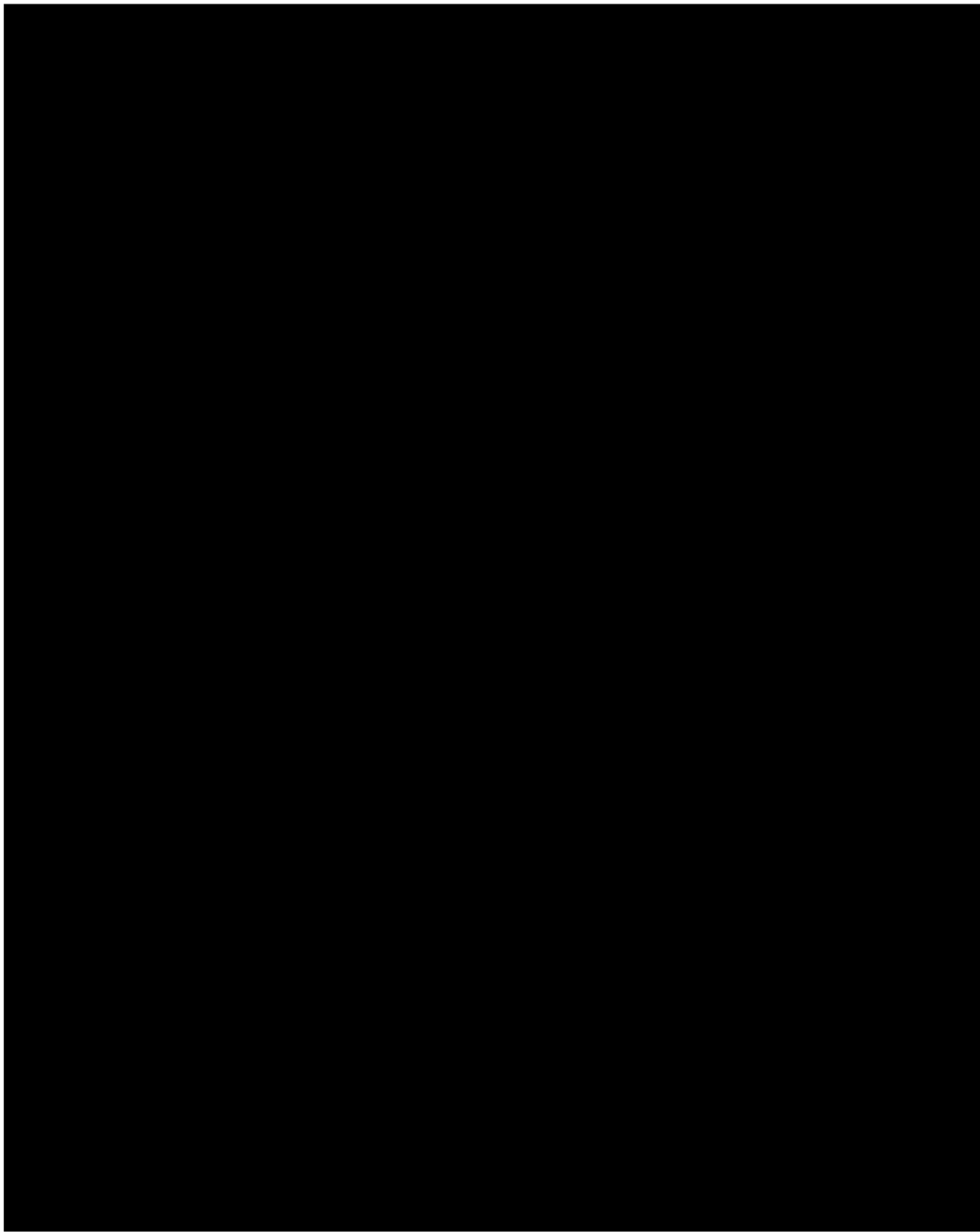


**NaBISCOP
USCIS FDNS-HB 602-001**



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES



NaBISCOP
USCIS FDNS-HB 602-001

125

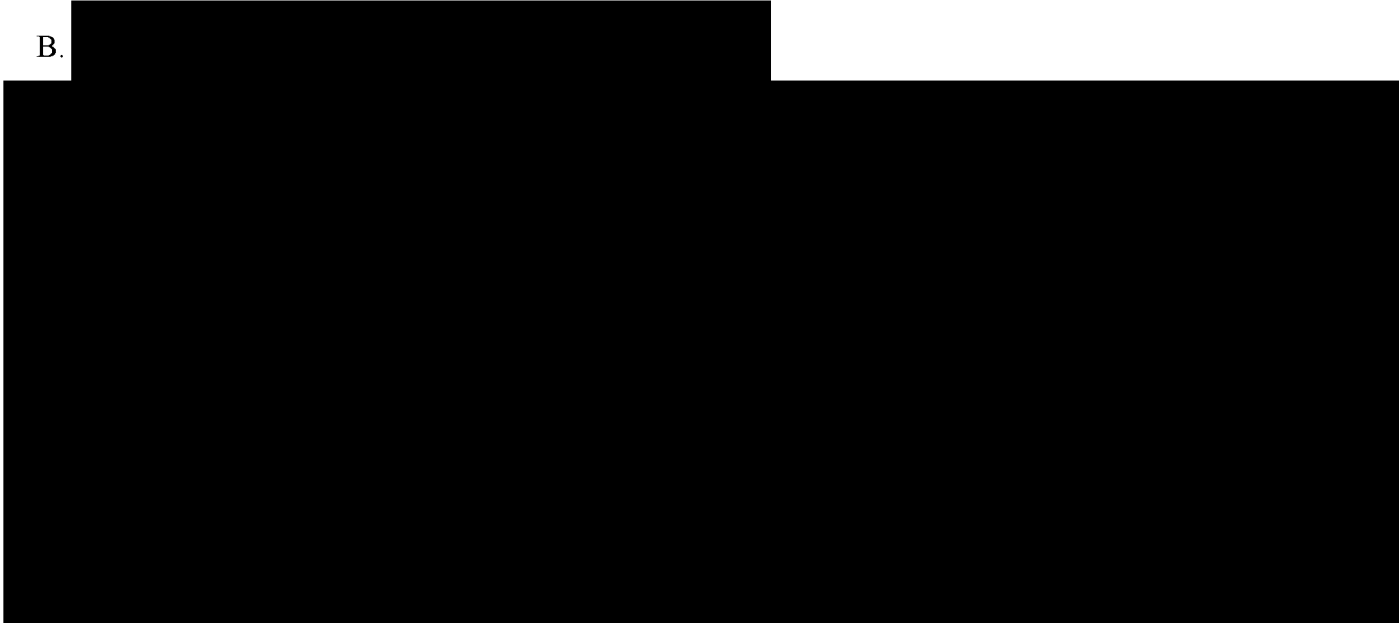
FOUO-LES



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

B.



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

C.

[REDACTED]

[REDACTED]

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

D.

[REDACTED]

[REDACTED]

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

E.

[REDACTED]

[REDACTED]

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

F.

[REDACTED]

[REDACTED]

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

IX. Resolution: National Security Concerns (CARRP)

Section Contents

- A. CARRP Policy and Operational Guidance
- B. Definitions of NS Concern
 - 1. Known or Suspected Terrorist (KST)
 - 2. Non-KST NS Concern
 - 3. Non National Security (NNS)
- C. Four Step Approach to Cases with National Security Concerns
- D. Employment and Travel Authorization Applications with NS Concerns
- E. Form I-90 with NS Concerns
- F. Santillan (EOIR Grants) with NS Concerns
- G. Request for Assistance to HQFDNS National Security Branch (NSB)

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,

[REDACTED]

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

[REDACTED]

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,

[REDACTED]

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

Operational Guidance

- Domestic Operations issued on April 24, 2008:

NaBISCOP
USCIS FDNS-HB 602-001

“Operational Guidance for Vetting and Adjudicating Cases with National Security Concerns,”
signed by Don Neufeld,

- 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,
- 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,
- Refugee Affairs Division and International Operations Division issued on November 19, 2008:
“Processing of Refugee Cases with National Security Concerns,” signed by Barbara Strack and Joanna Ruppel,
- 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,

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

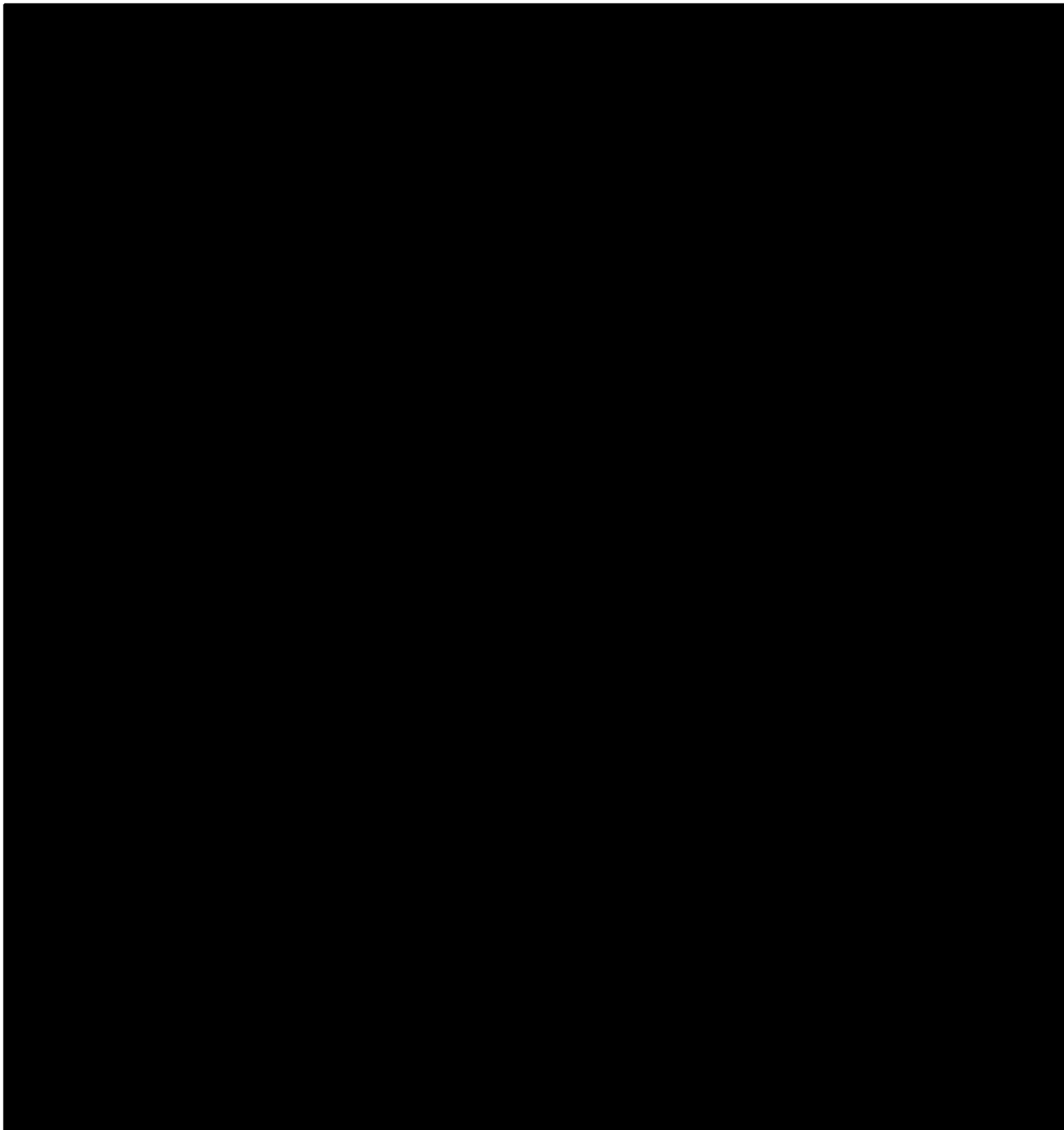
B. Definition of NS Concern

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:

NaBISCOP
USCIS FDNS-HB 602-001



NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

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.

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

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, “individual”¹³), 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). See Attachment A entitled “*Guidance for Identifying National Security Concerns*,”

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.

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

NaBISCOP
USCIS FDNS-HB 602-001

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.

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

D. Employment and Travel Authorization Applications with NS concerns

Form I-765 applications must be adjudicated within ninety (90) days of receipt unless an interim Employment Authorization Document (EAD) is issued or an exception applies under 8 CFR 274a.13(d).

**NaBISCOP
USCIS FDNS-HB 602-001**

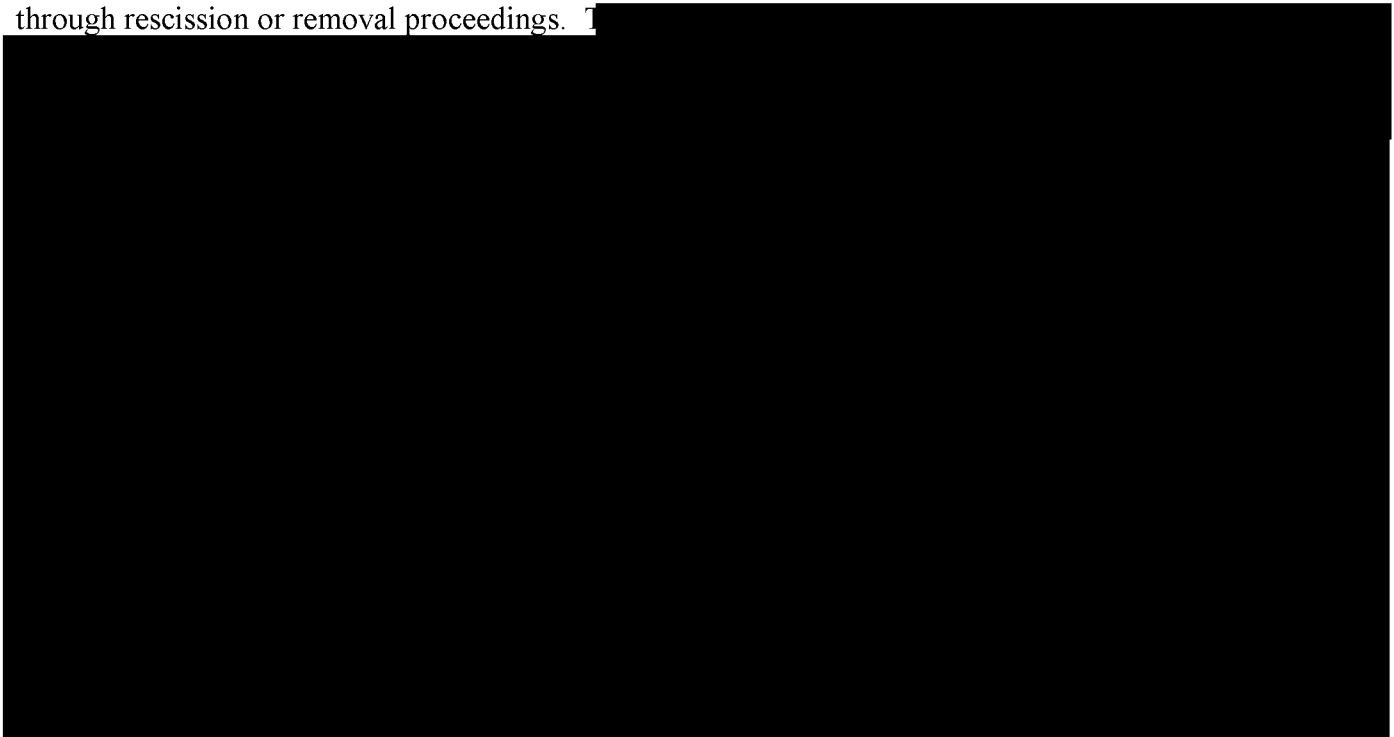


[Return to the Section Contents](#)

[Return to the Table of Contents](#)

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. [



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

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 status. These individuals are currently covered by the terms of the injunction order issued on December 22, 2005

**NaBISCOP
USCIS FDNS-HB 602-001**

(published at 2005 WL 3542661).¹⁴ 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.

[Return to the Section Contents](#)

[Return to the Table of Contents](#)

G. Request for Assistance to HQFDNS National Security Branch (NSB)

The field may contact HQFDNS for assistance during the processing of an application/petition with an NS concern. The field must obtain local management approval prior to sending RFA requests, and must have completed all internal vetting and the initial eligibility assessment.

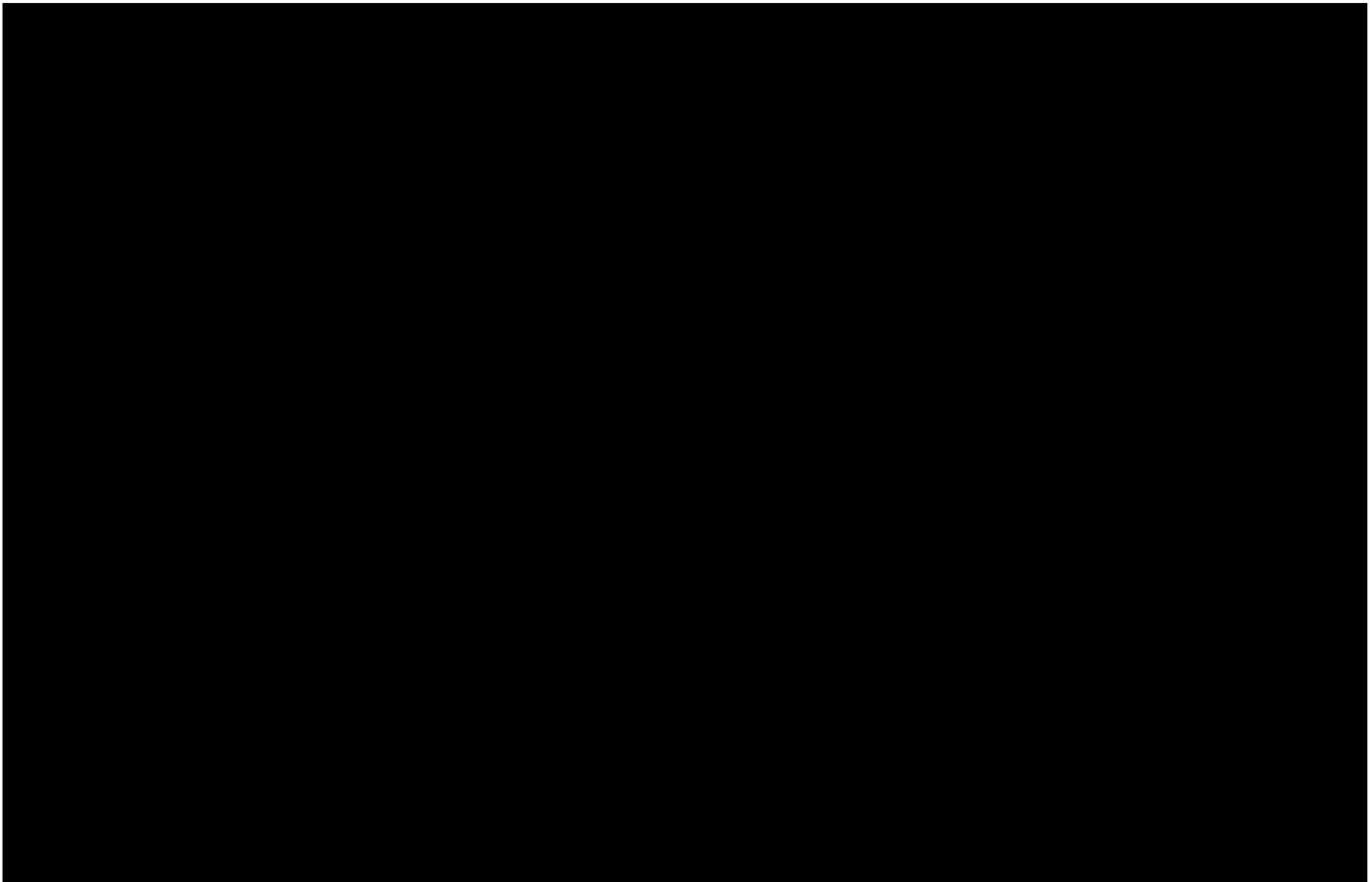
Upon obtaining local management approval, the field may e-mail an RFA to HQFDNS ([REDACTED]) under the following circumstances:

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

¹⁴ 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."

NaBISCOP
USCIS FDNS-HB 602-001

When requesting vetting or adjudicative assistance from HQFDNS, the designated officer sends a request for assistance to [REDACTED]. When sending a request containing PII, officers must comply with the PII requirements explained on page 6-7 of this manual. The request should be marked “For Official Use Only (FOUO)” and include the following information:



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

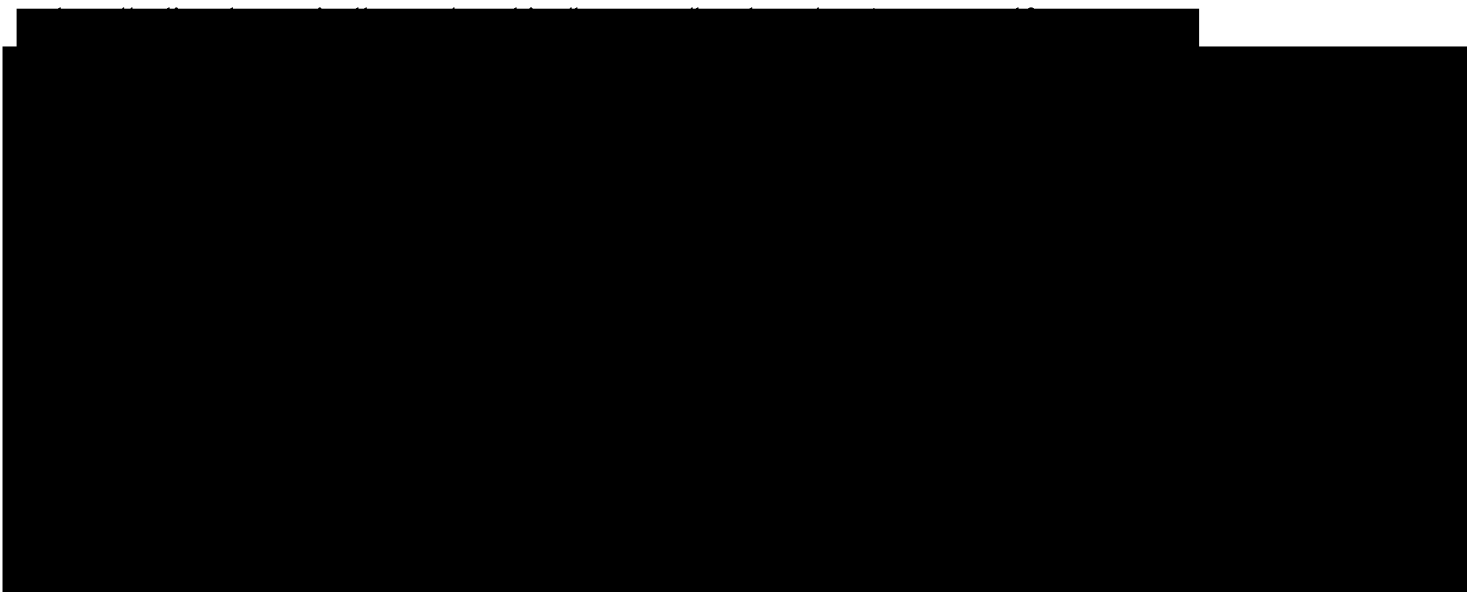
X. Resolution: Egregious Public Safety Concerns & Other Criminal Cases

Section Contents

- A. Egregious Public Safety (EPS) Policy and Guidance
- B. EPS Case Definition
- C. Adam Walsh Act
- D. International Marriage Broker Regulation Act
- E. Referral to ICE (RTI) for EPS Case
- F. Referral to ICE for Other Criminal Cases
- G. Exceptions to EPS RTI Criteria
- H. Employment and Travel Authorization Applications with EPS Concerns
- I. Form I-90 with EPS Concerns
- J. Santillan (EOIR Grants) with EPS Concerns

A. Egregious Public Safety (EPS) Policy and Guidance

USCIS has 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, and the accompanying policy memorandum entitled “*Disposition of Cases Involving Removable Aliens*,” dated July 11, 2006, and also referred to as Policy Memorandum 110,



[Return to the Section Contents](#)

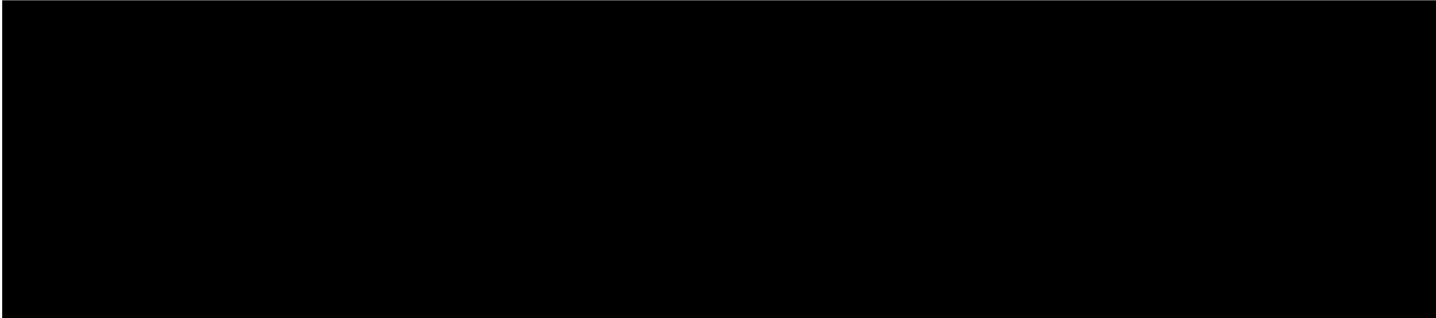
[Return to the Table of Contents](#)

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:

**NaBISCOP
USCIS FDNS-HB 602-001**

- 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.



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

C. 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.


[Return to the Section Contents](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

[Return to the Table of Contents](#)

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*,”

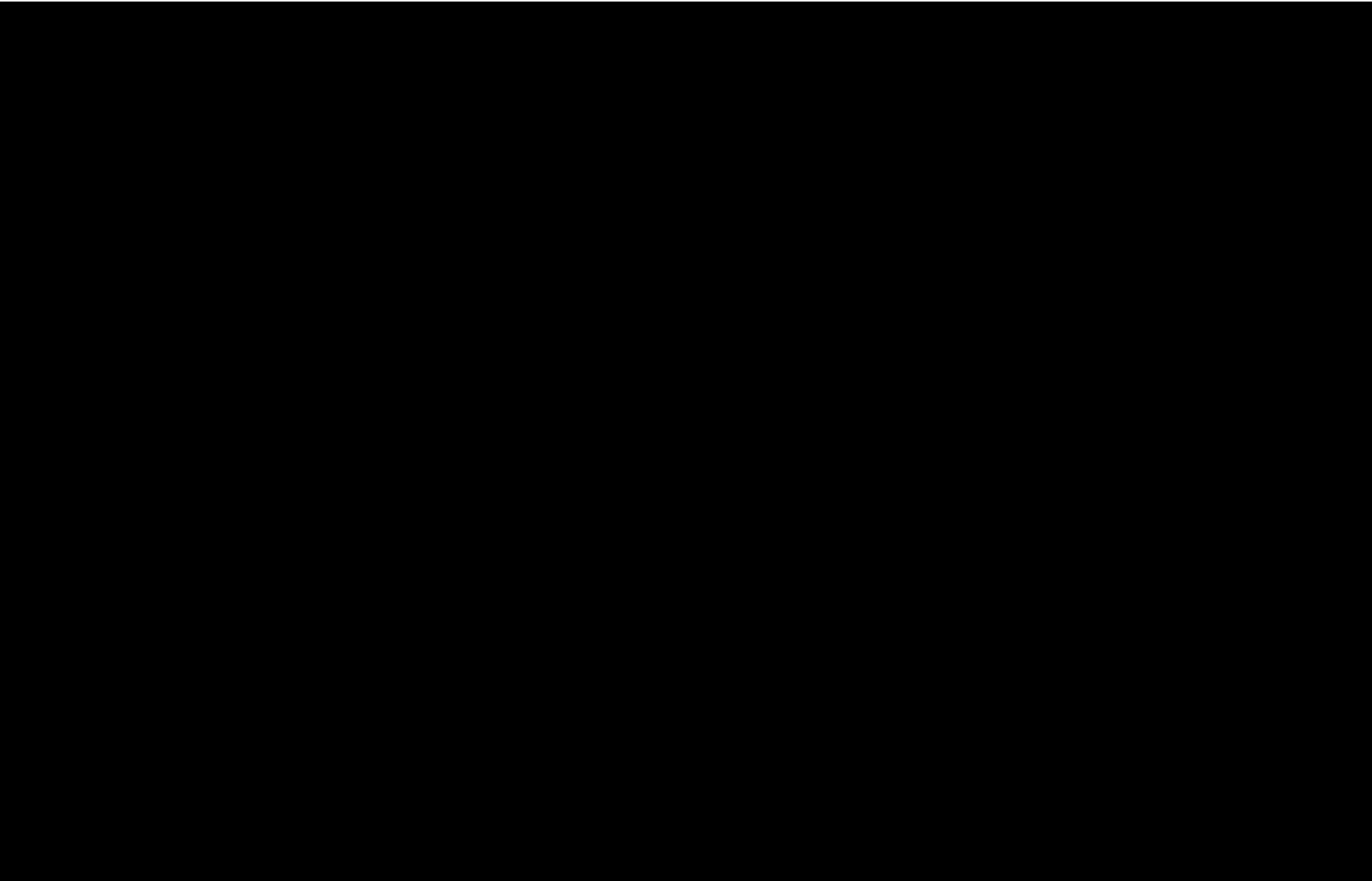


[Return to the Section Contents](#)

[Return to the Table of Contents](#)

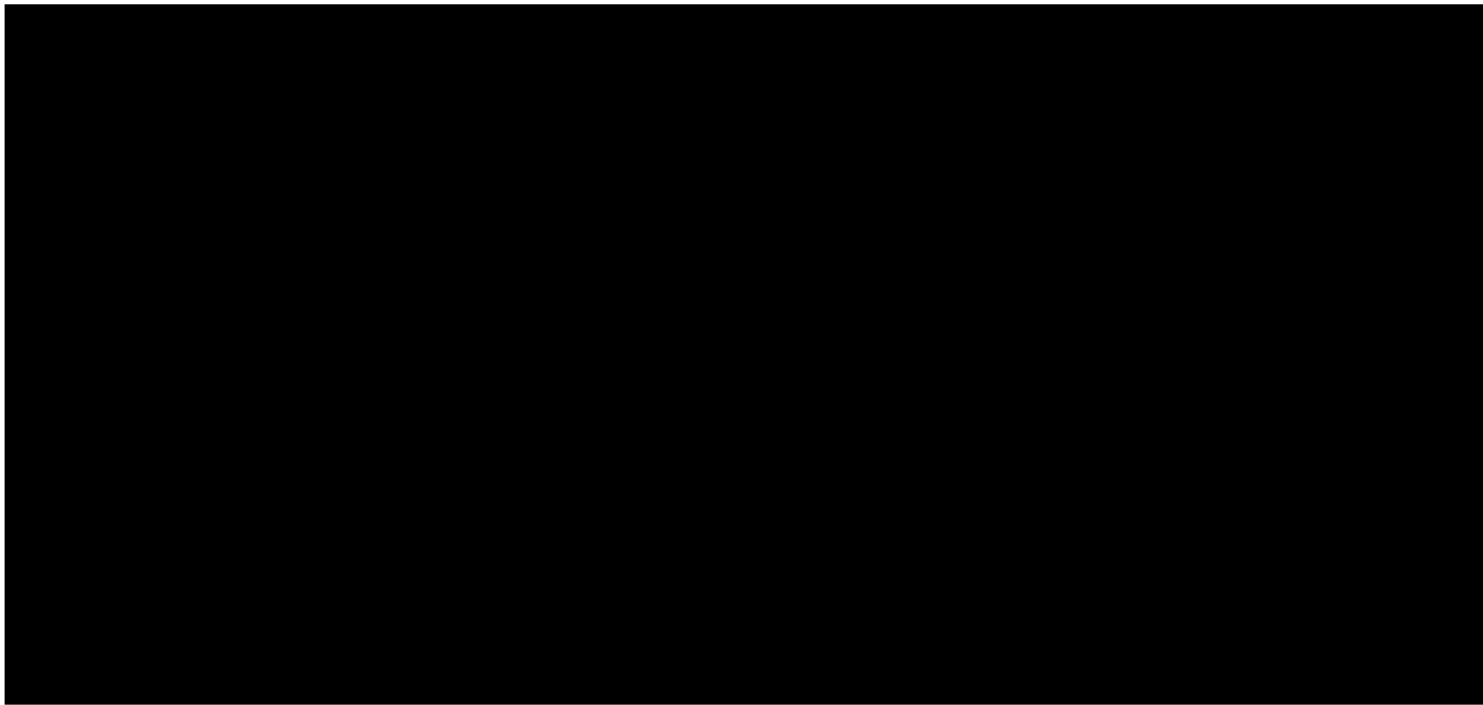
E. Referral to ICE (RTI) for EPS Case

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



¹⁵ 8 CFR 103.2(b)(18)

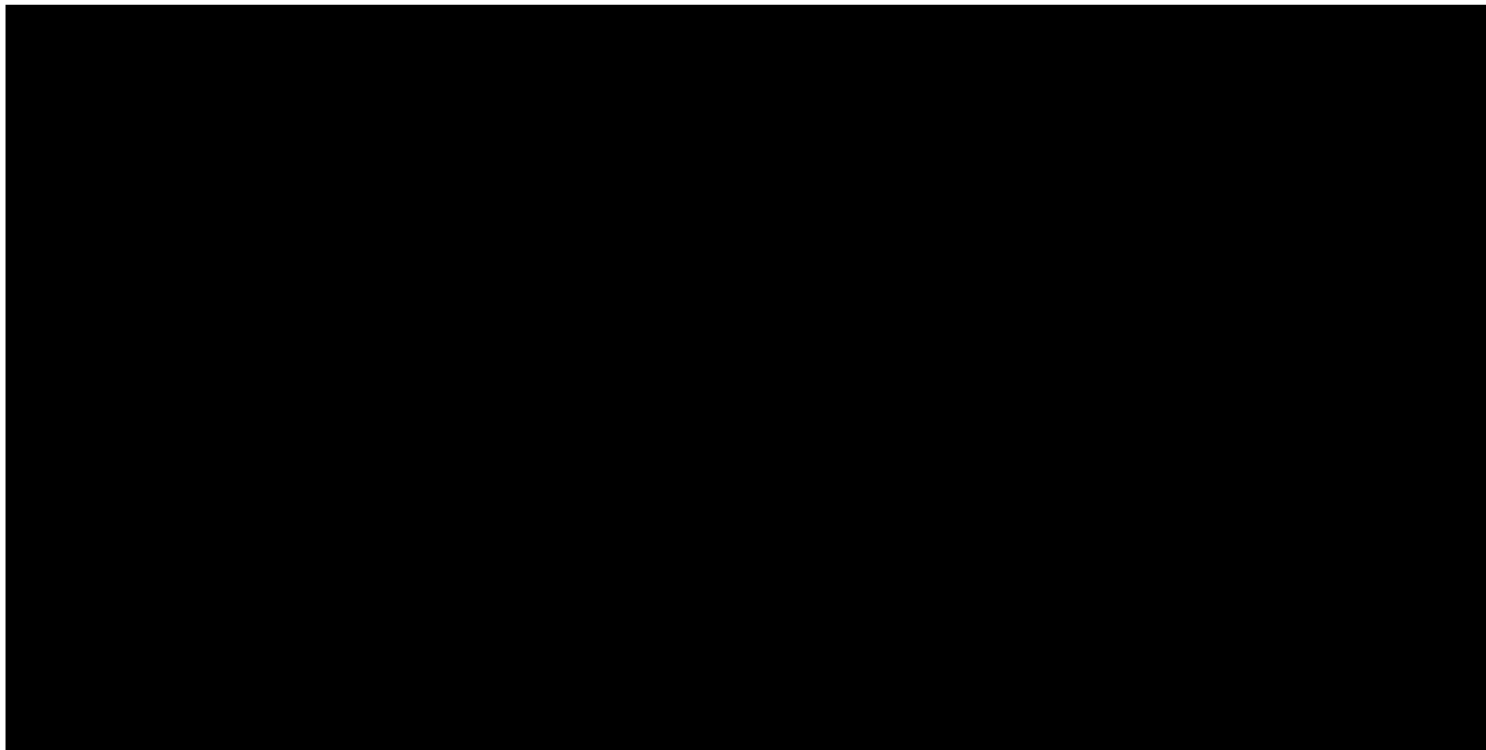
**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

F. Referral to ICE for Other Criminal Cases



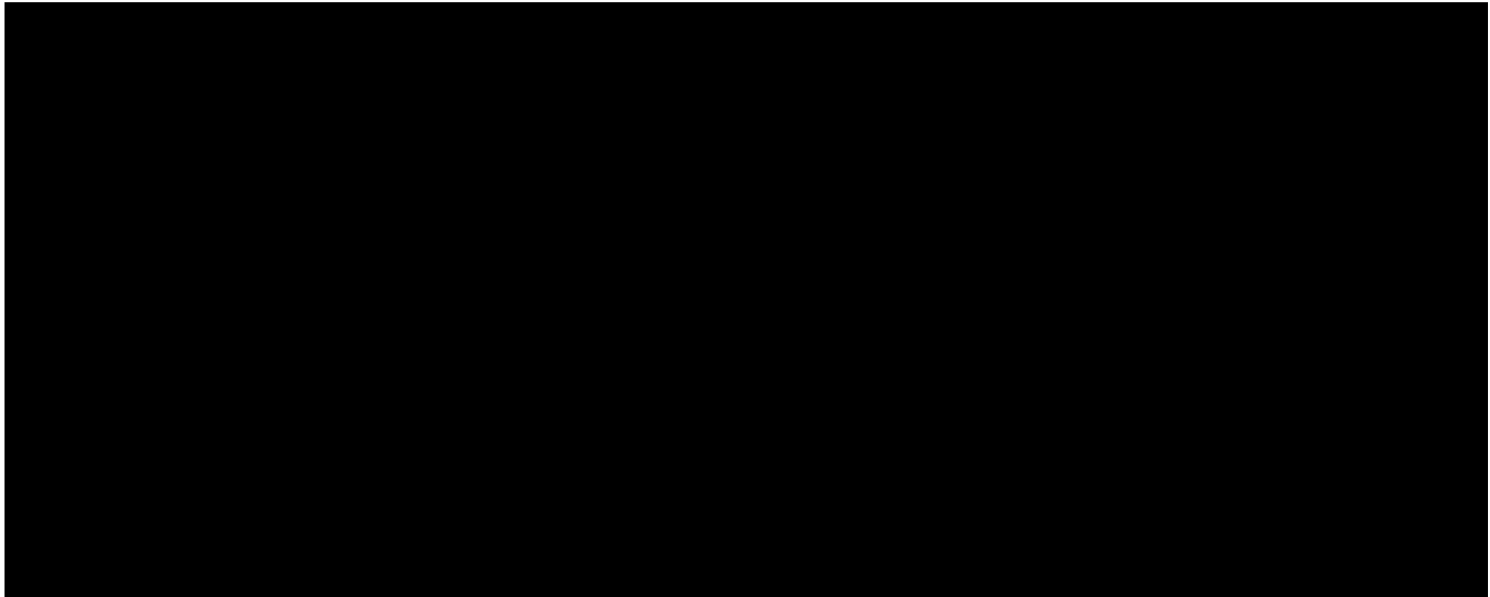
**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

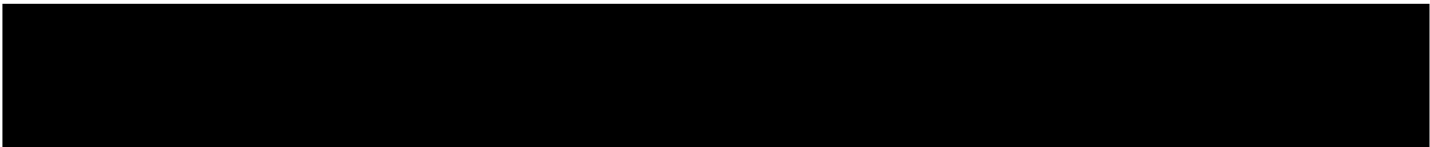
G. Exceptions to EPS RTI Criteria



[Return to the Section Contents](#)

[Return to the Table of Contents](#)

H. Employment and Travel Authorization Applications with EPS Concerns



Form I-765 applications must be adjudicated within ninety (90) days of receipt unless an interim Employment Authorization Document (EAD) is issued or an exception applies under 8 CFR 274a.13(d).

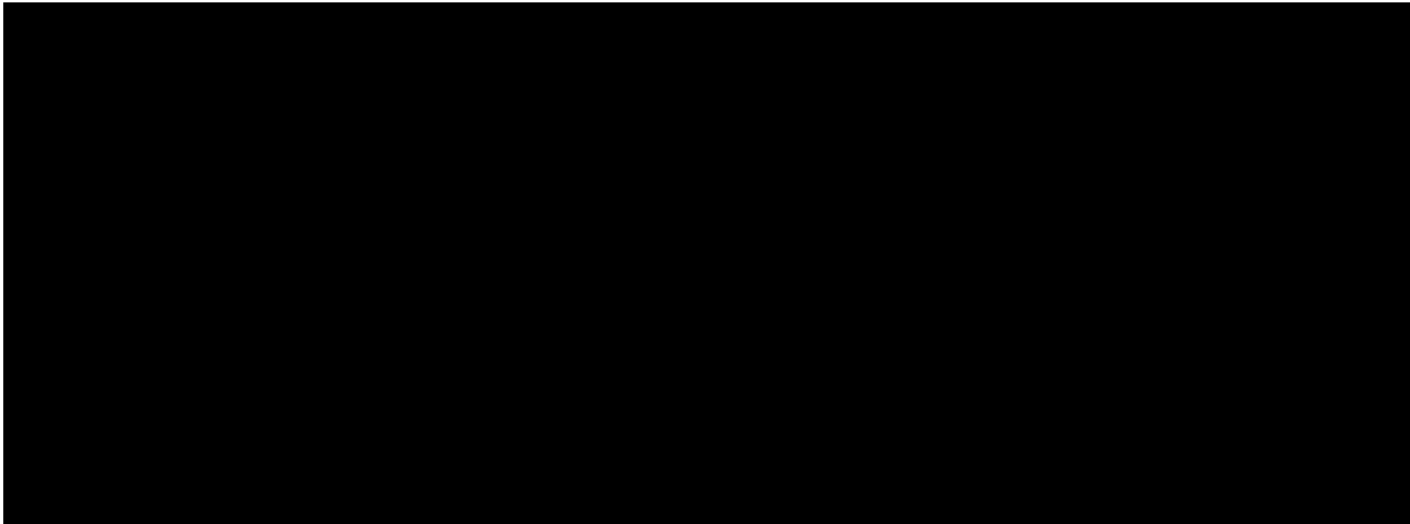
[Return to the Section Contents](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

[Return to the Table of Contents](#)

I. Form I-90 with EPS Concerns

A permanent resident holds lawful status and is entitled to evidence of that status until it is removed through rescission or removal proceedings.

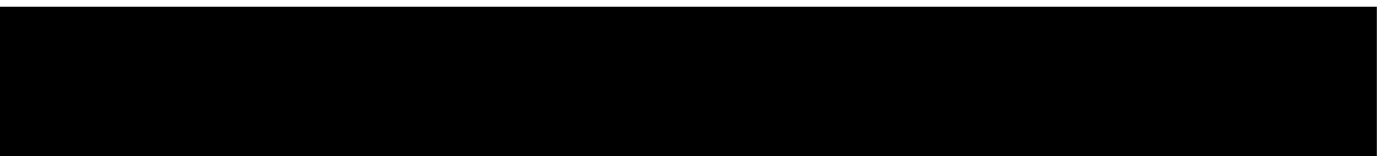


[Return to the Section Contents](#)

[Return to the Table of Contents](#)

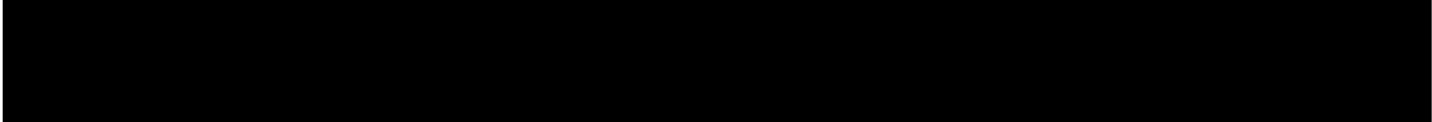
J. Santillan (EOIR Grants) with EPS Concerns

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](#)).¹⁶ 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.



¹⁶ 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.

NaBISCOP
USCIS FDNS-HB 602-001

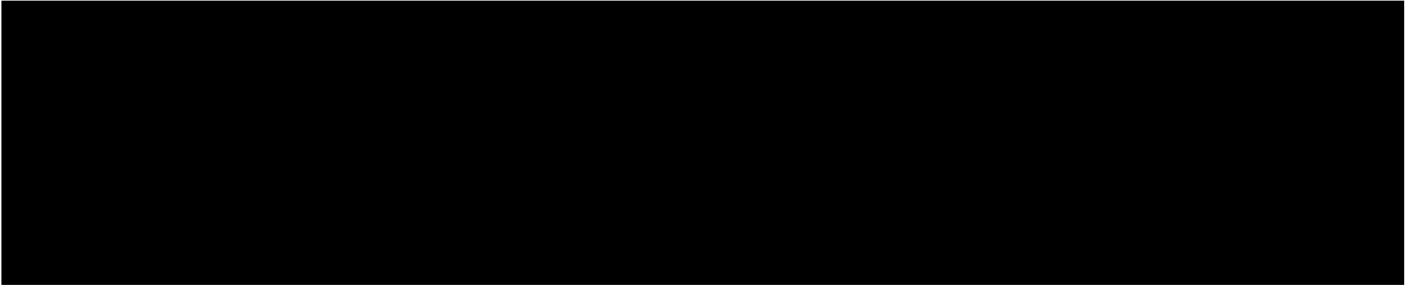


[Return to the Section Contents](#)

[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

XI. Resolution: Immigration Fraud



[Return to the Table of Contents](#)

NaBISCOP
USCIS FDNS-HB 602-001

XII. Appendices

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

Appendix B: Description of Form Numbers

Appendix C: TECS Terms Indicating Possible NS Concerns

Appendix D: List of Acronyms

Appendix E: Glossary of Terms

Appendix F: MS92

Appendix G: List of References

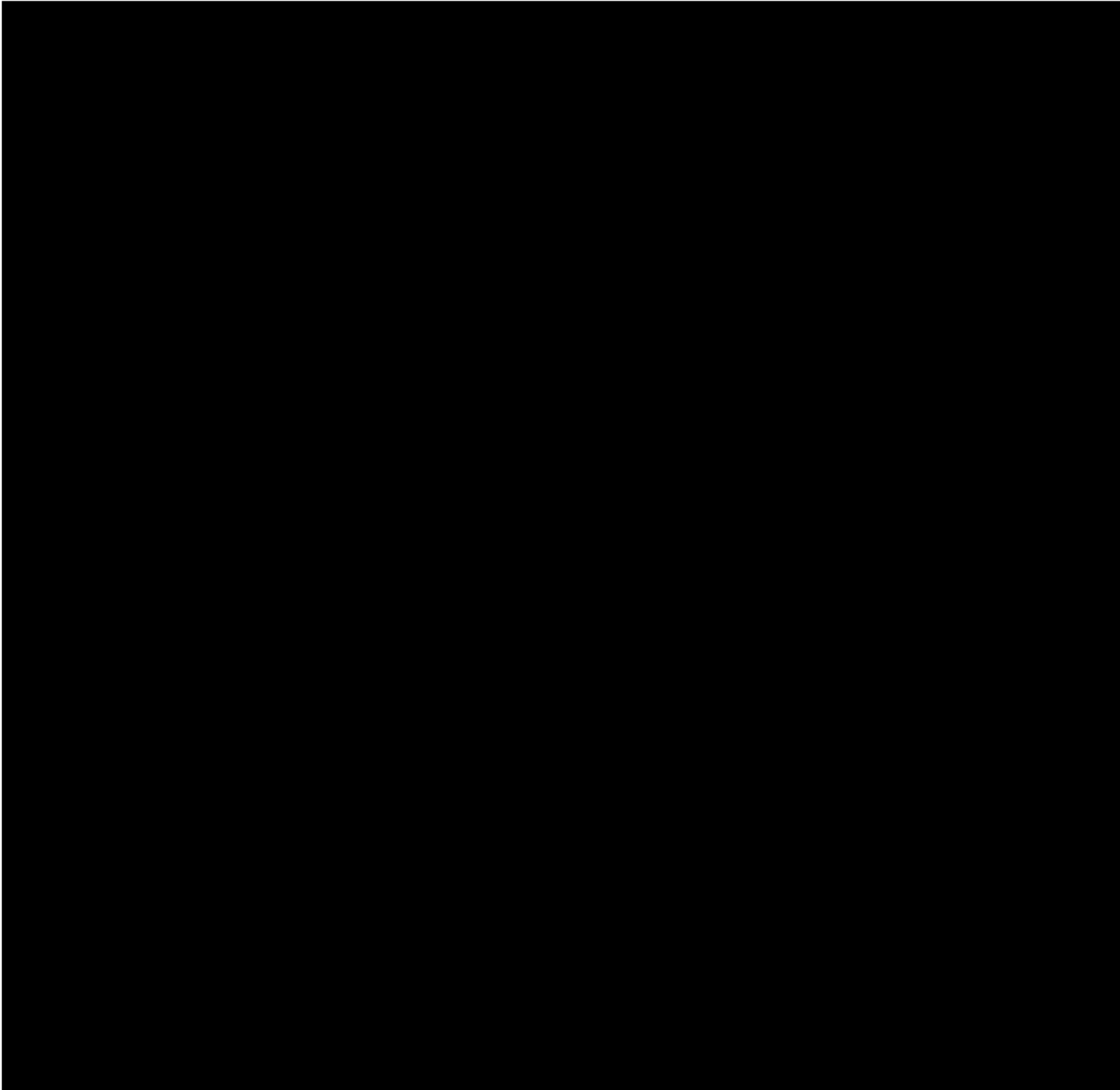
Appendix H: Notice to INTERPOL

Appendix I: Quick Reference

[Return to the Table of Contents](#)

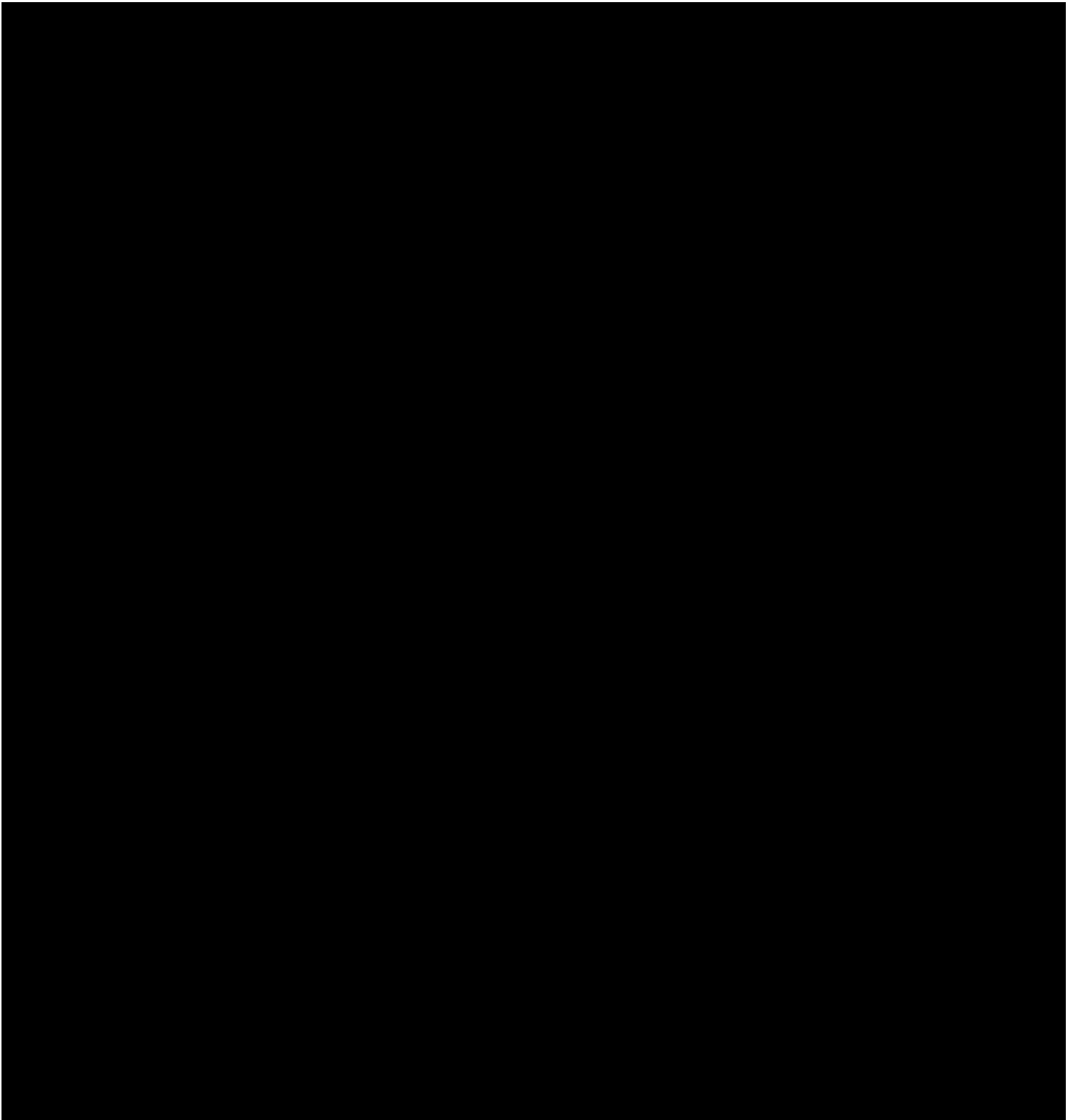
**NaBISCOP
USCIS FDNS-HB 602-001**

Security Check Requirements by Form Type & Quick Reference



**NaBISCOP
USCIS FDNS-HB 602-001**

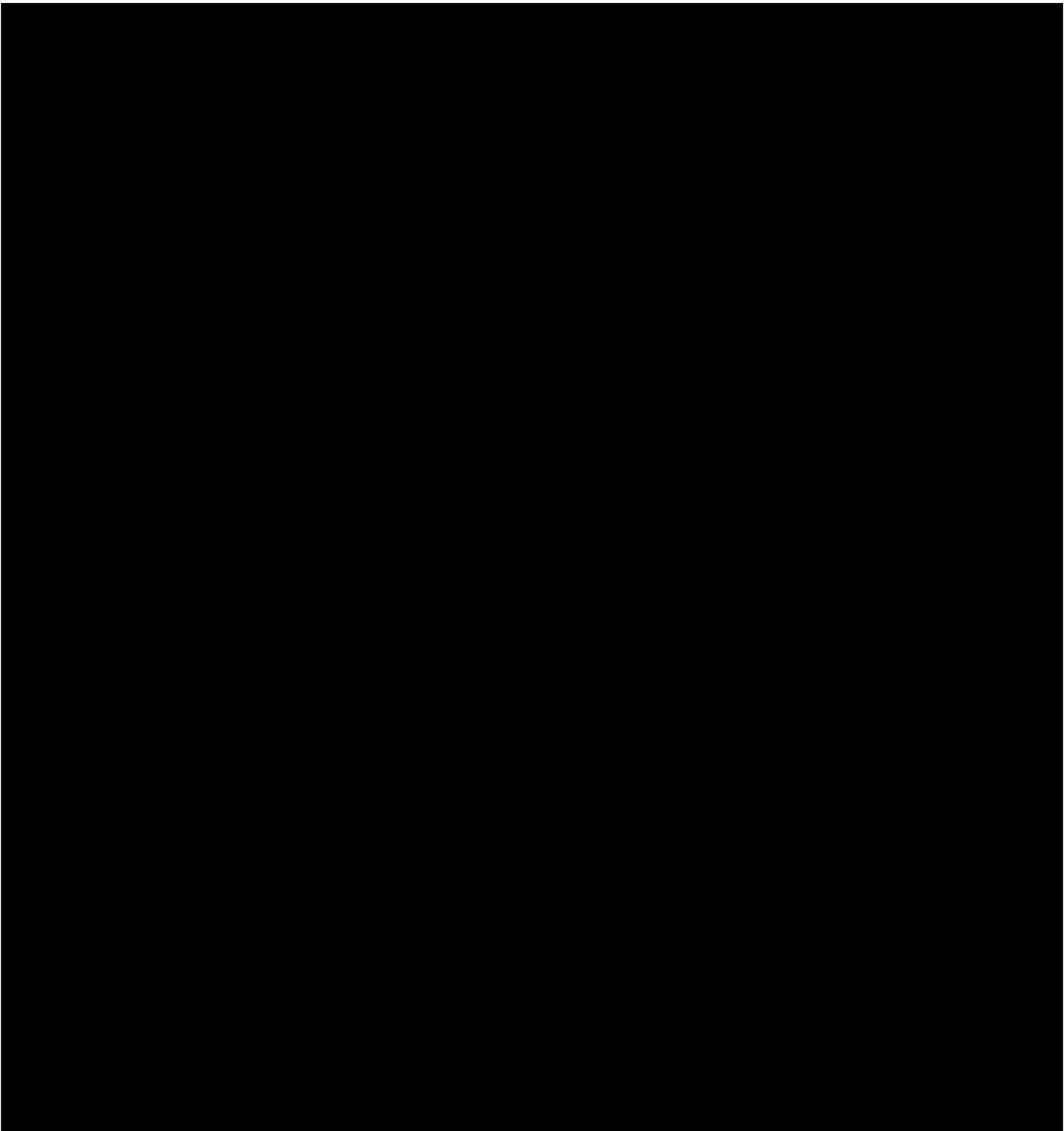
Appendix A



**NaBISCOP
USCIS FDNS-HB 602-001**

FOUO-LES

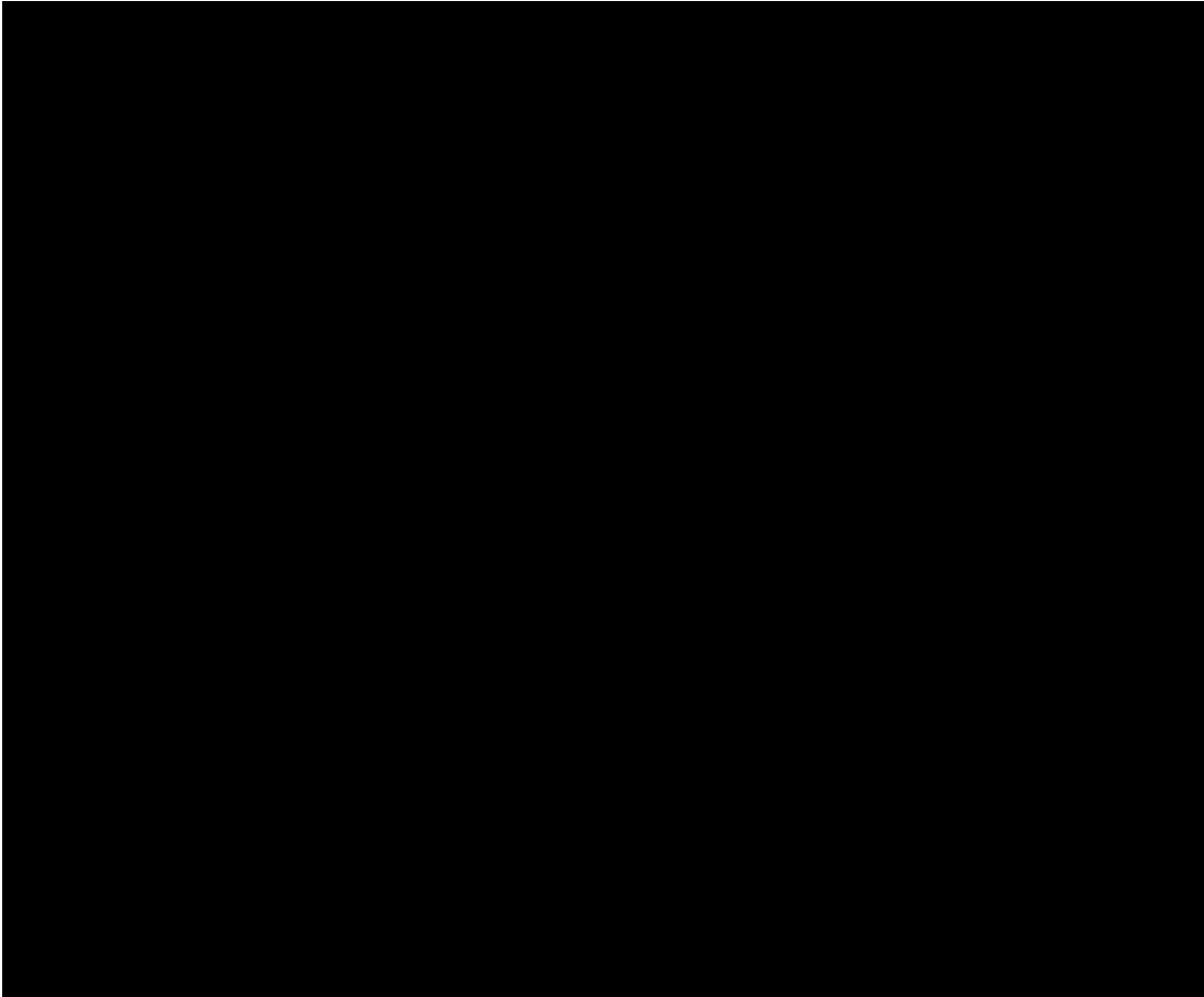
Appendix A



**NaBISCOP
USCIS FDNS-HB 602-001**

FOUO-LES

Appendix A



[Return to the Table of Contents](#)

[Return to List of Appendices](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

FOUO-LES

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	<u>Application to Replace Permanent Resident Card</u>
I-94	Arrival/Departure Record
I-95	Crewman's Landing Permit
I-102	<u>Application for Replacement/Initial Nonimmigrant Arrival-Departure Document</u>
I-129	<u>Petition for a Nonimmigrant Worker</u>
I-129F	<u>Petition for Alien Fiance(e)</u>
I-129S	<u>Nonimmigrant Petition Based on Blanket L Petition</u>
I-130	<u>Petition for Alien Relative</u>
I-131	<u>Application for Travel Document</u>
I-140	<u>Immigrant Petition for Alien Worker</u>
I-192	<u>Application for Advance Permission to Enter as a Nonimmigrant</u>
I-212	<u>Application for Permission to Reapply for Admission into the United States After Deportation or Removal</u>
I-290B	<u>Notice of Appeal or Motion</u>
I-360	<u>Petition for Amerasian, Widow(er), or Special Immigrant</u>
I-485	<u>Application to Register Permanent Residence or Adjust Status</u>
I-526	<u>Immigrant Petition by Alien Entrepreneur</u>
I-539	<u>Application To Extend/Change Nonimmigrant Status</u>
I-589	Application for Asylum and Withholding of Removal
I-590	Registration for Classification as Refugee
I-600	<u>Petition to Classify Orphan as an Immediate Relative</u>
I-600A	<u>Application for Advance Processing of Orphan Petition</u>
I-601	<u>Application for Waiver of Ground of Inadmissibility</u>
I-602	<u>Application By Refugee For Waiver of Grounds of Excludability</u>
I-612	<u>Application for Waiver of the Foreign Residence Requirement (under Section 212(e) of the Immigration and Nationality Act, as Amended)</u>
I-687	<u>Application for Status as a Temporary Resident Under Section 245A of the Immigration and Nationality Act</u>
I-690	<u>Application for Waiver of Grounds of Inadmissibility Under Sections 245A or 210 of the Immigration and Nationality Act</u>

NaBISCOP
USCIS FDNS-HB 602-001

Appendix B

Form Number	Form Name
I-694	<u>Notice of Appeal of Decision Under Sections 245A or 210 of the Immigration and Nationality Act</u>
I-698	<u>Application to Adjust Status from Temporary to Permanent Resident (Under Section 245A of Public Law 99-603)</u>
I-700	<u>Application for Temporary Resident Status as a Special Agricultural Worker</u>
I-730	<u>Refugee/Asylee Relative Petition</u>
I-751	<u>Petition to Remove the Conditions of Residence</u>
I-765	<u>Application for Employment Authorization</u>
I-800	<u>Petition to Classify Convention Adoptee as an Immediate Relative</u>
I-800A	<u>Application for Determination of Suitability to Adopt a Child from a Convention Country</u>
I-817	<u>Application for Family Unity Benefits</u>
I-821	<u>Application for Temporary Protected Status</u>
I-823	<u>Application - Inspections Facilitation Program</u>
I-824	<u>Application for Action on an Approved Application or Petition</u>
I-829	<u>Petition by Entrepreneur to Remove Conditions</u>
I-881	<u>Application for Suspension of Deportation or Special Rule Cancellation of Removal (Pursuant to Section 203 of Public Law 105-100 (NACARA))</u>
I-914	<u>Application for T Nonimmigrant Status</u>
I-914A	<u>Application for Immediate Family Member of T-1 Recipient</u>
I-918	<u>Petition for U Nonimmigrant Status</u>
N-300	<u>Application to File Declaration of Intention</u>
N-336	<u>Request for a Hearing on a Decision in Naturalization Proceedings (Under Section 336 of the INA)</u>
N-400	<u>Application for Naturalization</u>
N-470	<u>Application to Preserve Residence for Naturalization Purposes</u>
N-565	<u>Application for Replacement Naturalization/Citizenship Document</u>
N-600	<u>Application for Certificate of Citizenship</u>
N-600K	<u>Application for Citizenship and Issuance of Certificate under Section 322</u>
N-644	<u>Application for Posthumous Citizenship</u>

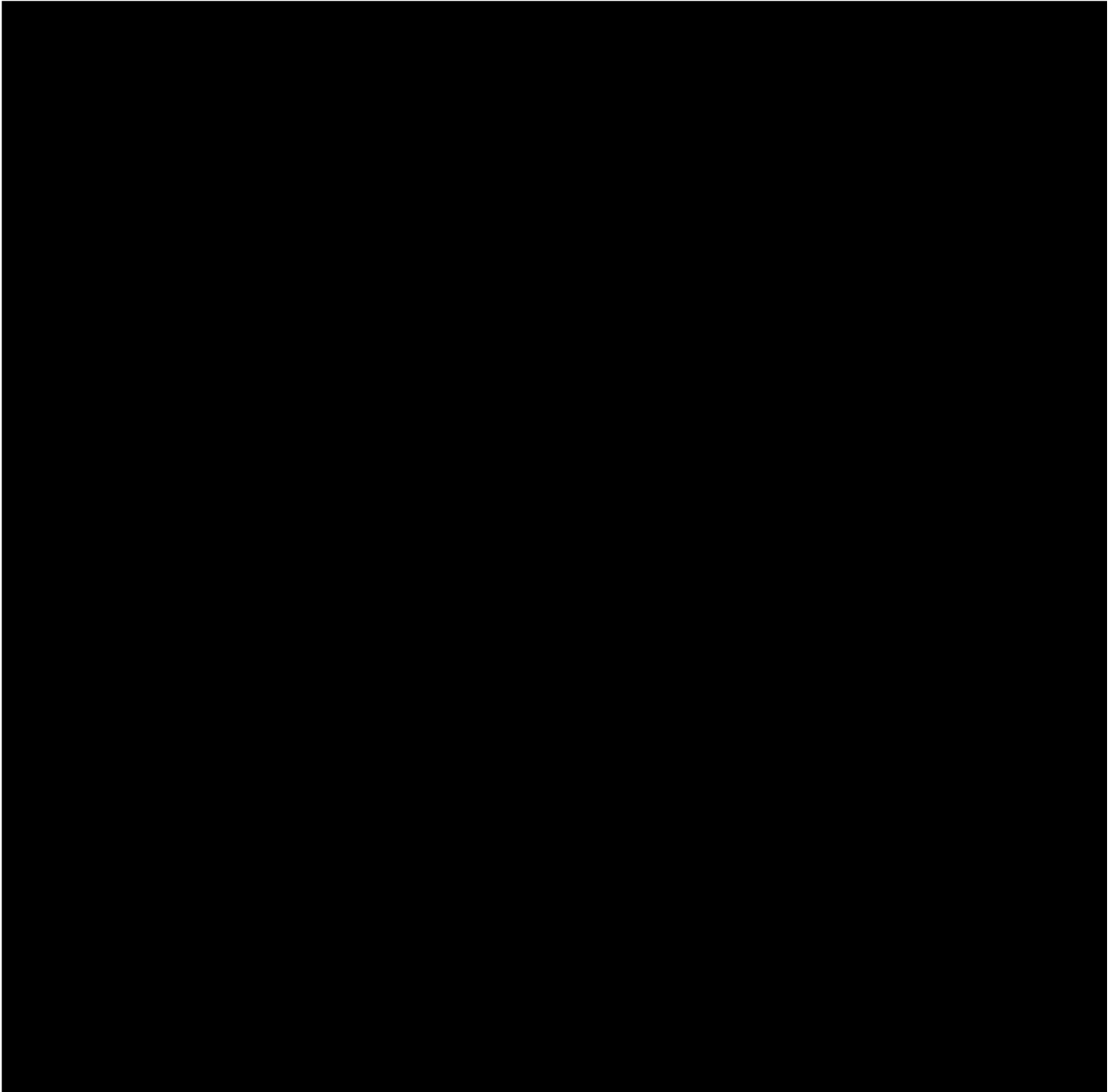
A list of USCIS applications can be found on the USCIS website, at <http://www.uscis.gov/forms>.

[Return to the Table of Contents](#)

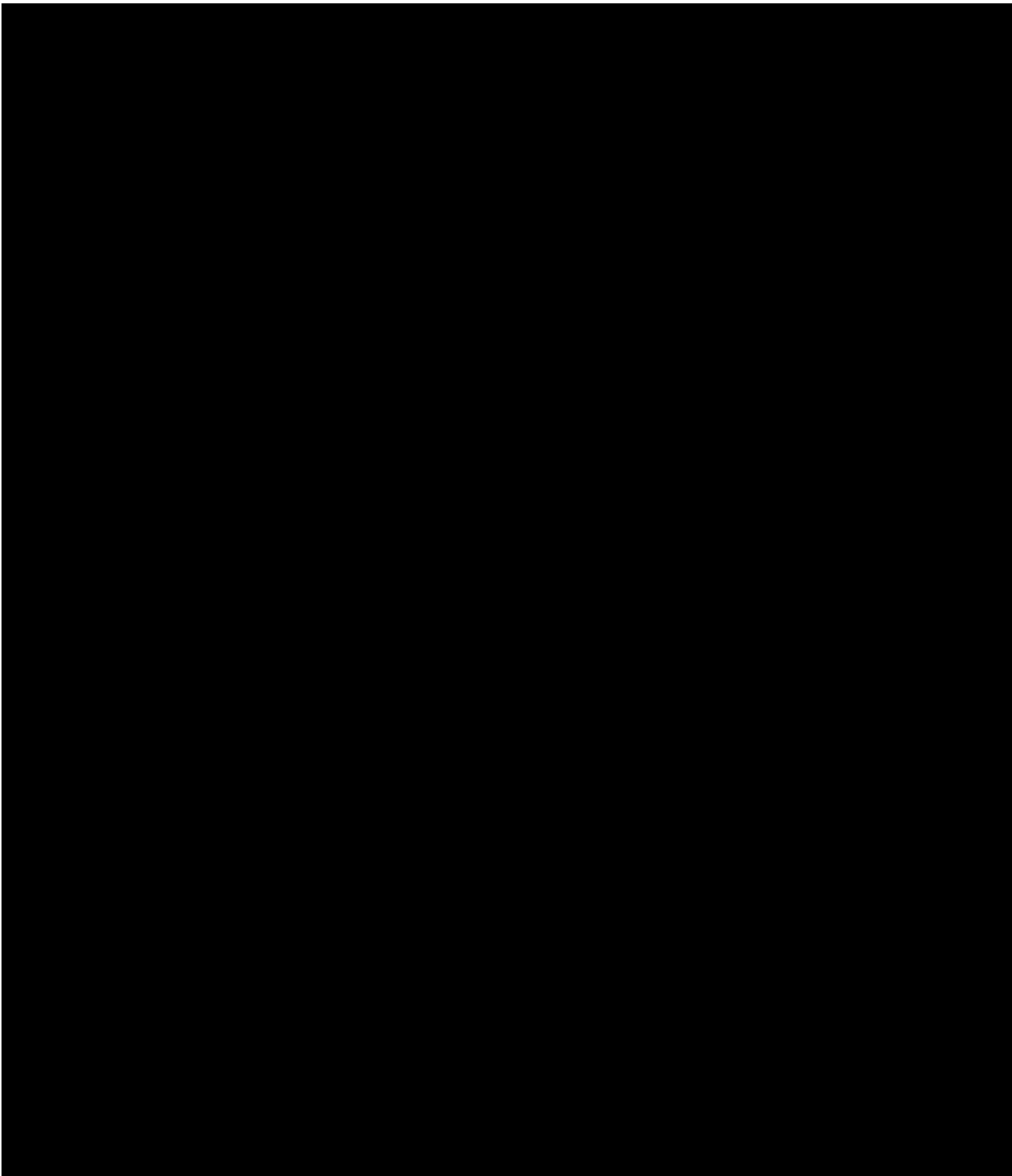
[Return to List of Appendices](#)

NaBISCOP
USCIS FDNS-HB 602-001

TECS Terms Indicating Possible NS Concerns

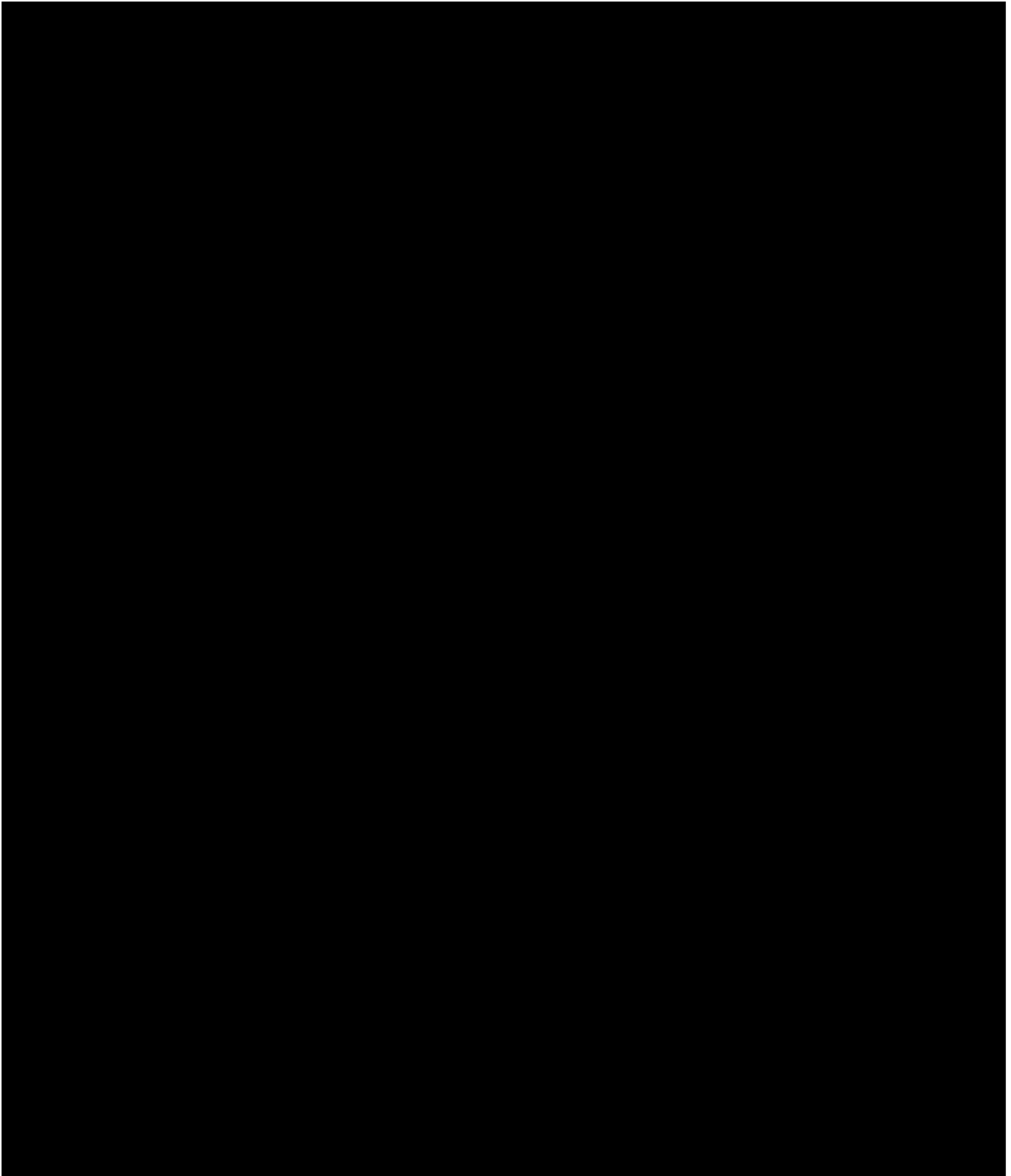


**NaBISCOP
USCIS FDNS-HB 602-001**



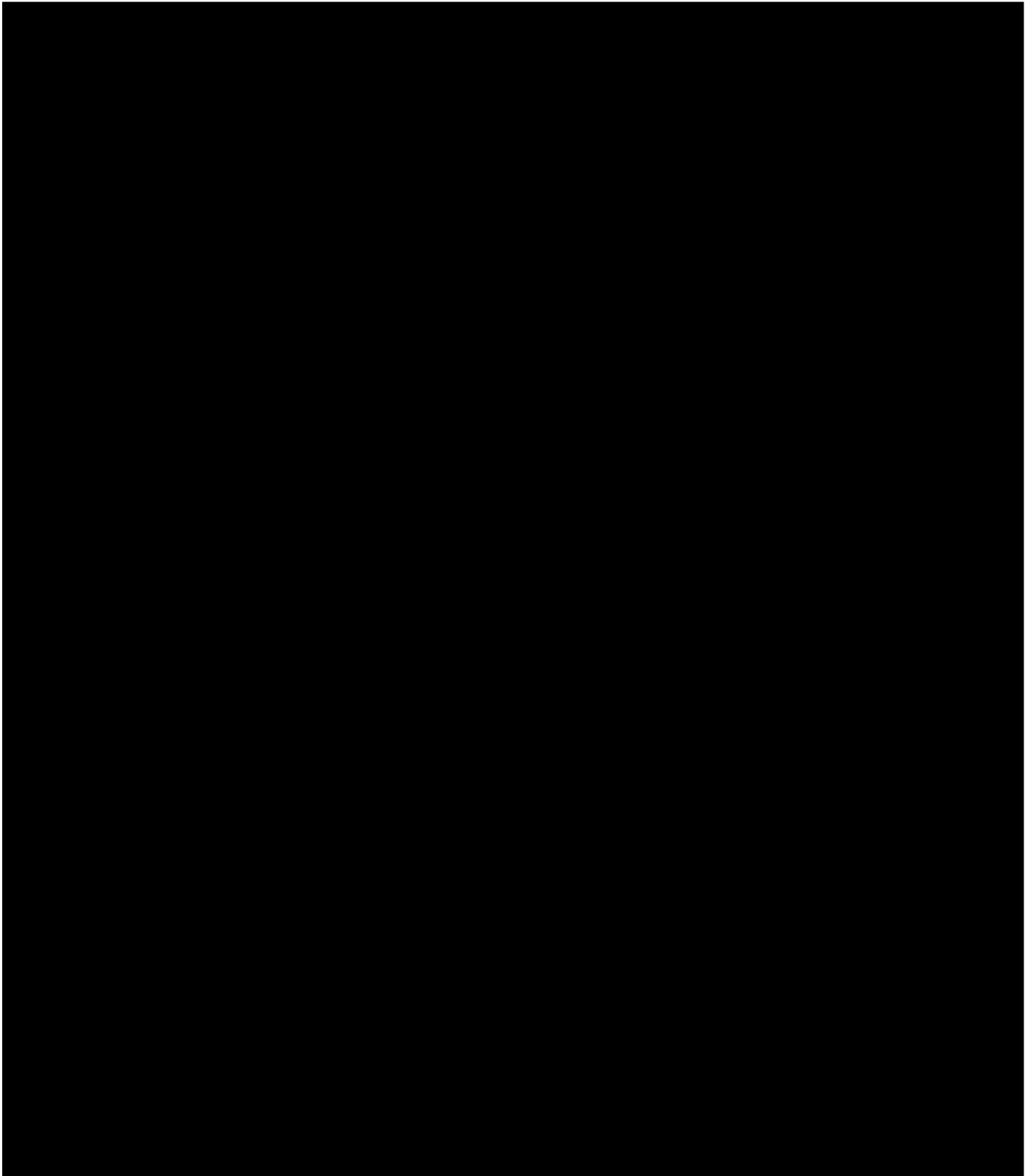
**NaBISCOP
USCIS FDNS-HB 602-001**

Appendix C



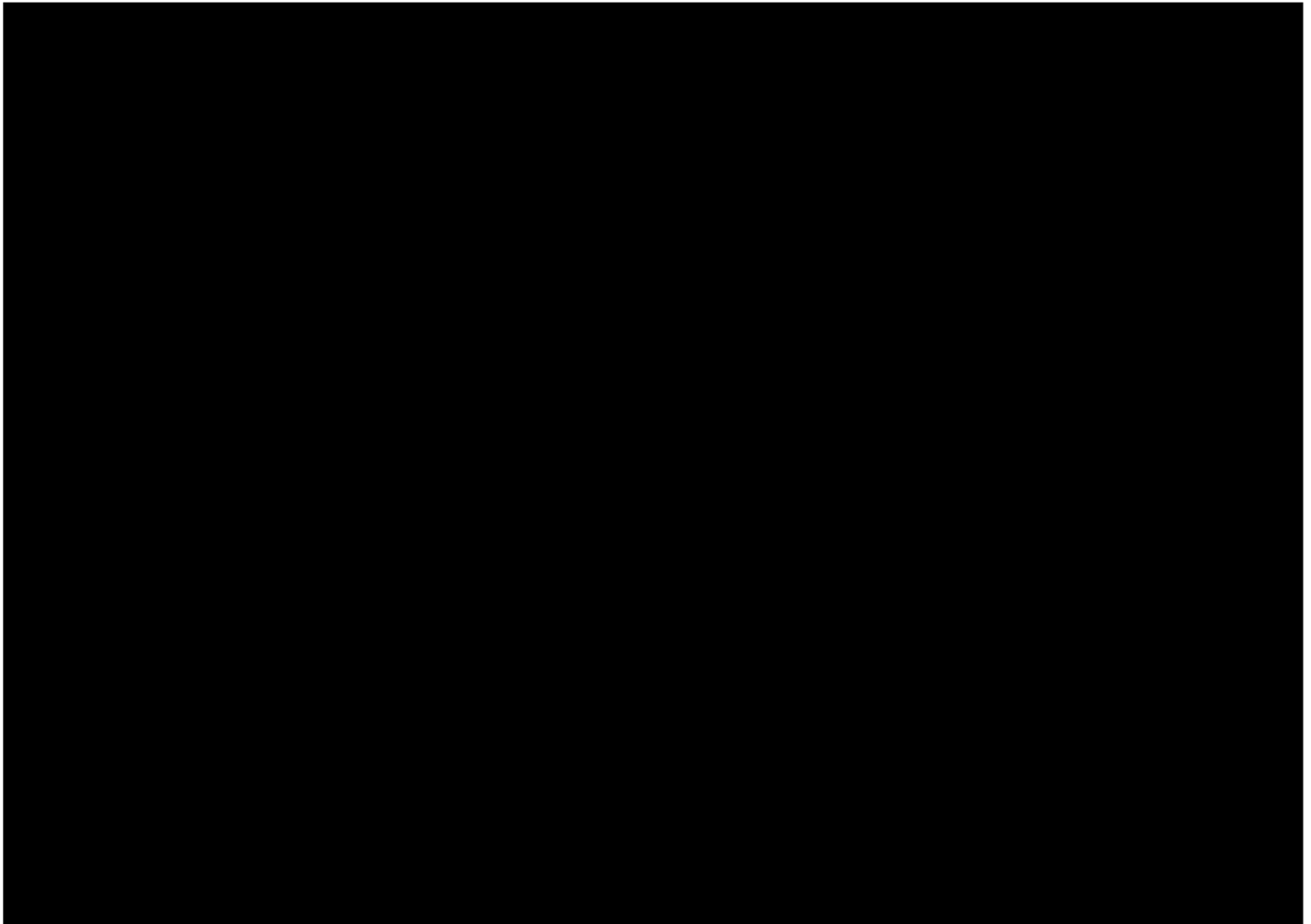
**NaBISCOP
USCIS FDNS-HB 602-001**

FOUO-LES



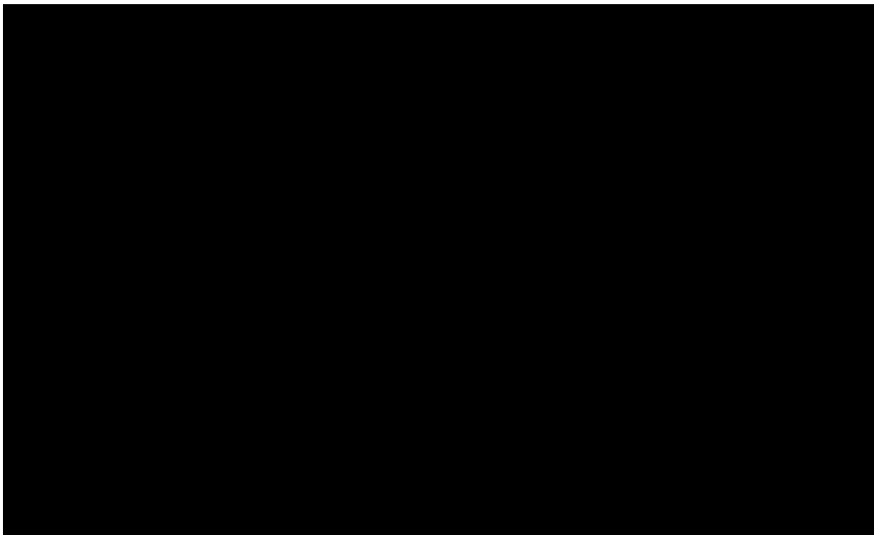
**NaBISCOP
USCIS FDNS-HB 602-001**

Appendix C

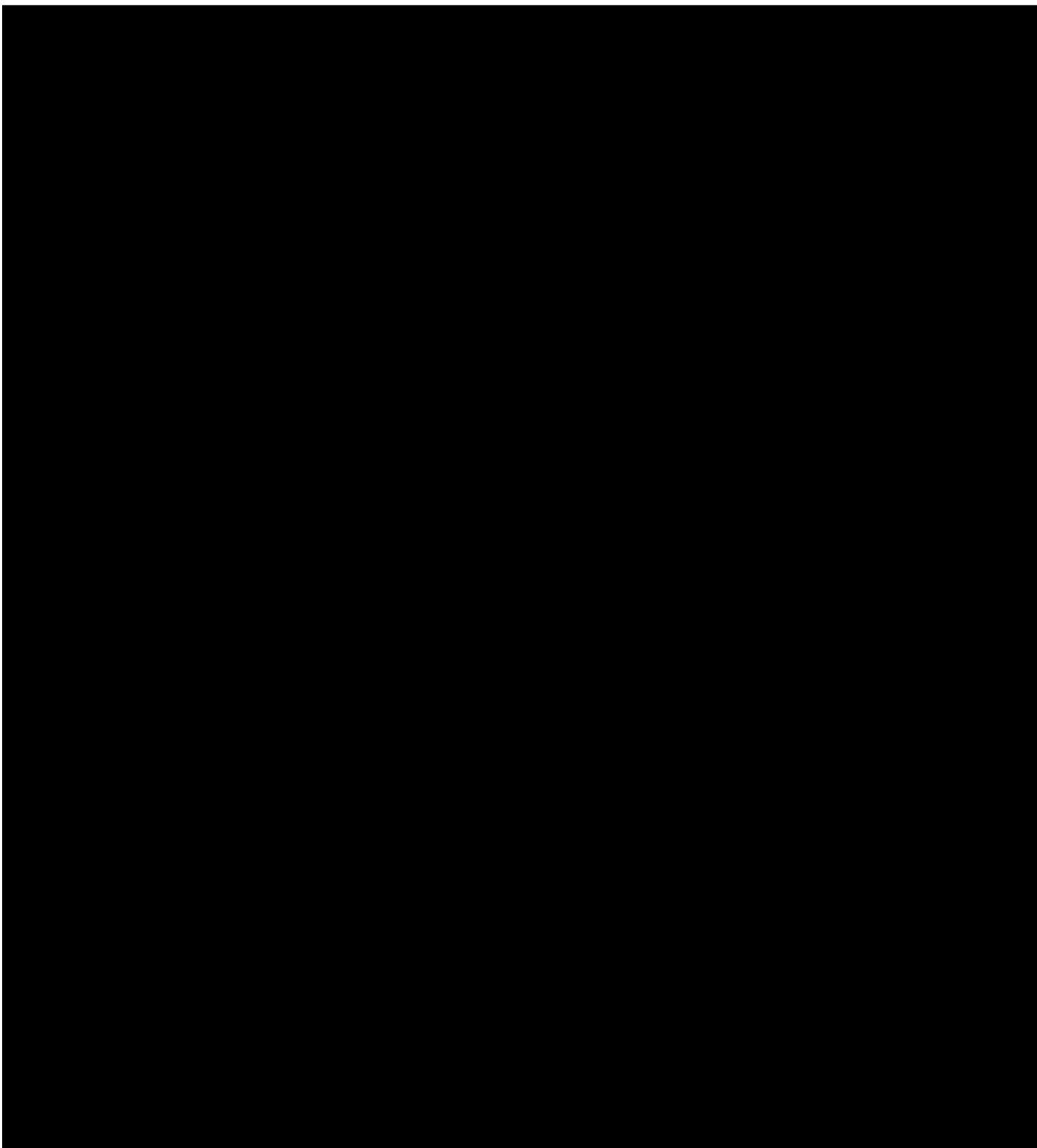


[Return to the Table of Contents](#)

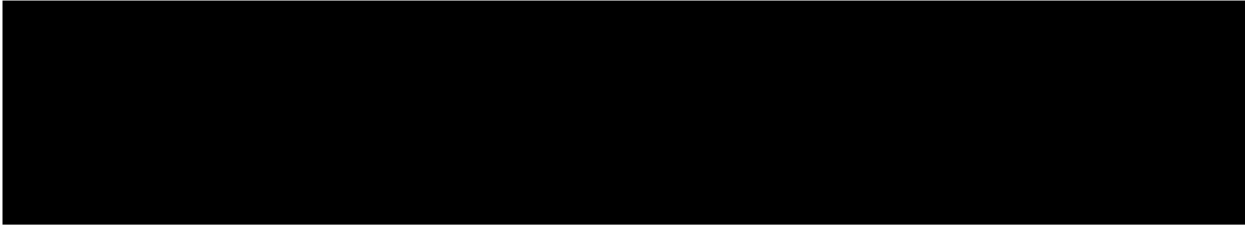
[Return to List of Appendices](#)



**NaBISCOP
USCIS FDNS-HB 602-001**



**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Table of Contents](#)

[Return to List of Appendices](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

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
BBSS	Benefits Biometric Support System
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
CIS	Central Index System

NaBISCOP
USCIS FDNS-HB 602-001

Appendix D

Acronym	Description
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
CRR	Case Resolution Record
DEA	Drug Enforcement Administration
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
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

NaBISCOP
USCIS FDNS-HB 602-001

Appendix D

Acronym	Description
HQ	Headquarters
HSTC	Human Smuggling and Trafficking Center
IAFIS	Integrated Automated Fingerprint Identification System (FBI)
IBIS	Interagency Border Inspection System
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
IRS	Intelligence Research Specialist
ISRS	Image Storage Retrieval System
KCC	Kentucky Consular Center (DOS)
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
NIIS	Nonimmigrant Information System
NLETS	National Law Enforcement Telecommunications System
NQP	Naturalization Quality Procedures
NNCP	National Name Check Program

NaBISCOP
USCIS FDNS-HB 602-001

Appendix D

Acronym	Description
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
NVC	National Visa Center (DOS)
OFL	Office of Fingerprint Liaison
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
POC	Point-of-Contact
RAD	Refugee Affairs Division
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
ROIQ	Record of IBIS Query
ROH	Records Operation Handbook
ROP	Record of Proceeding
RSO	Regional Security Offices
RTI	Referral to ICE

NaBISCOP
USCIS FDNS-HB 602-001

Appendix D

Acronym	Description
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)
TPS	Temporary Protected Status
TSA	Transportation Security Administration
UNI	FBI's Universal Index
USC	United States Citizen
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

NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

Appendix D

Acronym	Description
WMD	Weapons of Mass Destruction
WRAPS	DOS's Worldwide Refugee Admissions Processing System

[Return to the Table of Contents](#)

[Return to List of Appendices](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

FOUO-LES

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.
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

NaBISCOP
USCIS FDNS-HB 602-001

Appendix E

Term	Description
	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.
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.

NaBISCOP
USCIS FDNS-HB 602-001

Appendix E

Term	Description
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	Any decision of approval, denial, abandonment denial, revocation, reaffirmation, referral to immigration judge, or withdrawal of a benefit application/petition.
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.
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.

NaBISCOP
USCIS FDNS-HB 602-001

Appendix E

Term	Description
Interpol	International Criminal Police Organization, the world's largest international police organization. This organization facilitates cross-border police cooperation and supports and assists all organizations, authorities, and services whose mission is to prevent or combat international crime.
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 "P" for person and ending in a "B10," and should indicate that the individual is a "Known Terrorist" or "Suspected Terrorist."
National Security (NS) Concern	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 determination requires that the case be handled in accordance with CARRP policy outlined in the memorandum issued April 11, 2008.

NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

Appendix E

Term	Description
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.
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.
OSI	Office of Security and Integrity
Record Owner	The person who created or owns a given record, or the

NaBISCOP
USCIS FDNS-HB 602-001

FOUO-LES

Appendix E

Term	Description
	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.
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 is 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 SQ16 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.
Supporting Documentation	Documentation provided by the applicant, petitioner,

NaBISCOP
USCIS FDNS-HB 602-001

Appendix E

Term	Description
	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.
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 Record	A uniquely numbered and identifiable entry into TECS or NCIC made by a contributing agency.
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 List (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.

NaBISCOP
USCIS FDNS-HB 602-001

Appendix E

Term	Description
Terrorist Activity	Defined in 212(a)(3)(B)(iii) of the Act.
[Redacted Content]	
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

**NaBISCOP
USCIS FDNS-HB 602-001**

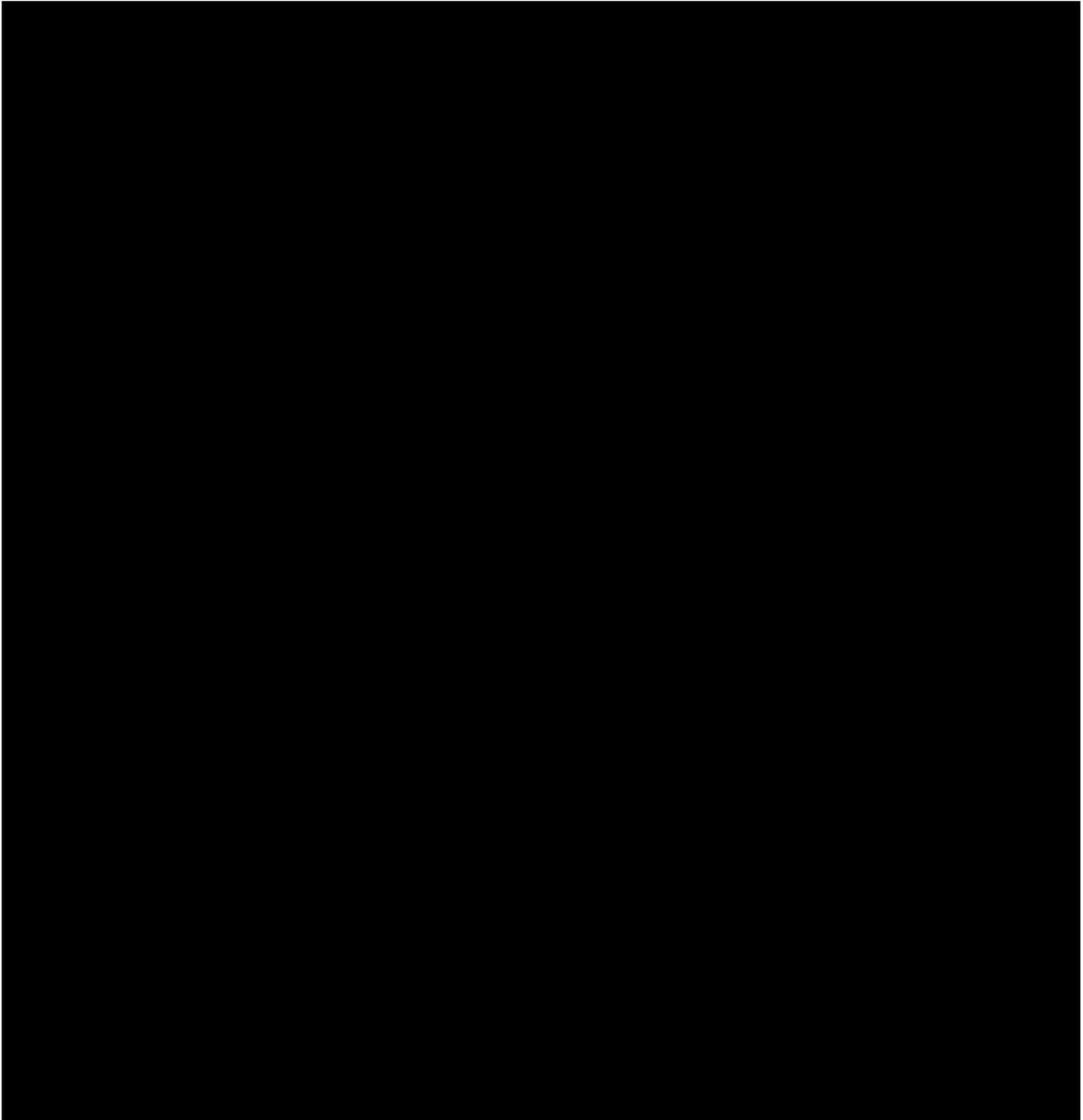
Term	Description
	that entered into a contract with USCIS to perform specified functions.
[Redacted]	
Work Folder	An unofficial file created at a local office for working purposes.

[Return to the Table of Contents](#)

[Return to List of Appendices](#)

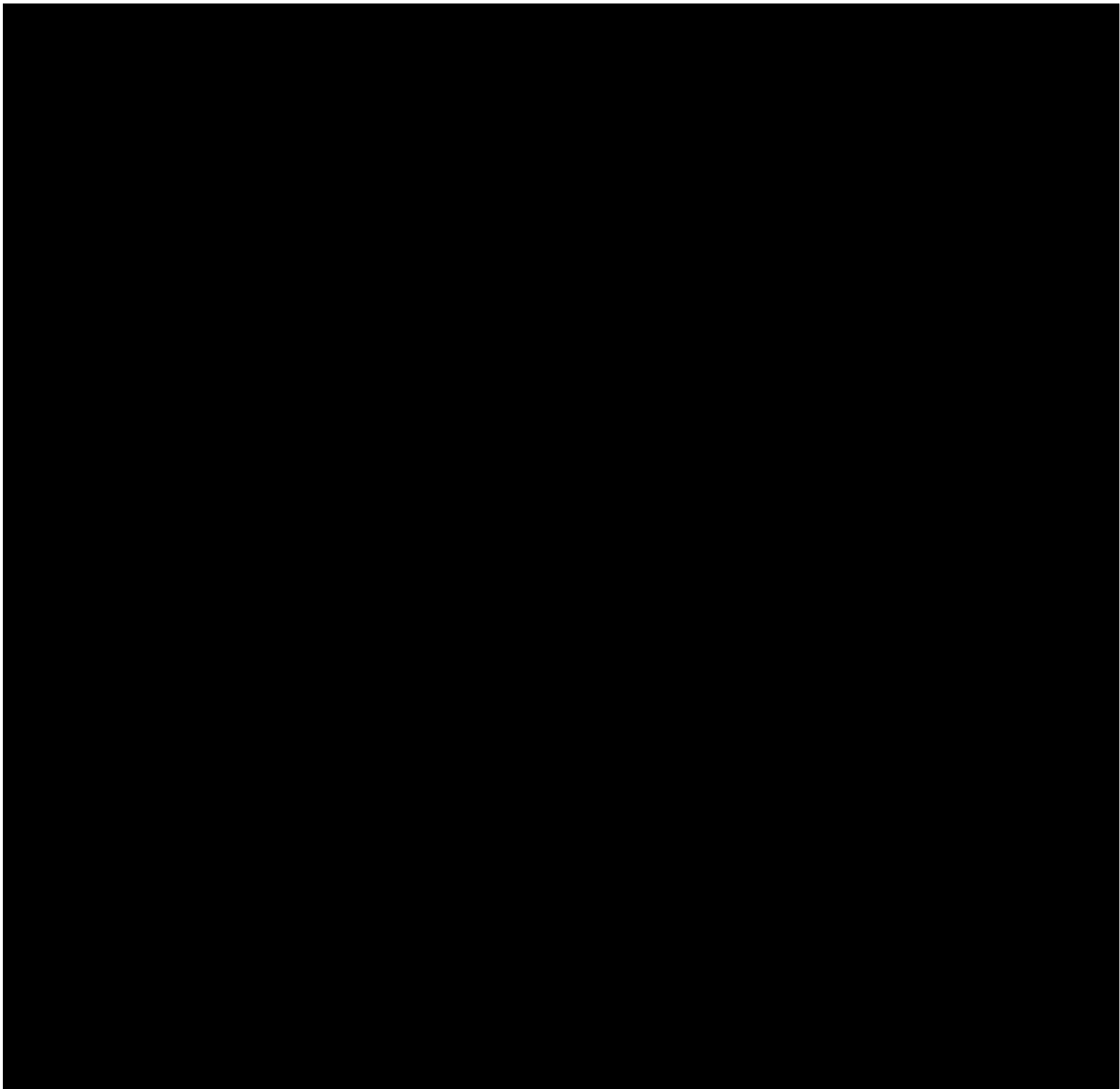
**NaBISCOP
USCIS FDNS-HB 602-001**

MS92

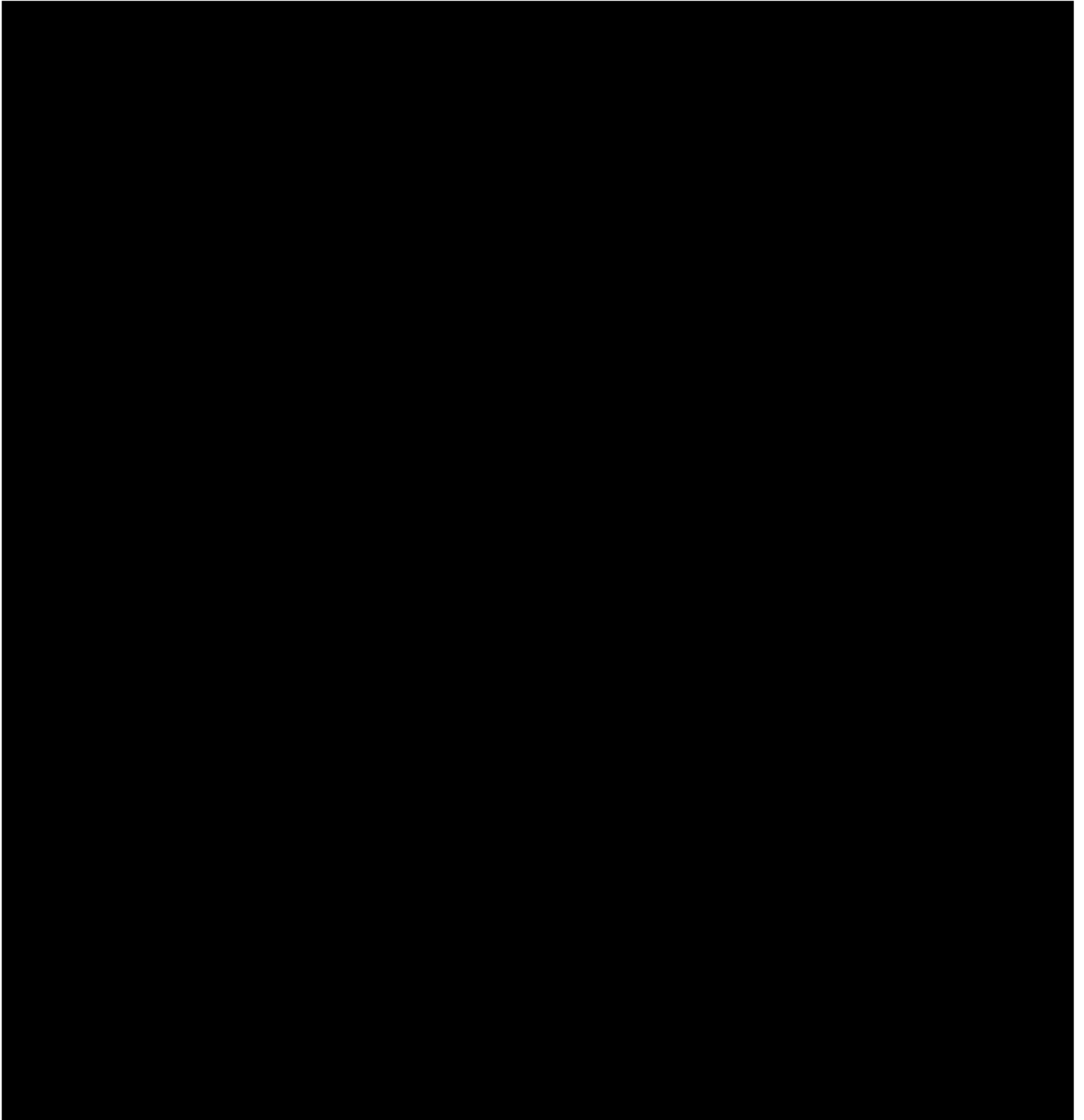


**NaBISCOP
USCIS FDNS-HB 602-001**

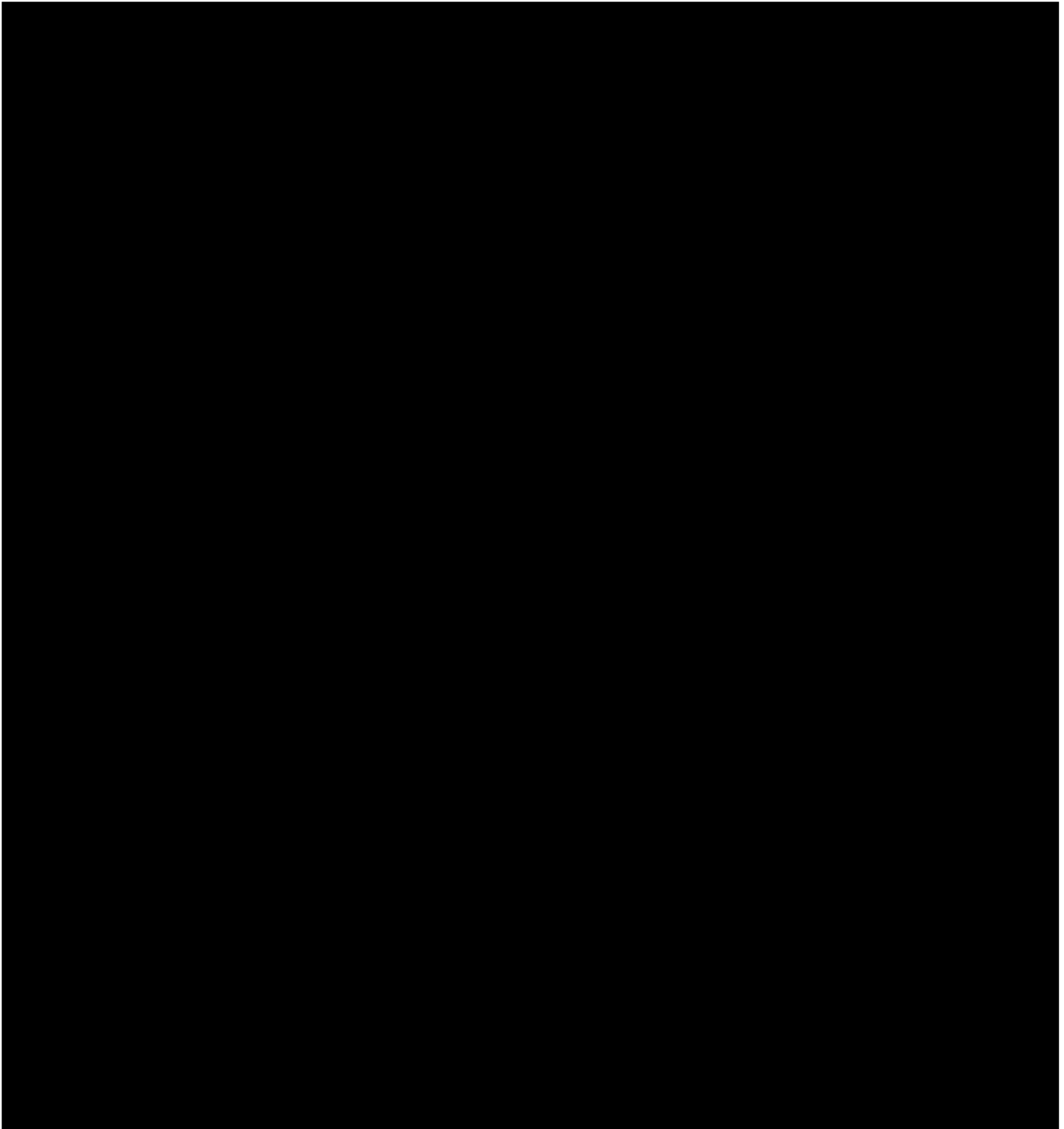
How to Enter a TECS Record?



NaBISCOP
USCIS FDNS-HB 602-001



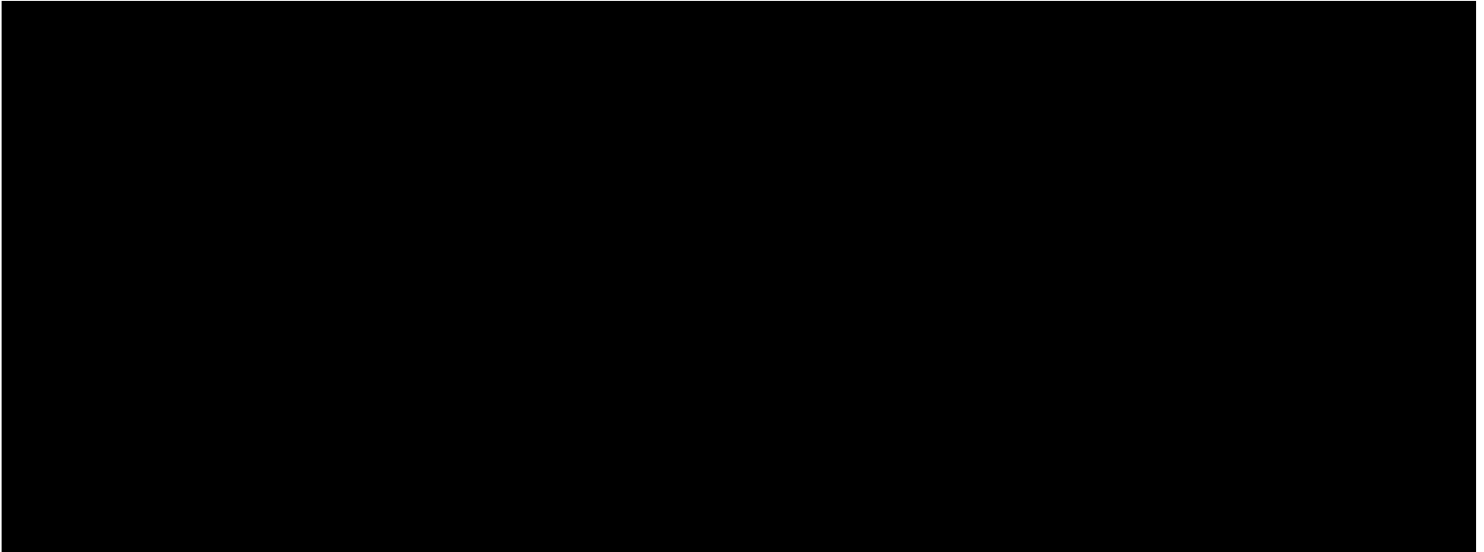
**NaBISCOP
USCIS FDNS-HB 602-001**



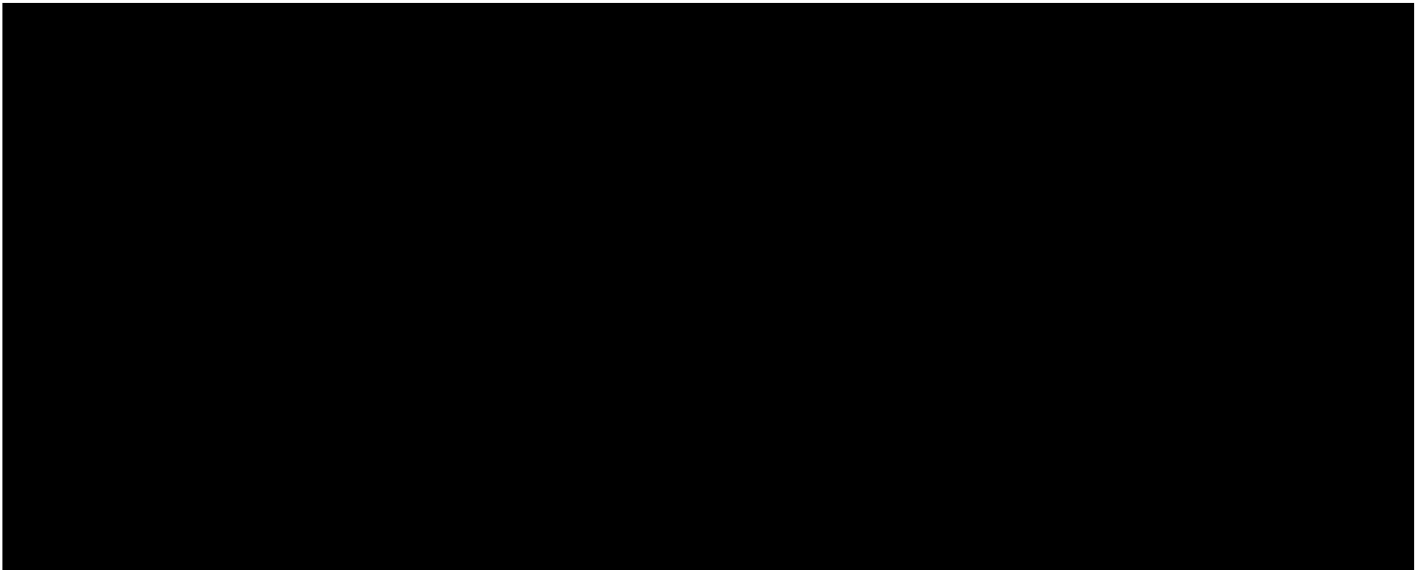
**NaBISCOP
USCIS FDNS-HB 602-001**



How to Link Subject Records



How to Delete Subject Records from TECS



**NaBISCOP
USCIS FDNS-HB 602-001**

Appendix F



[Return to the Table of Contents](#)

[Return to List of Appendices](#)

**NaBISCOP
USCIS FDNS-HB 602-001**

List of References

Cornell University Law School, Legal Information Institute U.S. Code Collection § 552a. Records Maintained on Individuals, (2009) (available at website http://www.law.cornell.edu/uscode/html/uscode05/usc_sec_05_00000552---a000-.html).

Department of Homeland Security, US-VISIT: Current Ports of Entry, (January 31, 2008) (available at website http://www.dhs.gov/files/programs/editorial_0685.shtm).

Department of Homeland Security Management Directive System, Safeguarding Sensitive But Unclassified (For Official Use Only) Information, (MD Number: 11042.1) (January 6, 2005) (available at

[REDACTED]

Donald Hawkins, Privacy Officer, Office of Security and Integrity, Chapter 8: Classified National Security Information (NSI), (September 10, 2009) [REDACTED]

[REDACTED]

Donald Hawkins, Privacy Officer, Office of Security and Integrity, Personally Identifiable Information (PII), (September 3, 2009) [REDACTED]

[REDACTED]

Donald Hawkins, Privacy Officer, Office of Security and Integrity, Safeguarding Classified and Sensitive Unclassified Information, (July 31, 2008) [REDACTED]

[REDACTED]

Donald Hawkins, Privacy Officer, Office of Security and Integrity, Significant Incident Reports (SIRs), (September 3, 2009) [REDACTED]

[REDACTED]

INTERPOL, INTERPOL Notices, (September 3, 2009) (available at website <http://www.interpol.int/Public/Notices/default.asp>).

Memorandum from Donald K. Hawkins, Chief Privacy Officer, to all USCIS employees and contractors, USCIS Policy Regarding Personally Identifiable Information, (July 8, 2008) (available at

[REDACTED]

**NaBISCOP
USCIS FDNS-HB 602-001**

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, (DOMO 70/2.2) (June 17, 2008) (available at [REDACTED])

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, (HQ 70/1-P) (September 24, 2008) (available at [REDACTED])

Memorandum from Donald Neufeld, Acting Associate Director, Office of Domestic Operations, to Field Leadership, National Security Adjudication and Reporting Requirements – Update, (HQ 70/23 & 70/28.1) (February 9, 2009) (available at [REDACTED])

[REDACTED]

Memorandum from Joseph E. Langlois, Chief, Asylum Division, to all Asylum Office Personnel, Issuance of Updated IBIS and US-VISIT Procedures and Security Checklist, (HQRAIO 120/9.3a) (January 26, 2007) (available at [REDACTED])

Memorandum from Joseph E. Langlois, Chief, Asylum Division, to Asylum Office Directors and Deputy Directors, Disclosure of Consular Affairs Visa Data in Asylum Adjudications, (HQRAIO 50/18.5.9) (January 24, 2008) (available at [REDACTED])

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, (HQ FDNS 70/2.1) (December 14, 2004) (available at [REDACTED])

Memorandum from Michael Aytes, Associate Director, Domestic Operations, to all

NaBISCOP
USCIS FDNS-HB 602-001

Appendix G

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) (available at [REDACTED])

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, (HQOPRD 70/6.2.11) (July 21, 2006) (available at [REDACTED])

[REDACTED] in
[REDACTED] nd

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, (HODOMO 70/1-P) (February 8, 2007) (available at [REDACTED])

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, Disposition of Cases Involving Removable Aliens, (Subject Code: 70/1-P) (July 11, 2006) (available at [REDACTED])

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, (HQFDNS 180/8.1-P) (July 5, 2006) (available at [REDACTED])

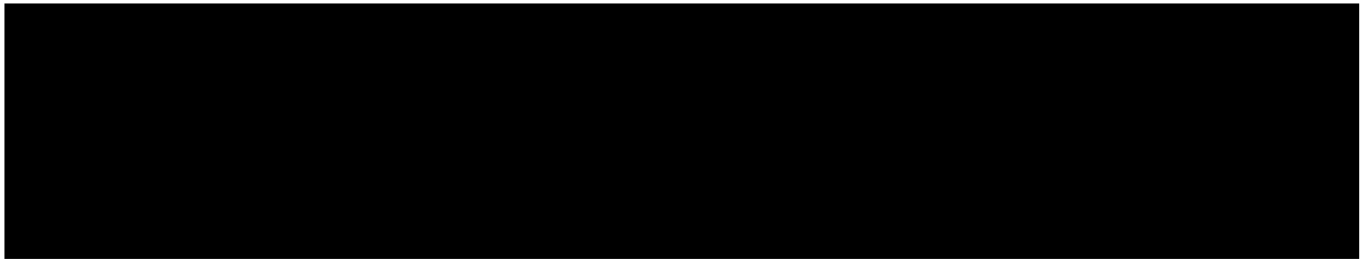
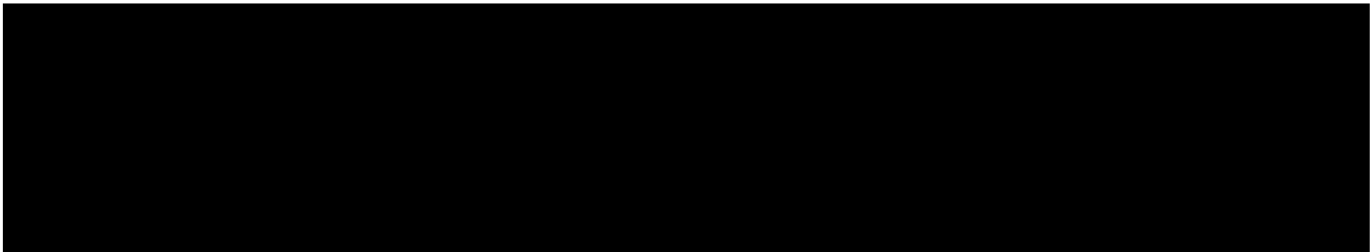
**NaBISCOPE
USCIS FDNS-HB 602-001**



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) (available at



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, (HQOPRD 70/6.22/04) (April 2, 2004) (available



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, (2007-2) (June 4, 2007) (available at



NaBISCOP
USCIS FDNS-HB 602-001

Appendix G

United States Citizenship and Immigration Services, Asylum Division, Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants, (June 3, 2005) (available at [REDACTED])

United States Citizenship and Immigration Services, Domestic Operations, Standard Operating Procedure Form I-862, Notice to Appear, (Septem 8, 2006) (available at [REDACTED])

United States Citizenship and Immigration Services, Form G-639, Freedom of Information Act/Privacy Act Request, (September 1, 2009) (available at <http://www.uscis.gov/G-639>).

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) (available at website [REDACTED])

United States Citizenship and Immigration Services, Office of Fraud Detection and National Security, Fraud Detection Standard Operating Procedures, (June 18, 2009) (available at [REDACTED])

United States Citizenship and Immigration Services, Office of Fraud Detection and National Security, IBIS Standard Operating Procedure, (March 1, 2006) (available at [REDACTED])

United States Citizenship and Immigration Services, Office of Fraud Detection and National Security, Attachment A – Guidance for Identifying National Security Concerns, (April 11, 2008) (available at [REDACTED])

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) (available at website http://www.usdoj.gov/eoir/ogc/SantillanPadilla/Final_agreement.santillan.padilla_settlement_070208.pdf).

NaBISCOP
USCIS FDNS-HB 602-001

Appendix G

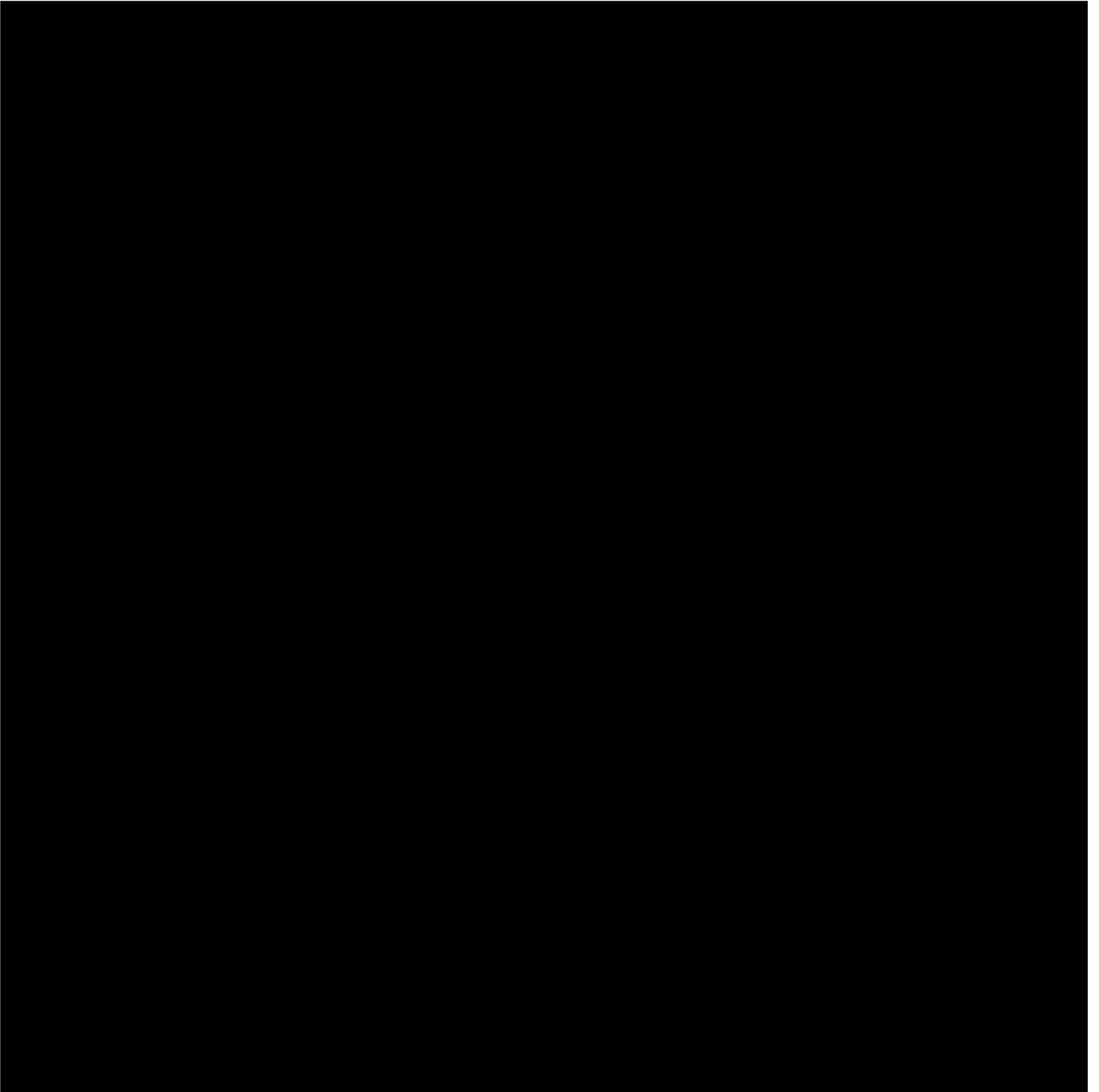
[Return to the Table of Contents](#)

[Return to List of Appendices](#)

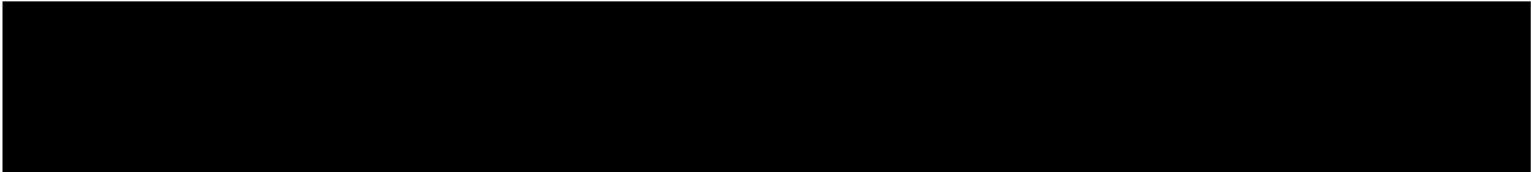
**NaBISCOP
USCIS FDNS-HB 602-001**

FOUO-LES

Notice to INTERPOL



**NaBISCOP
USCIS FDNS-HB 602-001**

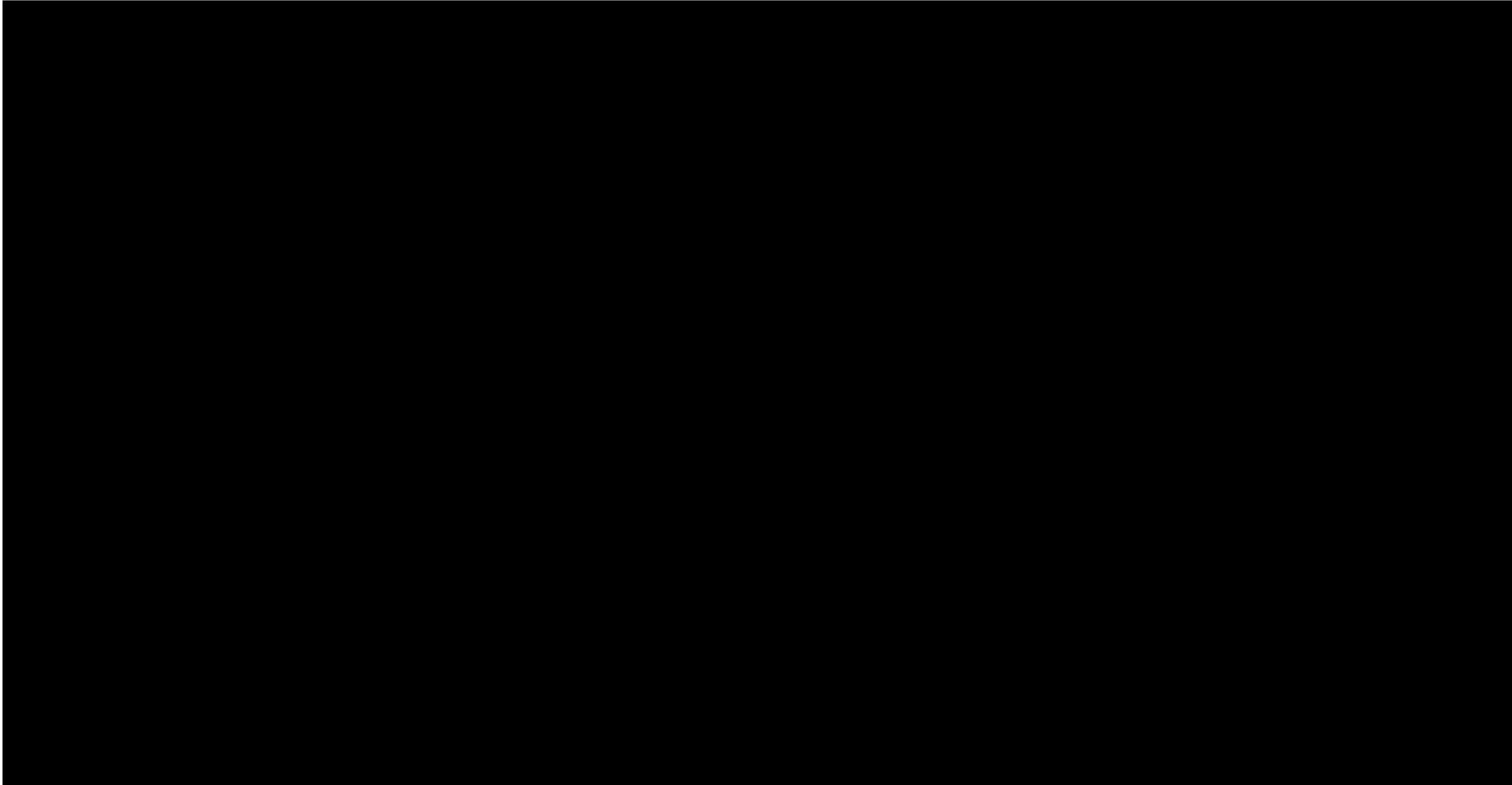


[Return to the Table of Contents](#)

[Return to List of Appendices](#)

NaBISCOP
USCIS FDNS-HB 602-001

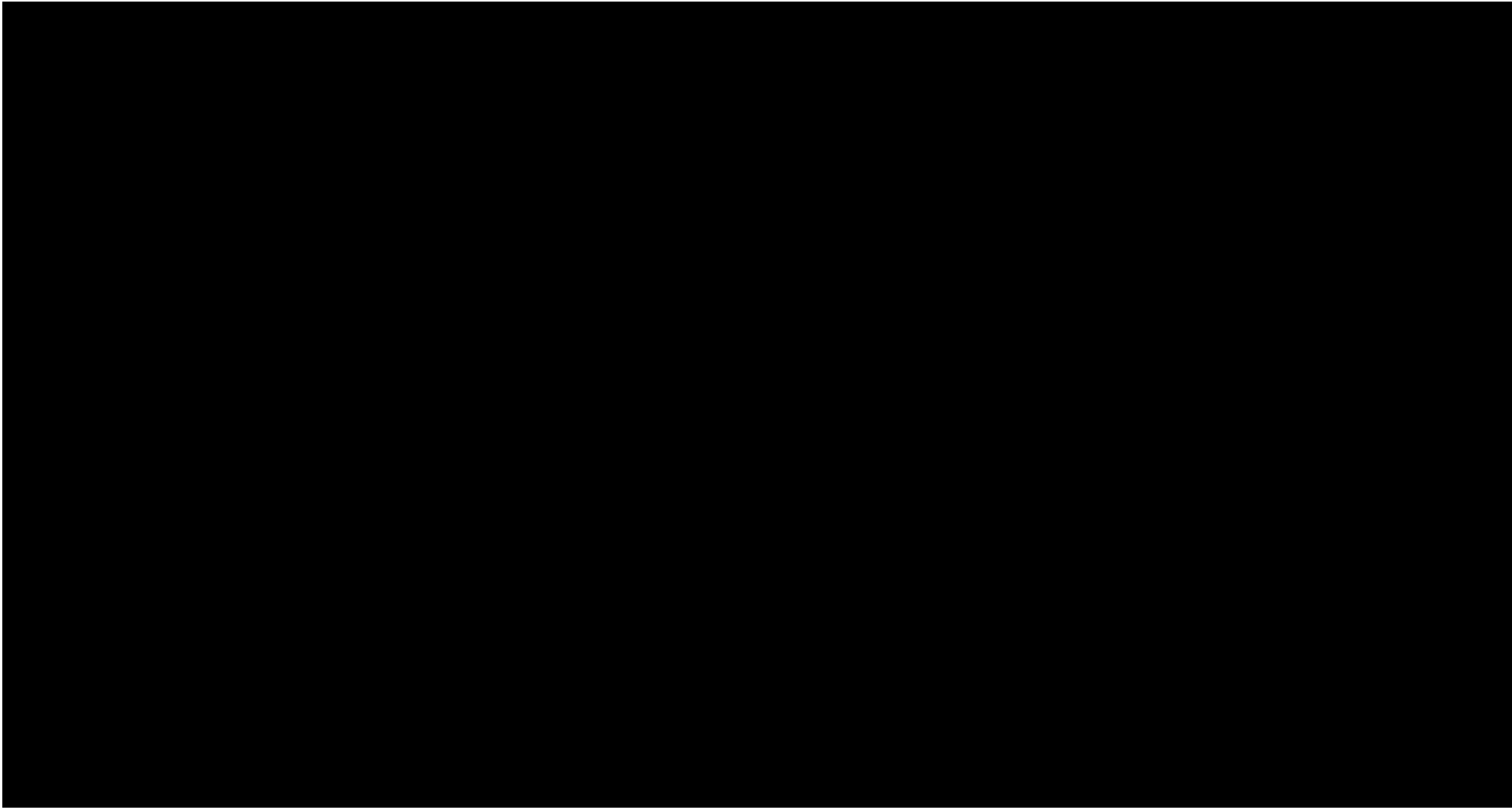
Quick Reference



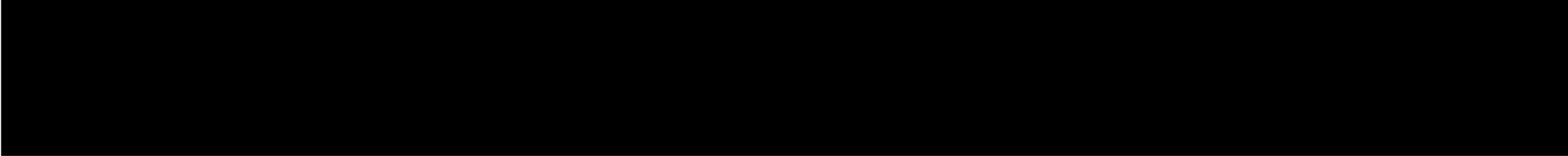
**NaBISCOP
USCIS FDNS-HB 602-001**

187

FOUO-LES



**NaBISCOP
USCIS FDNS-HB 602-001**

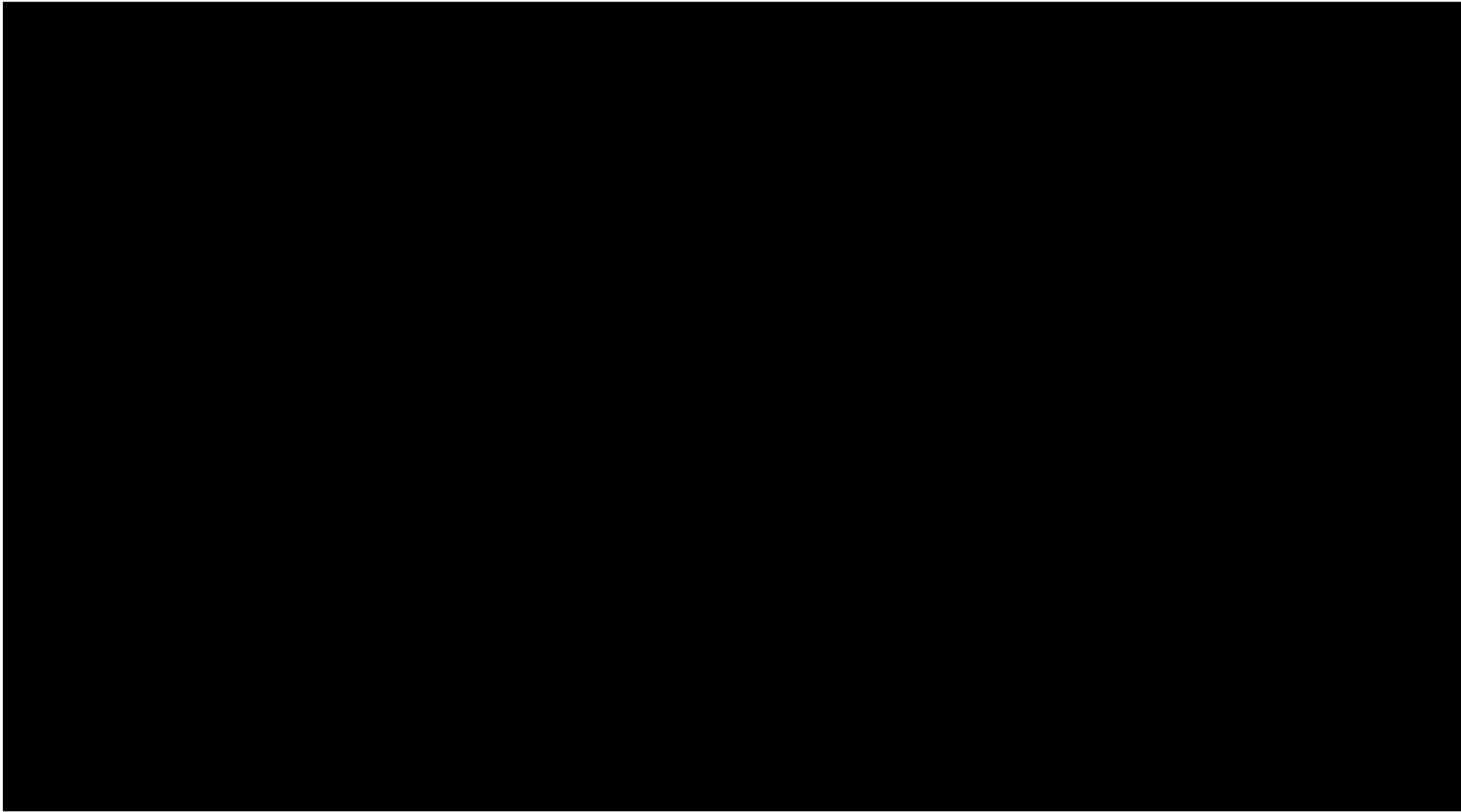


[Return to the Table of Contents](#)
[Return to List of Appendices](#)

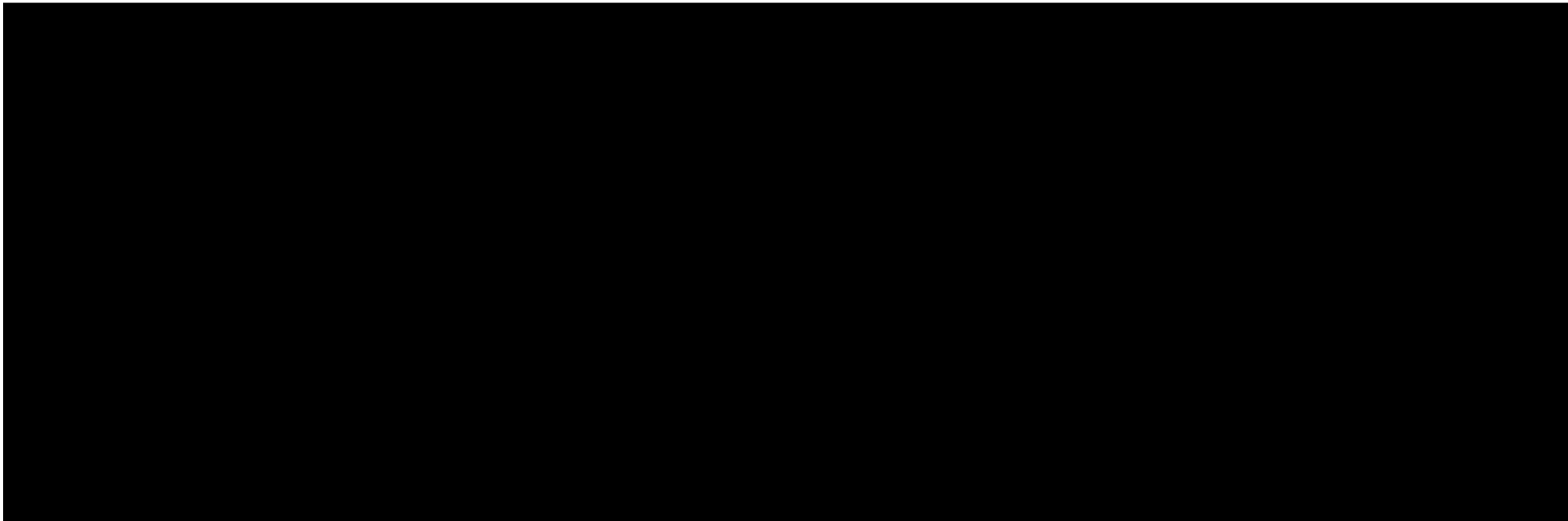
FBI Name Check



NaBISCOP
USCIS FDNS-HB 602-001



**NaBISCOP
USCIS FDNS-HB 602-001**



[Return to the Table of Contents](#)

[Return to List of Appendices](#)

NaBISCOP
USCIS FDNS-HB 602-001