

TABLE OF CONTENTS

SECTION I: Introduction	1
Purpose of SOP	2
About the SOP	2
About this Section	2
Scope of the SOP	2
About IBIS	3
About TECS	3
About NCIC	4
USCIS Policy on IBIS Usage	4
USCIS Policy on IBIS	
Equipment and Technical Assistance	5
Program Development and Training	5
Third Agency Rule	6
Privacy Act	7
SECTION II:	
Operational Guidelines	9
About this Section	10
Who Performs IBIS Queries	10
Types of IBIS Queries	10
When to Perform IBIS Queries	11
Who to Query	12
Documentation of IBIS Query	14
Annotating the ROIQ	15

SECTION III: SQ-11	17
About this Section	18
SQ-11 Query Objective	18
Conducting an SQ-11 Query	18
SQ-11 Search Criteria	19
Name and DOB Rules	20
SECTION IV: Batch Query	27
About this Section	28
Batch Query Objective	28
When Batch Queries are Performed	28
Batch Query Process	29
SECTION V: SQ-16	30
About this Section	31
SQ-16 Query Objective	31
Conducting an SQ-16 Query	31
SQ-16 Search Criteria	31
SECTION VI:	
Center Resolution Process	32
About this Section	33
Purpose of ITU	33
Purpose of FDU	33
Purpose of FOCUS	33
Hit Paradigm	34
Resolution Process	34
Additional Queries	40
IBIS Stamp	40
Record of Proceeding (ROP)	41
Explanation of Completed ROIQ	43

SECTION VII:

Field Resolution Process	44
About this Section	45
Hit Paradigm	45
Resolution Process	46
Additional Queries	49
Record of Proceeding (ROP)	50
Explanation of Completed ROIQ	52

SECTION VIII:

FDU Resolution Process	53
About this Section	54
Hit Paradigm	54
Resolution Process	55
Resolution Memo	60
Return to Work Flow	61
Record of Proceeding (ROP)	61

GLOSSARY	62
-----------------	----

APPENDIX	74
-----------------	----

APPENDIX A:	Guide to IBIS Hits	75
APPENDIX B:	Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants	86
APPENDIX C:	Reading an NCIC Query Response	93
APPENDIX D:	DACS NCIC Offense Codes	95
APPENDIX E:	DACS Charge Codes	117
APPENDIX F:	DACS System Codes	133
APPENDIX G:	DOS Refusal Codes	161
APPENDIX H:	HQ Policy Memorandum: <i>Accessing National Crime Information Center Interstate Identification Index (NCIC III) Data</i> (June 17, 2005)	

APPENDIX I:	IBIS NN16 User Agreement	170
	HQ Policy Memorandum: <i>CLARIFICATION and MODIFICATION of New Resolution Process for IBIS National Security/Terrorist Related Positive Results</i> (March 29, 2005)	174

APPENDIX J:	<div style="border: 1px solid black; width: 450px; height: 40px; margin: 5px 0;"></div>	(b)(5) 179 (b)(7)(e)
-------------	---	-------------------------

APPENDIX K:	HQ Policy Memorandum: <i>Discontinuation of IBIS Alias Name Checks for Petitions and Applications When the Beneficiary and Dependents are Not Physically Present in the United States</i> (March 23, 2005).....	182
APPENDIX L:	HQ Policy Memorandum: <i>Safeguarding Sensitive but Classified Information</i> (January 27, 2005)	
	DHS Management Directive System MD Number: 11042.1: <i>Safeguarding Sensitive but Unclassified (For Official Use Only) Information</i> (January 6, 2005)	
	DHS Policy Memorandum: <i>Management Directive 11041.1: Safeguarding Sensitive but Unclassified (For Official Use Only) Information</i> (January 11, 2005)	186
APPENDIX M:	HQ Policy Memorandum: <i>New Resolution Process for IBIS National Security/Terrorism Related Positive Results</i> (November 29, 2004)	
	IBIS National Security Case Resolution Request	
	IBIS National Security Record	
	IBIS National Security Notification.....	204
APPENDIX N:	HQ Policy Memorandum: <i>Required Security Checks</i> (August 4, 2004).....	212
APPENDIX O:	HQ Policy Memorandum: <i>New National Security Related IBIS Procedures</i> (May 21, 2004).....	215
APPENDIX P:	HQ Policy Memorandum: <i>IBIS Technical Support Guidelines at POEs</i> (March 2, 2001).....	219
APPENDIX Q:	Memorandum of Understanding Between the U.S. Customs Service and the Immigration and Naturalization Service for Use of Treasury Enforcement Communications System (TECS) (July 9, 1993).....	223
APPENDIX R:	Interconnection Security Agreement Between Immigration and Naturalization Service and United States Customs Service: <i>INS Use of IBIS (TECS) Workstation with Internet Access</i> (October 2002).....	232
APPENDIX S:	Codes for TECS User Agencies and Sub Agencies (February 16, 2006)	240

TABLE OF FIGURES

FIGURE II-1: WHO TO QUERY CHART	13
FIGURE II-2: ROIQ	16
FIGURE VI-1: COMPLETED ROIQ (Center)	41
FIGURE VII-1: COMPLETED ROIQ (Field)	51

SECTION I:

Introduction

Introduction, Continued

Section I: Introduction

Purpose of the SOP The purpose of the Interagency Border Inspection System (IBIS) Standard Operating Procedure (SOP) is to establish standards for United States Citizenship and Immigration Services (USCIS) employees and contractors specific to running IBIS queries and resolving relating hits.

About the SOP The IBIS SOP is created for USCIS personnel working with benefit petitions and applications, who have the required security clearances for IBIS, and who have been trained, certified, and currently conduct IBIS queries as part of the adjudicative process.

About this Section In this section, you will find information about the following topics:

- Scope of the SOP
- About IBIS
- About TECS
- About NCIC
- USCIS Policy on IBIS Usage
- USCIS Policy on IBIS Equipment and Technical Assistance
- Program Development and Training
- Third Agency Rule
- Privacy Act

Scope of the SOP This SOP supersedes ALL prior guidance for IBIS purposes, including local policies and procedures, e-mail guidance, and instructions otherwise provided unless the guidance is specifically cited within the body of this SOP. This SOP covers IBIS processing for Service Centers, Fraud Detection Units, the National Benefits Center, District Offices, sub-offices, and their related satellite offices.

This document is an SOP for completing IBIS queries on pending applications and petitions for immigration benefits in USCIS offices. The IBIS SOP is to be considered a living document relating specifically to IBIS in the background/name checks arena for benefits purposes, and will be updated as the need arises. This SOP serves to establish a standardized process for IBIS queries across USCIS, incorporating valuable information that has been learned by USCIS personnel since the implementation of the first IBIS SOP on November 21, 2002.

This SOP does not provide any adjudicative guidance for files with relating hits, nor does this SOP address the role of officer discretion in the adjudicative process. Please refer to existing SOPs for each form type for a more thorough description of the process that should be followed for the actual adjudication of that casework.

(b)(5)

(b)(7)(e)

Introduction, Continued

About IBIS

IBIS is a multi-agency effort to improve border enforcement and facilitate inspections of applicants for admission into the United States. It strengthens border security by identifying threats to national security and/or public safety, and other law enforcement violations. The system integrates computer resources to assist inspections, investigations, adjudications, law enforcement, and intelligence agencies. It combines information from many federal agencies into the Treasury Enforcement Communications System (TECS) database and interfaces with other sources such as the National Crime Information Center (NCIC).

Its usage has been expanded to include background/name checks on persons seeking immigration benefits and travel documents. USCIS personnel use IBIS for the following reasons:

- To assist federal, state, and local law enforcement and intelligence agencies in identifying individuals who pose a risk to national security and/or public safety
- To prevent ineligible aliens from obtaining immigration benefits

IBIS queries do not replace other mandated background/name checks.

About TECS

TECS is an automated enforcement and inspection lookout system. TECS is the system that USCIS personnel access when logging on to IBIS. The system is maintained by U.S. Customs and Border Protection (CBP).

About NCIC

Introduction, Continued

USCIS Policy on IBIS Usage

Data in IBIS is "For Official Use Only (FOUO)." Access to data is granted on a need-to-know basis for official use only. According to DHS Management Directive 11042.1, there are numerous additional caveats (i.e. "Law Enforcement Sensitive") used by various agencies to identify unclassified information as "Sensitive but Unclassified (For Official Use Only)." Regardless of the caveat used for identification, the reason for designation does not change.

All IBIS users must be certified through an on-line security certification test and must be re-certified every two years. Abuse or misuse of IBIS could result in loss of access, termination of employment, and/or criminal prosecution. Restrictions on IBIS use include:

- Never leave your terminal unattended while logged into IBIS
 - Never leave IBIS materials unattended in unprotected places
 - Never store IBIS information or records on the hard drive
 - Ensure all IBIS printouts are secured or destroyed
 - Never confirm or deny the existence of an IBIS record to the public or unauthorized users
 - Only use IBIS to perform official duties required by your job. Browsing is not permitted. Do not query friends or family members; do not access IBIS simply out of curiosity.
-

Introduction, Continued

USCIS Policy on IBIS Equipment and Technical Assistance

Guidelines regarding IBIS equipment and technical assistance include:

- For help concerning IBIS access issues, contact your local System Control Officer (SCO)
 - For technical help concerning IBIS issues, contact the TECS Help Desk at (b)(7)(e) [REDACTED]
 - Technical support staff will follow the guidelines outlined in the March 2, 2001 memo titled *IBIS Technical Support Guidelines at POEs*.
 - All workstations' Virtual Terminal Access Module (VTAM) identification (ID) addresses and Internet Protocol (IP) addresses will be statically assigned and coordinated with IBIS personnel prior to installation or changes
 - All terminals used to process IBIS queries will be clearly labeled
-

Program Development and Training

USCIS has designated the Office of Fraud Detection and National Security (FDNS) as the USCIS office that develops and oversees background check policy and procedures. Any IBIS-related training conducted in Service Centers, the National Benefits Center, District Offices, sub-offices, and their related satellite offices must adhere to the FDNS-approved IBIS SOP and current policies and procedures.

Any updates to this SOP or modifications to IBIS policies and procedures can be found on the FDNS web-site <http://powerport.uscis.dhs.gov/uscisfdns/index.htm>.

Any questions regarding this SOP or IBIS in general should be e-mailed to the FDNS mailbox [REDACTED]

Introduction, Continued

Third Agency Rule

(b)(7)(e)

The 1993 Memorandum of Understanding (MOU) between the Immigration and Naturalization Service and the U.S. Customs Service on the use of TECS (IBIS), which is now applicable to USCIS, sets out a system specific Third Agency Rule. This MOU provision uses a different definition of "agency" than is used under the Privacy Act and only applies to IBIS records.

(b)(5)

Under the IBIS Third Agency Rule the term "agency" applies to each agency regardless of Department (e.g. CBP, ICE, USCIS, and DOS are all agencies).

BEST PRACTICE:

RECORD LEVEL:

Introduction, Continued

Privacy Act

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

The Privacy Act protects information on United States citizens (USC) and lawful permanent residents (LPR). The Privacy Act does not apply to aliens who are not LPRs.

The protected information is contained in a USCIS system of records where a name or unique identifying number of an individual (i.e. A#) can be used to retrieve information. DHS maintains information in A-files and electronically in the Central Index System (CIS), and in IBIS. Because these types of records can be retrieved by name and A#, the Privacy Act covers information contained in A-files, in CIS, and in IBIS.

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.

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. All agencies within DHS are considered to be one agency, for the purpose of this law. An example follows:
 - 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)
- 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. Some common examples include:
- USCIS can share information with 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 USC/LPR may have violated a law that is enforced by that agency

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, must give any USC or LPR access to any records maintained on him/her. A USC or LPR may obtain information about himself/herself contained in his/her file or in CIS if he/she makes a request in writing.

Introduction, Continued

Privacy Act (Cont.)

CAUTION: IBIS records and/or resolution memos may not be provided to the individual USC or LPR due to law enforcement exceptions.

It is a violation of the Privacy Act to access or share information, for personal use, from a system of records where the name and/or unique identifying number of an individual can retrieve information. A violation of the Privacy Act can result in civil liability (i.e. damage award) and/or criminal penalties (i.e. a misdemeanor charge and a fine).

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

SECTION II:

Operational Guidelines

Section II: Operational Guidelines

About this Section

In this section, you will find information about the following topics:

- Who Performs IBIS Queries
 - Types of IBIS Queries
 - When to Perform IBIS Queries
 - Who to Query
 - Who to Query Chart
 - Documentation of IBIS Query
 - Annotating the ROIQ
 - ROIQ
-

Who Performs IBIS Queries

USCIS personnel must meet all of the following requirements to perform IBIS queries:

- Proper National Agency Check with Inquiries (NACI) background checks
 - Successful completion of mandatory IBIS and NCIC training and certification
 - Citizen of the United States of America
-

Types of IBIS Queries

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

- SQ-11 (Person Subject) Query
 - SQ-16 (Organization Subject) Query
 - Batch Processing
 - NN-16 (Criminal History) Query, with appropriate authorization as discussed in the Introduction Section
 - Others as deemed appropriate by local policy
-

Operational Guidelines, Continued

When to Perform IBIS Queries

An IBIS query must be run on all new applications/petitions within 15 calendar days of initial receipt.

The validity period for an IBIS query is 90 days.

EXCEPTION: For beneficiaries who are not physically present in the United States and who intend to apply for their visas abroad, the primary name and DOB must be queried only once prior to final adjudication.

Prior to final adjudication, IBIS queries must be performed on additional name and DOB variations discovered during the adjudicative process. IBIS queries must be valid at the following times:

- Time of final decision (i.e. approval, denial, abandonment denial, revocation, reaffirmation)
- Time of naturalization ceremony
- When relocating a pending application/petition from a Center to a District Office

EXCEPTION: This is not required for N-400 cases.

- When relocating an appeal or motion to an appellate body (i.e. AAO, BIA)
- When providing temporary evidence of lawful permanent residence to an alien (i.e. ADIT stamp in passport or on I-94)

IBIS queries are not required at the following times because no new adjudicative action is being taken:

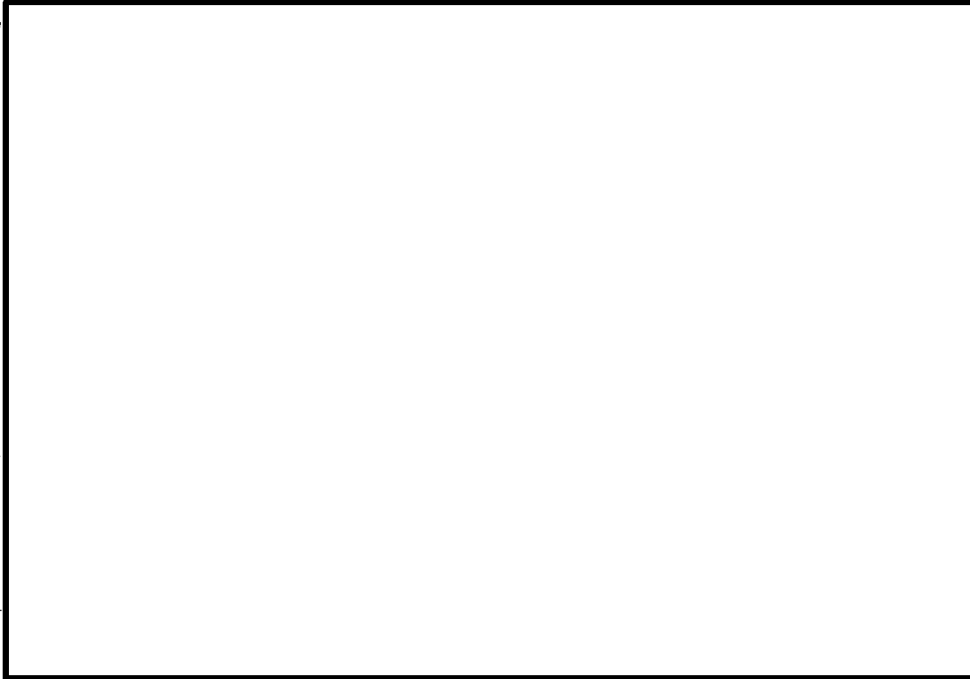
- Updating case as ADMINISTRATIVE CLOSE
 - Updating case as CASE TERMINATED; STATUS ACQUIRED THROUGH OTHER MEANS
 - Changing validity dates of a benefit
 - Re-issuing notices
 - Re-issuing undeliverable cards
 - Issuing a Notice to Appear (NTA)
-

Operational Guidelines, Continued

Who to Query

(b)(5)

(b)(7)(e)



Operational Guidelines, Continued

Figure II-1: Who to Query Chart

(b)(7)(e)

(b)(5)

FORM	Applicant	Petitioner	Beneficiary	Derivatives	Household Members
BONDS					
EOIR-29					
I-90					
I-94					
I-95					
I-102					
I-129					
I-129F					
I-129S					
I-130					
I-131					
I-140					
I-192					
I-212					
I-290A					
I-290B					
I-360					
I-485					
I-526					
I-539					
I-589					
I-600					
I-600A					
I-601					
I-602					
I-612					
I-687					
I-690					
I-694					
I-698					
I-700					
I-730					
I-751*					
I-765					
I-817					
I-821					
I-824					
I-829					
I-881					
I-914					
I-914A					
I-918					
N-300					
N-336					
N-400					
N-470					
N-565					
N-600					
N-600K					
N-643					
N-644 **					

Operational Guidelines, Continued

- Documentation of IBIS Query** At the time of final adjudication, each file must contain documentation confirming an IBIS query was performed on each and every required name and DOB variation. Documentation may take one of the following forms:
- CLAIMS 3 history printout – demonstrates results of query for the primary name and DOB only
 - Record of IBIS Query (ROIQ) (hard copy or electronic version) – demonstrates results of queries for all name and DOB variations
 - Electronic record of IBIS queries (i.e. CLAIMS update) – only for cases that are part of special programs or projects using electronic adjudication or system verification (i.e. TPS)
-

Operational Guidelines, Continued

Annotating the ROIQ

The following page contains a blank example of the ROIQ. USCIS personnel must use this form to record the results of IBIS queries. Each file must contain its own ROIQ.

In the "A-Number or Receipt Number" field, document the file number. If the application/petition is not contained in a file, document the subject's A-number.

(b)(5)

In the "Last Name, First Name" and "DOB" fields, document the last name, first name, and date of birth exactly as queried in IBIS. The "DOB" field does not apply for SQ-16 queries.

(b)(7)(e)

Check the appropriate box to classify the subject queried:

A=Applicant

P=Petitioner

B=Beneficiary

D=Derivative/Household Member

In the "#" boxes, number each query (i.e. 1, 2, 3, 4, 5, 6).

If Soundex was queried, annotate "Soundex" under the search criteria queried.

Annotate the date of the query AND the legible initials or identifying number of the individual conducting the query. Annotate the results of the IBIS query in one of the following three blocks:

- Annotate in the NO MATCH block if the query resulted in no IBIS hit
- Annotate in the DNR block if the query resulted in an IBIS hit that does not relate to the subject queried
- Annotate in the RELATES block if a query resulted in an IBIS hit that does relate to the subject queried



Operational Guidelines, Continued

Figure II-1:ROIQ

Record of IBIS Query (ROIQ)						
A-Number or Receipt Number : _____						
#	Last Name, First Name	DOB	NO MATCH	DNR	RELATES	Resolution Memo Completed?
	<div style="text-align: center;"> _ _ _ _ A P B D </div>	2 nd Check 3 rd Check				—
	<div style="text-align: center;"> _ _ _ _ A P B D </div>	2 nd Check 3 rd Check	_____			—
	<div style="text-align: center;"> _ _ _ _ A P B D </div>	2 nd Check 3 rd Check	_____			—
	<div style="text-align: center;"> _ _ _ _ A P B D </div>	2 nd Check 3 rd Check	_____			—
	<div style="text-align: center;"> _ _ _ _ A P B D </div>	2 nd Check 3 rd Check	_____			—
	<div style="text-align: center;"> _ _ _ _ A P B D </div>	2 nd Check 3 rd Check	_____			—

Properly annotate IBIS results on the ROIQ:
 *Include the date of query in the appropriate box (NO MATCH, DNR, RELATES).
 *Include the initials and identifying number of the USCIS personnel conducting the query in the same box as the date.
 *If the hit was a RELATES and a Resolution Memo was completed, check the Resolution Memo Completed box in the last column.

NO MATCH – No information found in IBIS
 DNR – Information found in IBIS but does not relate to the subject.
 RELATES – Information found in IBIS that relates to the subject, case referred for resolution
 A = Applicant P = Petitioner
 B = Beneficiary D = Derivative/Household Member

SECTION III:

SQ-11

SQ-11, Continued

Section III: SQ-11

About this Section

In this section, you will find information about the following topics:

- SQ-11 Query Objective
- Conducting an SQ-11 Query
- SQ-11 Search Criteria
- Name and DOB Rules
 - First Names
 - Spelling Variations
 - Name Variations/Aliases
 - Names with Initials
 - Names with Hyphens
 - Names with Apostrophes
 - Names with Parentheses
 - Names with Prefixes
 - Names with Suffixes
 - Names Found in Translations
 - Foreign Alphabets
 - Single Name Queries
 - DOB Queries

SQ-11 Query Objective

The objective of the SQ-11 Query is to confirm the existence or non-existence of information in IBIS that relates to a subject of a pending application/petition.

Conducting a SQ-11 Query

(b)(5)

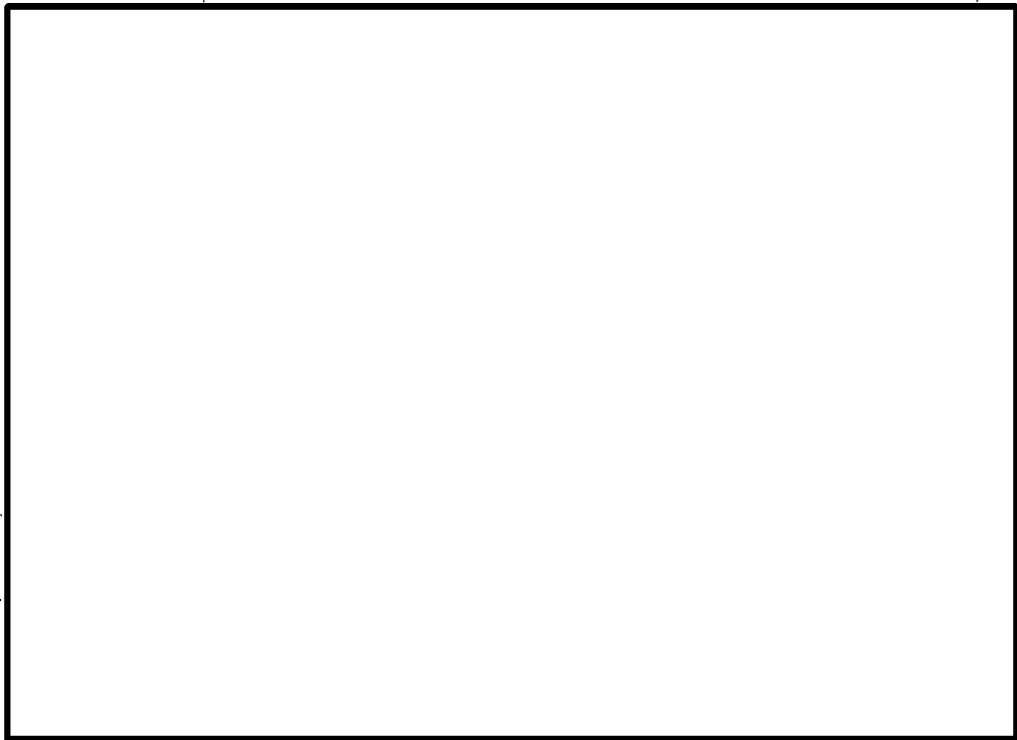
(b)(7)(e)

SQ-11, Continued

SQ-11 Search Criteria

(b)(5)

(b)(7)(e)



SQ-11, Continued

Name and DOB Rules

In the examples contained in this section, ALL LAST NAMES are found in ALL CAPITAL LETTERS.

Name and DOB Rules: First Names

The first name field in IBIS is a "shorter string match search." Results may match all or only a portion of the queried first name. In the case of a subject with multiple variations of a first name or compound first name, **ONLY** query the portion of the first name that is common to all variations.

Example #1

The subject's name appears on the petition as, [REDACTED] Documents in the file show the subject's first name appears as, [REDACTED] Because of the shorter string match search, a query of the common portion of all three variations (in this case, [REDACTED]) is sufficient to cover all three name variations. If the last name and DOB are common to the name variations, query:

(b)(6)

[REDACTED]

Example #2

The subject's name appears on the application as, [REDACTED] Documents in the file show the subject's name as, [REDACTED] Because of the shorter string match search, query:

[REDACTED]

Example #3

The subject's name appears on the petition as, [REDACTED] Documents in the file show the subject's name as [REDACTED] and do not distinguish between the first name and middle name. Because of the shorter string match search, query:

[REDACTED]

SQ-11, Continued

Name and DOB Rules: Spelling Variations

What to do with spelling variations in names.

Example #1

The subject's name appears on the petition as, [redacted] Documents in the file show the subject's name as, [redacted] Query both:

[redacted]

(b)(6)

Example #2

The subject's name appears on the application as, [redacted] Documents in the file show a longer version of the first name as, [redacted] Query both:

[redacted]

Name and DOB Rules: Name Variations/ Aliases

What to do with name variations/aliases.

Example #1

The subject's name appears on the petition as, [redacted]
Documents in the file show the subject's name as, [redacted]

Query:

[redacted]

Example #2

The subject's name appears on the application as, [redacted]
Documents in the file show the subject's name as, [redacted]

Query both:

[redacted]

NOTE: The names "DOE, John" and "DOE, Jane" are not considered valid aliases and should not be queried.

SQ-11, Continued

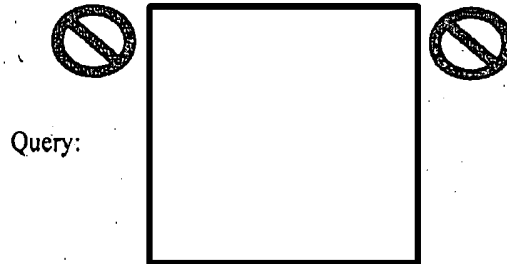
Name and DOB Rules: Names with Initials

Do **NOT** query initials after last or first names, even if the initials appear on the application/petition or on documents provided in support of the application/petition.

Example #1

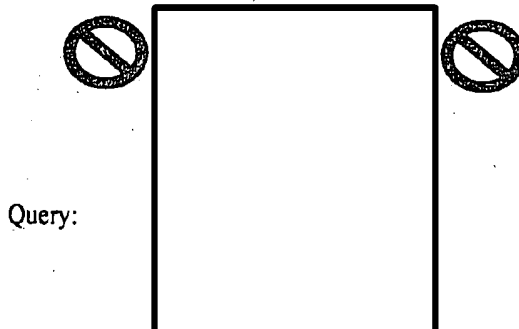
The subject's name appears on the application as Do **NOT** query the initial, even if the initial appears after the first name in the first name field on the application. Do **NOT** query:

(b)(6)



Example #2

The subject's name appears on the petition as, "GONZALEZ P, Jose L." Do **NOT** query the initials after the first or last name of a subject, even if the initials appear in the first or last name field on the petition. Do **NOT** query:



SQ-11, Continued

Name and DOB Rules: Names with Hyphens

For names with hyphens, query both with the hyphen **AND** with a space in place of the hyphen. Conversely, do **NOT** add a hyphen to a name.

Example #1

The subject's name appears on the application as,
Query the name both as it appears on the application and with a space in place of the hyphen as follows:

(b)(6)

Example #2

The subject's name appears on the application as, Do **NOT** add a hyphen to the query:



Query:



Name and DOB Rules: Names with Apostrophes

For names with apostrophes, query both without the apostrophe **AND** with a space in place of the apostrophe. Do **NOT** query apostrophes.

Example

The subject's name appears on the application as, Query both:

Name and DOB Rules: Names with Parentheses

For compound last names where one part of the name is in parentheses, query each part of the name separately.

Example

The subject's name appears on the petition as, Documents in the file show the subject's name as, Query both:

SQ-11, Continued

Name and DOB Do NOT query prefixes (such as Dr., Mr., Mrs., Ms., or Rev.).

Rules: Names

with

Prefixes

Example

The subject's name appears on the petition as,

Query:

Name and DOB Do NOT query suffixes (such as Jr., Sr., I, or II).

Rules: Names

with Suffixes

Example

The subject's name appears on the application as,

Query:

Name and DOB For documents written in a foreign language, query names found in translations to English.

Rules: Names

Found in

Translations

Example

The subject's name appears on the application as,
of a document in the file shows the subject's name

The translation
Query both:

(b)(6)

SQ-11, Continued

Name and DOB
Rules: Foreign
Alphabets

If a name is written with the same characters as the English language but includes a special character such as an accent mark, drop the special character and query using the underlying letter.

Example

The subject's name appears on the petition as, Since IBIS does not accept special characters, query:

Do **NOT** query names with characters from foreign alphabets. Do **NOT** attempt to convert foreign language characters to English letters. Only use the English translated name.

(b)(6)

The following is an example of a name containing characters from a foreign alphabet:



Name and DOB
Rules: Single
Name Queries

Some individuals only have one name. A single name may be queried when necessary. Enter the single name in the last name field, leaving the first name field blank.

Example

The subject's name appears on the application as Documents in the file also show the subject's name only as Since single names can be queried in the last name field, query:

NOTE: Visa pages may list a first name as "FNU," First Name Unknown. Do not query "FNU" as the first name. Consider the subject to have only one name.

SQ-11, Continued

Name and DOB
Rules: DOB
Queries

(b)(5)



SECTION IV:

Batch Query

(b)(5)

(b)(7)(e)

Section IV: Batch Query

About this Section

In this section, you will find information about the following topics:

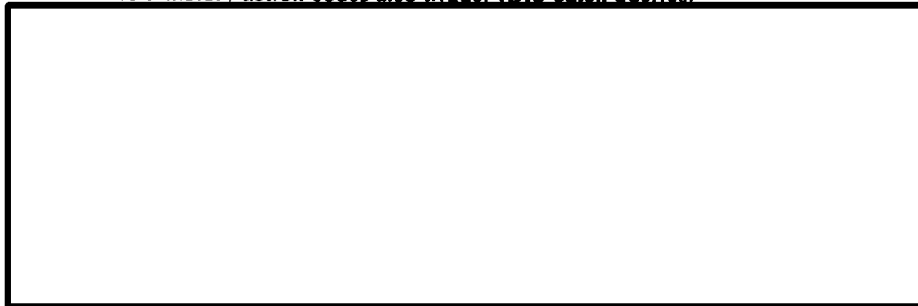
- Batch Query Objective
 - When Batch Queries are Performed
 - Batch Query Process
-

Batch Query Objective

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

When Batch Queries are Performed

Centers are required to run a batch query on the primary names and DOBs on all new applications/petitions within 15 calendar days of initial receipt. The following CLAIMS 3 history action codes also trigger IBIS batch queries:



In the Batch Query process, search criteria are automatically extracted from select cases in CLAIMS 3/GUI, MFAS, and CLAIMS 4. Batch queries may also be used to process aliases entered into local IBIS Alias programs.

Batch Query, Continued

Batch Query Process

(b)(5)

(b)(7)(e)

Step	Action
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

SECTION V:

SQ-16

(b)(7)(e)

(b)(5)

Section V: SQ-16

About this Section

In this section, you will find information about the following topics:

- SQ-16 Query Objective
 - Conducting an SQ-16 Query
 - SQ-16 Search Criteria
-

SQ-16 Query Objective

The objective of the SQ-16 Query is to confirm the existence or non-existence of information in IBIS that relates to a business, school, organization, etc.

Conducting an SQ-16 Query

SQ-16 Search Criteria

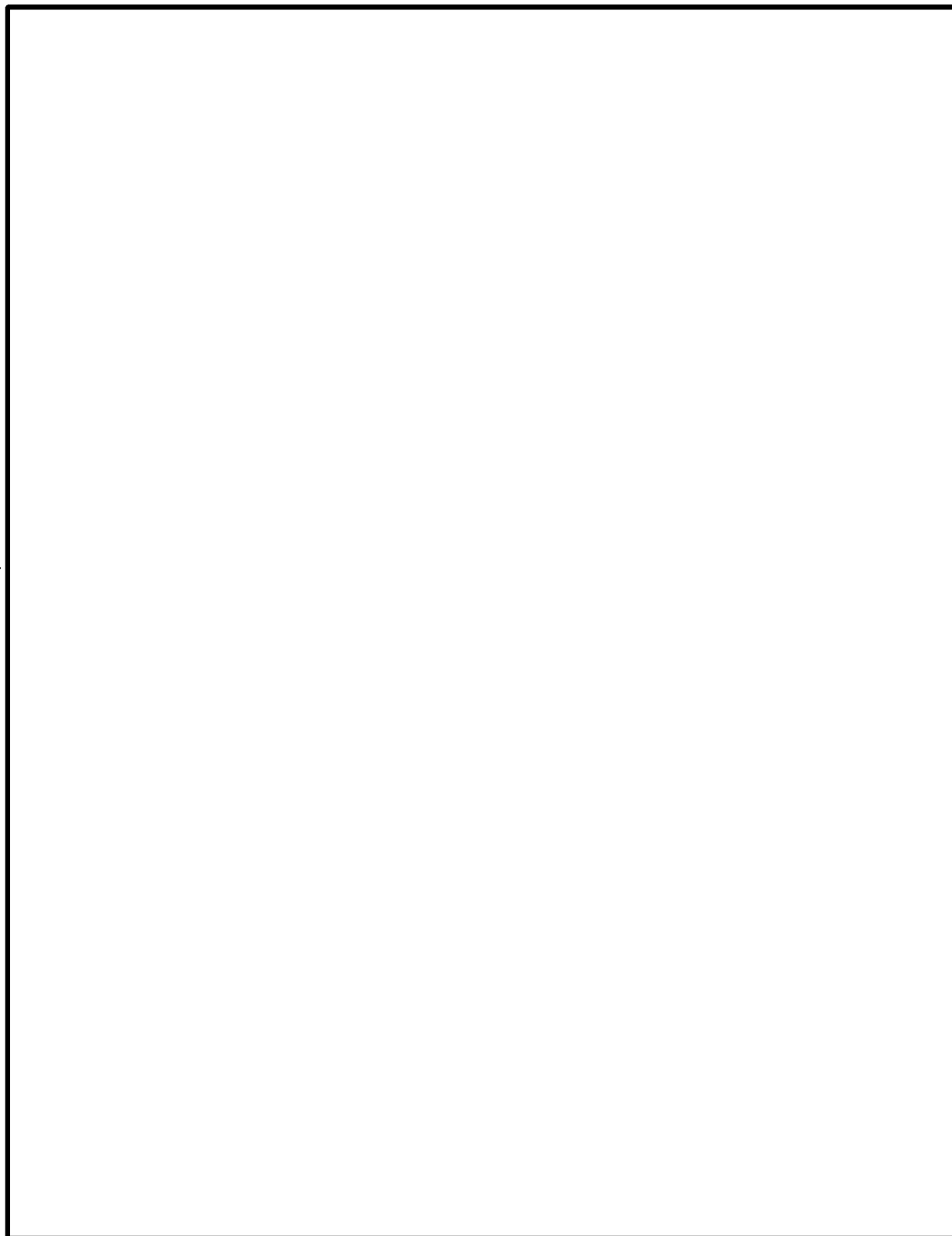
SECTION VI:

Center Resolution Process

(b)(5)

(b)(7)(e)

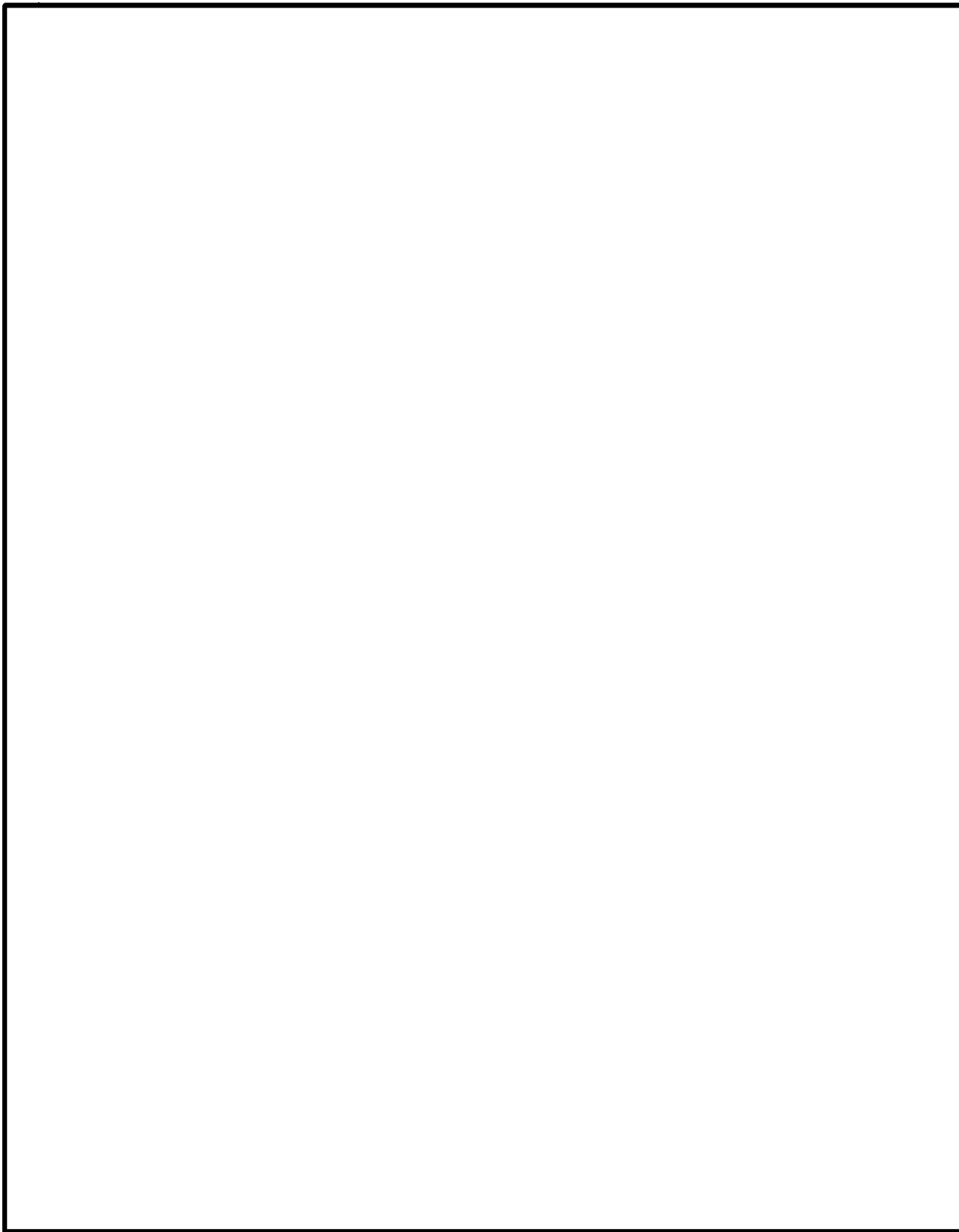
Section VI: Center Resolution Process



(b)(5)

(b)(7)(e)

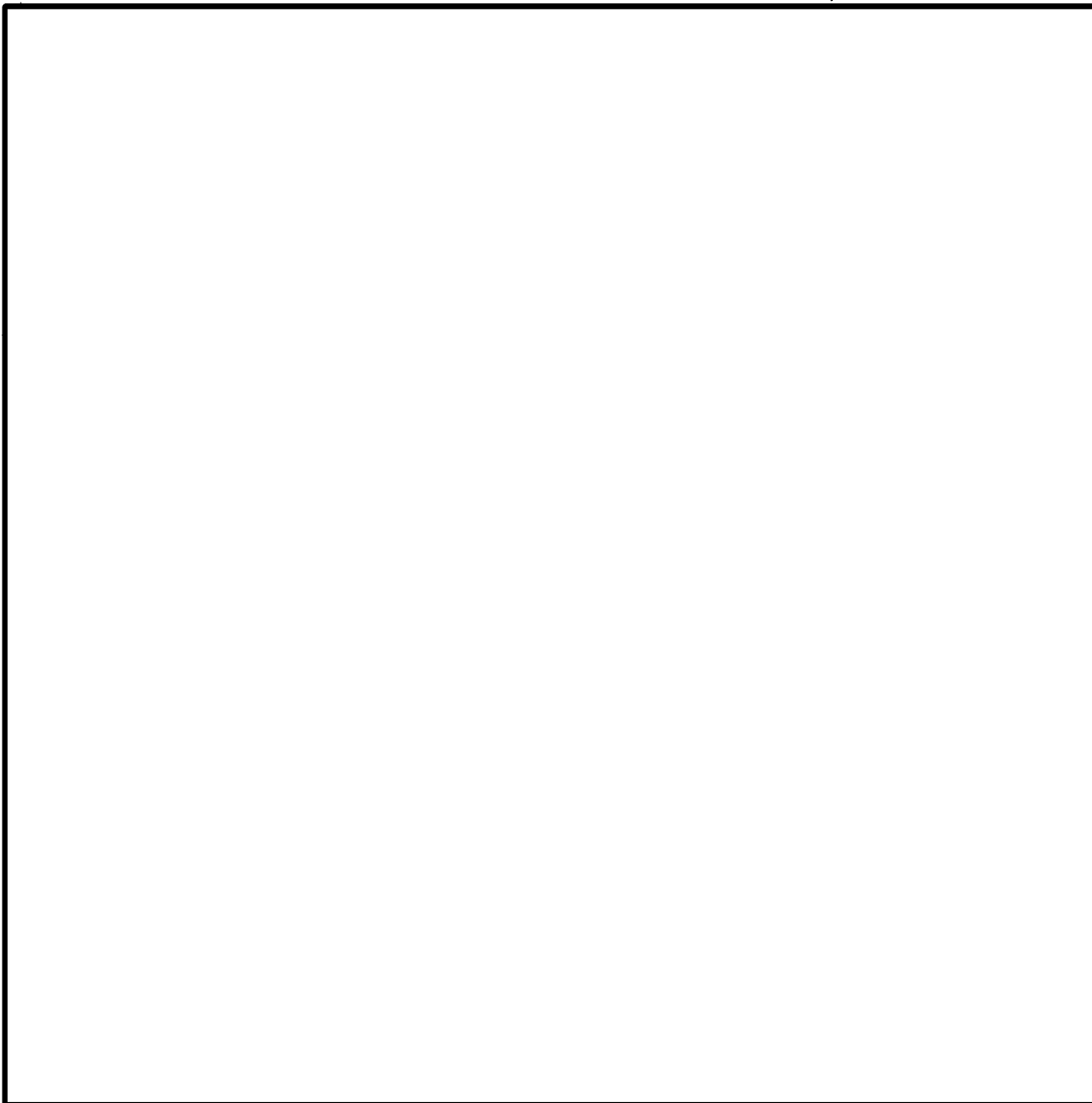
Center Resolution Process, Continued



(b)(5)

(b)(7)(e)

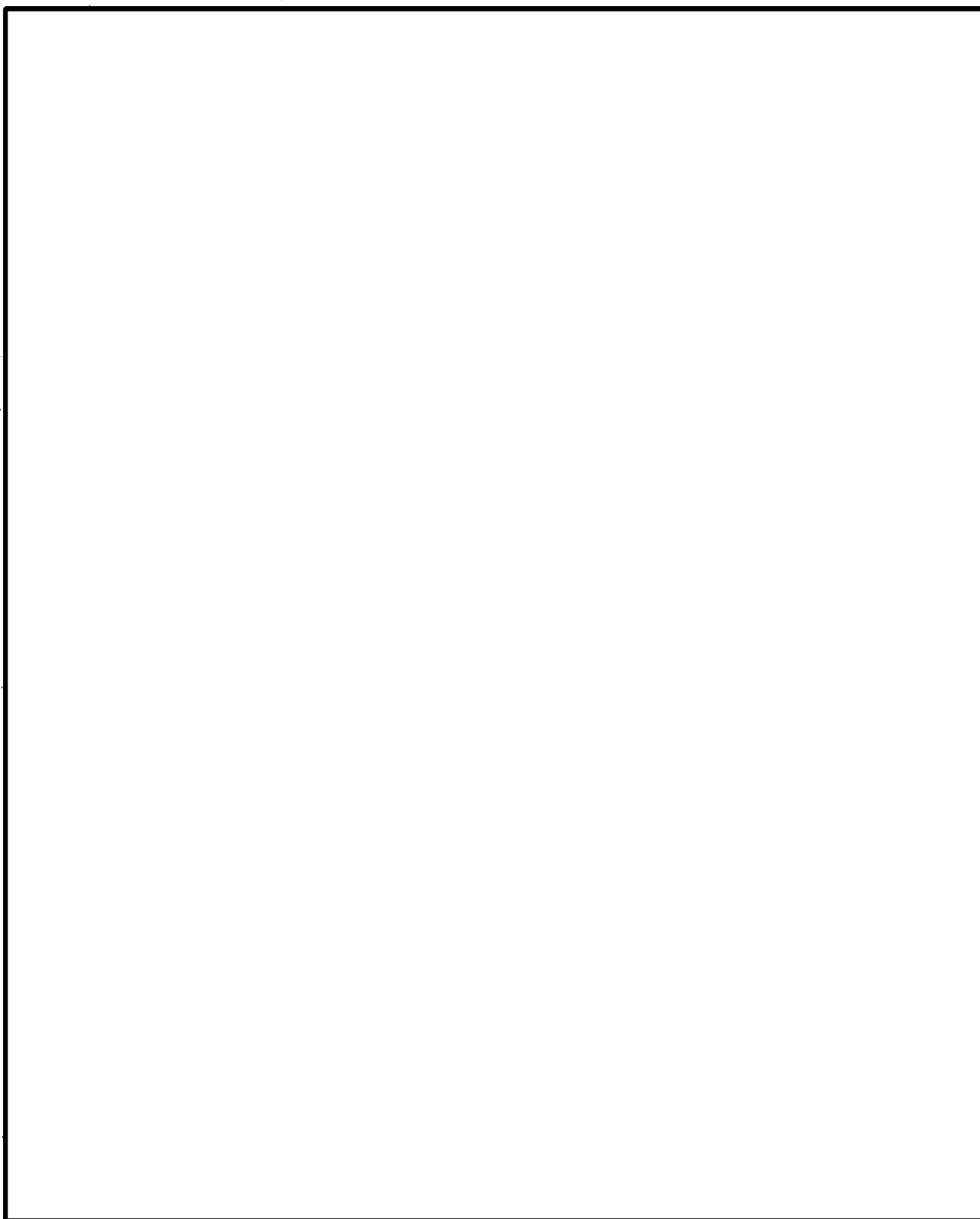
Center Resolution Process, Continued



(b)(5)

(b)(7)(e)

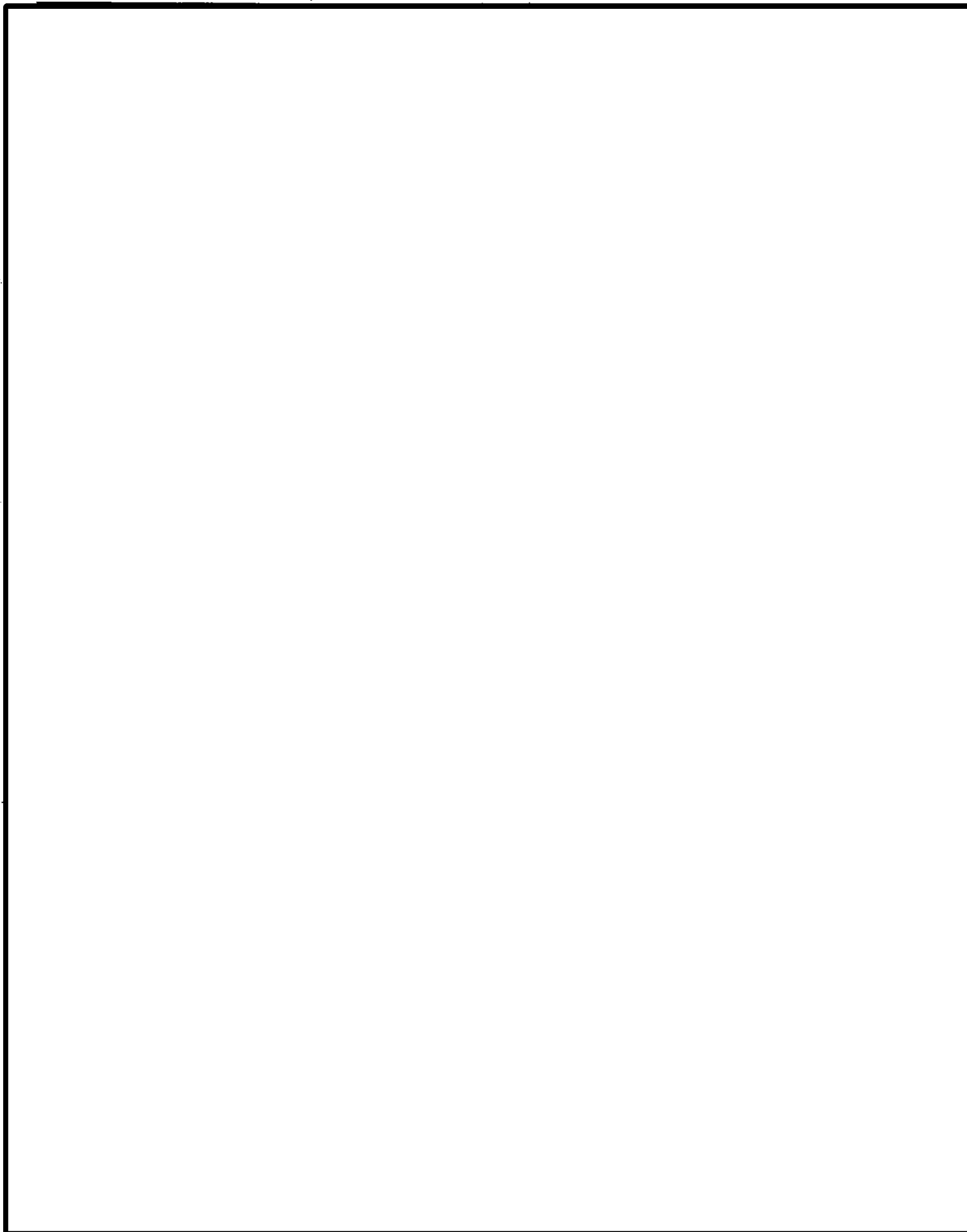
Center Resolution Process, Continued



(b)(5)

(b)(7)(e)

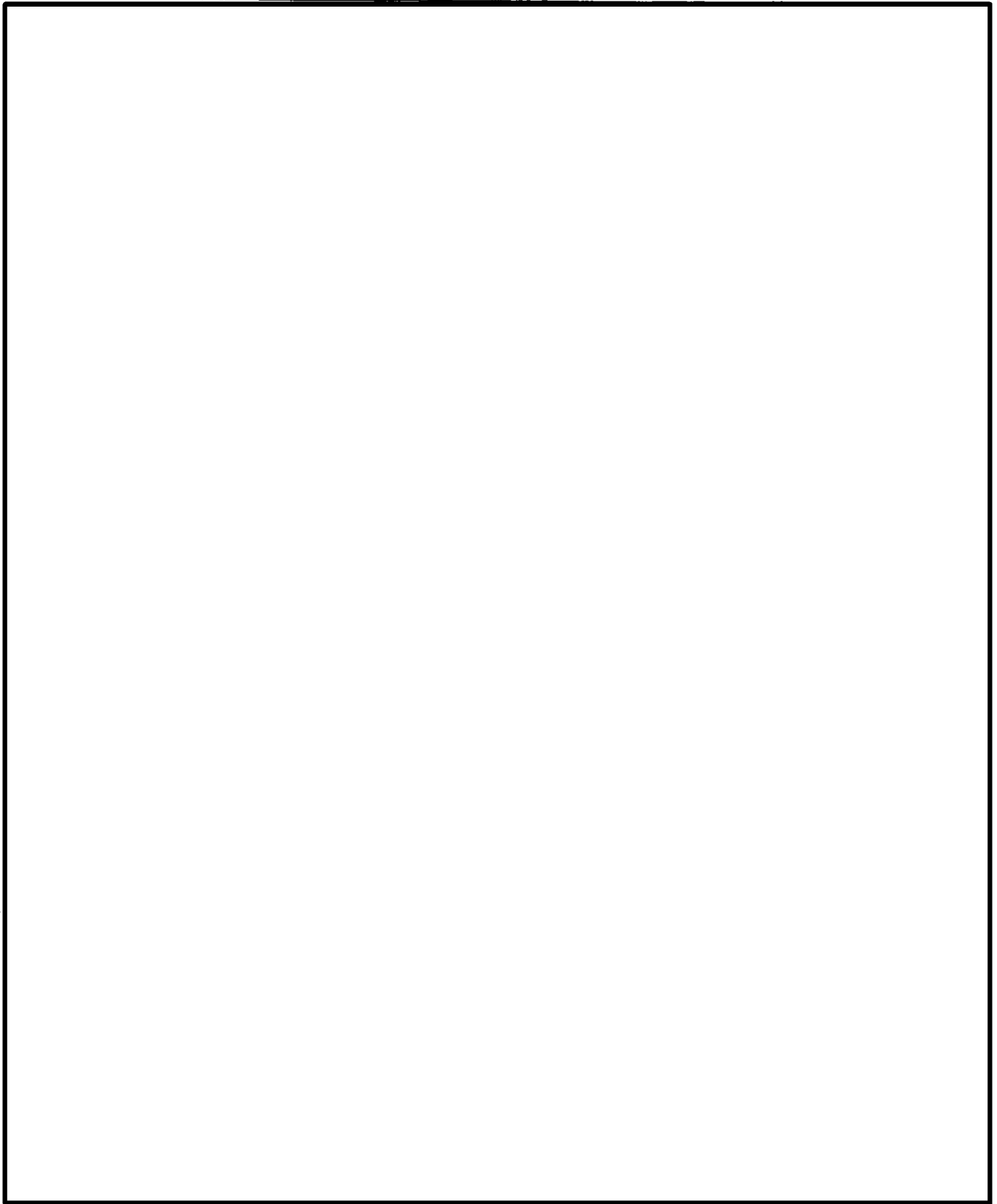
Center Resolution Process, Continued



(b)(5)

(b)(7)(e)

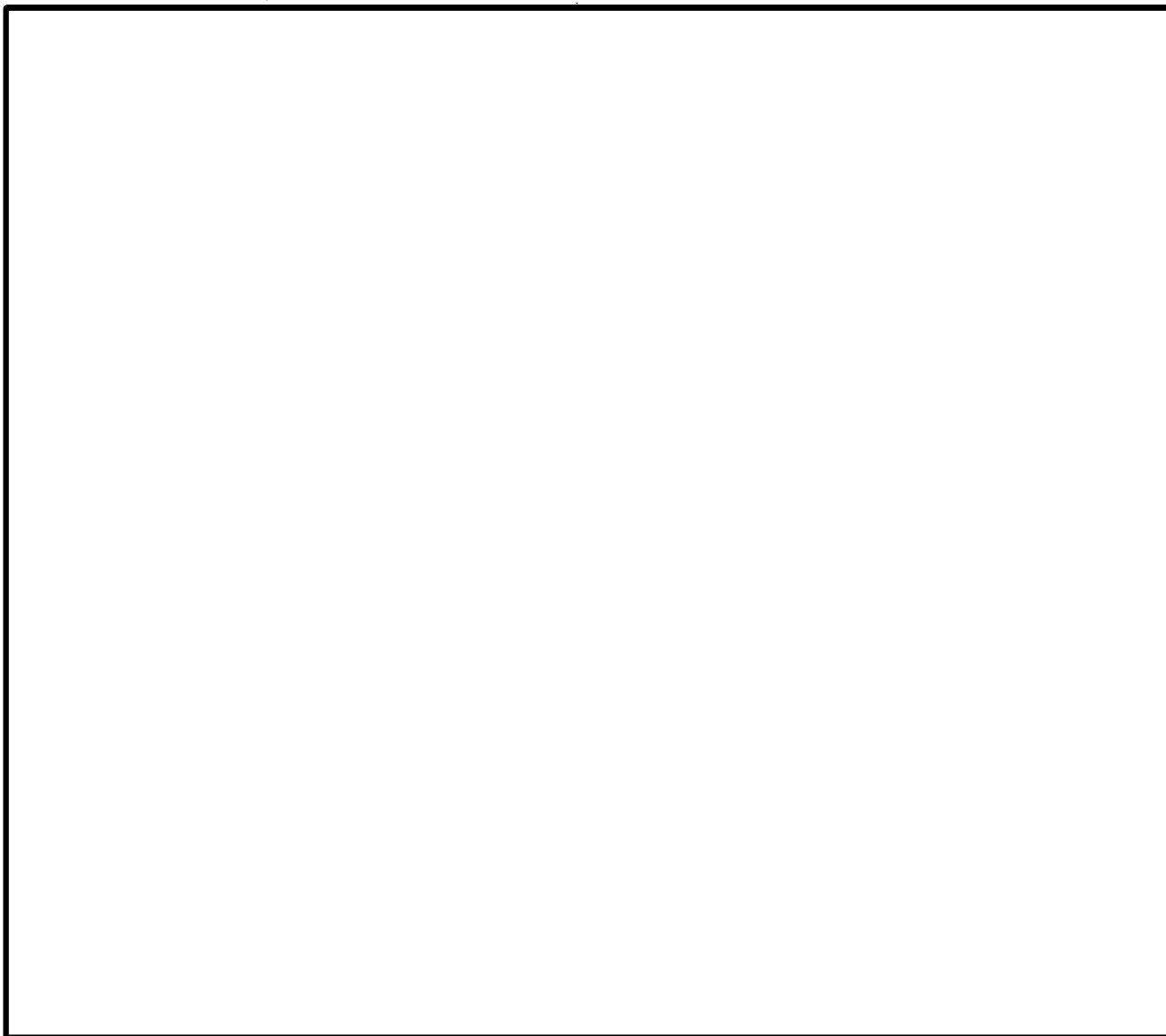
Center Resolution Process, Continued



(b)(5)

(b)(7)(e)

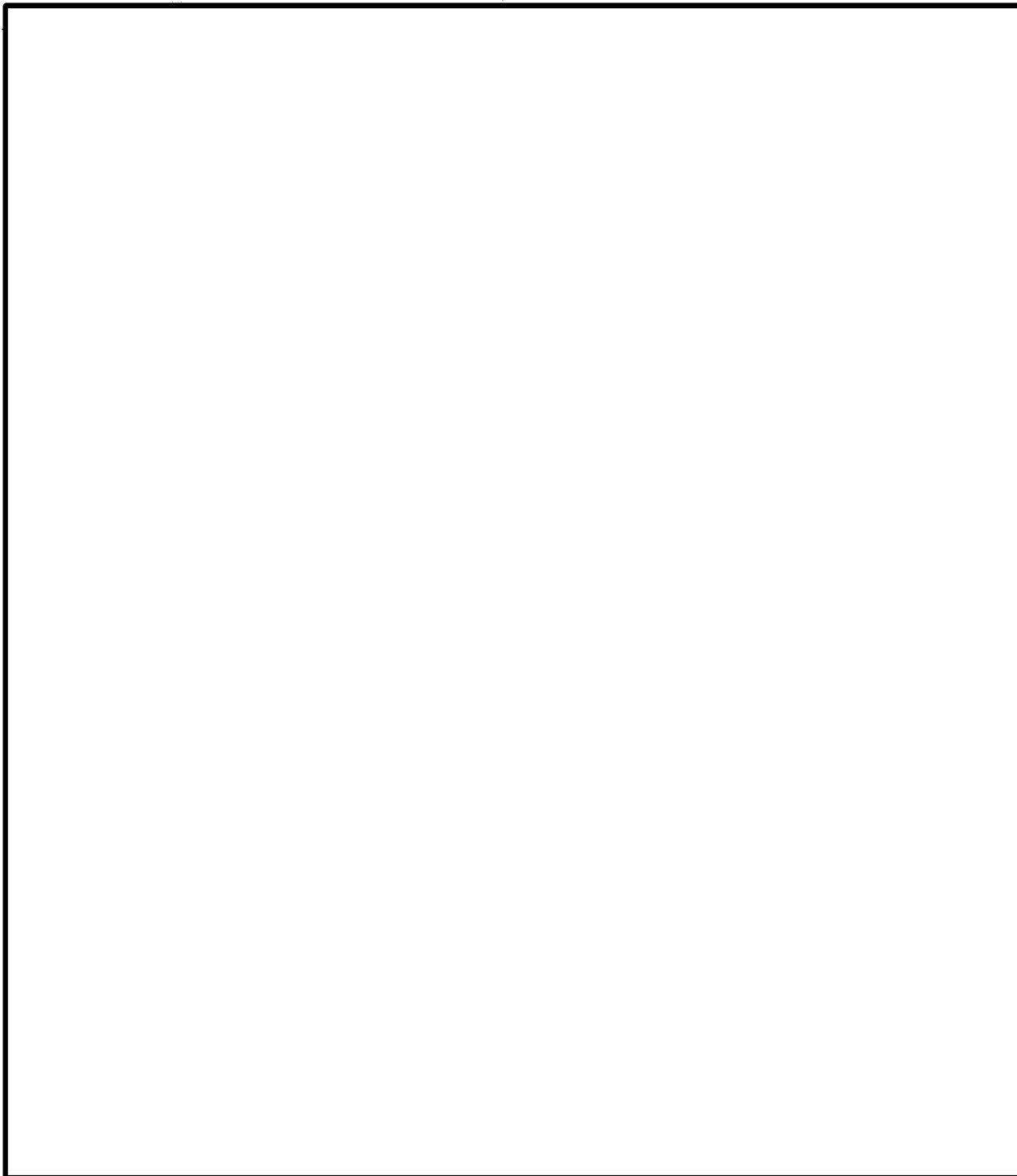
Center Resolution Process, Continued



(b)(5)

(b)(7)(e)

Center Resolution Process, Continued



(b)(5)

(b)(7)(e)

Center Resolution Process, Continued



Center Resolution Process, Continued

(b)(7)(e)

Figure VI-1: Completed ROIQ (Center)

(b)(7)(c)

Record of IBIS Query (ROIQ)						
A-Number or Receipt Number 						
#	Last Name, First Name	DOB	NO MATCH	DNR	RELATES	Resolution Memo Completed?
1						
2						
3						
<div style="text-align: center;"> X _ _ _ _ A P B D </div>		2 nd Check				
		3 rd Check				
<div style="text-align: center;"> _ _ _ _ A P B D </div>		2 nd Check				
		3 rd Check				
<div style="text-align: center;"> _ _ _ _ A P B D </div>		2 nd Check				
		3 rd Check				

Properly annotate IBIS results on the ROIQ:

*Include the date of query in the appropriate box (NO MATCH, DNR, RELATES).

*Include the initials and identifying number of the USCIS personnel conducting the query in the same box as the date.

*If the hit was a RELATES and a Resolution Memo was completed, check the Resolution Memo Completed box in the last column.

NO MATCH – No information found in IBIS

DNR – Information found in IBIS but does not relate to the subject.

RELATES – Information found in IBIS that relates to the subject, case referred for resolution.

A = Applicant

B = Beneficiary

P = Petitioner

D = Derivative/Household Member

Center Resolution Process, Continued

Explanation of
Completed
ROIQ

(b)(5)

(b)(7)(c)

(b)(7)(e)

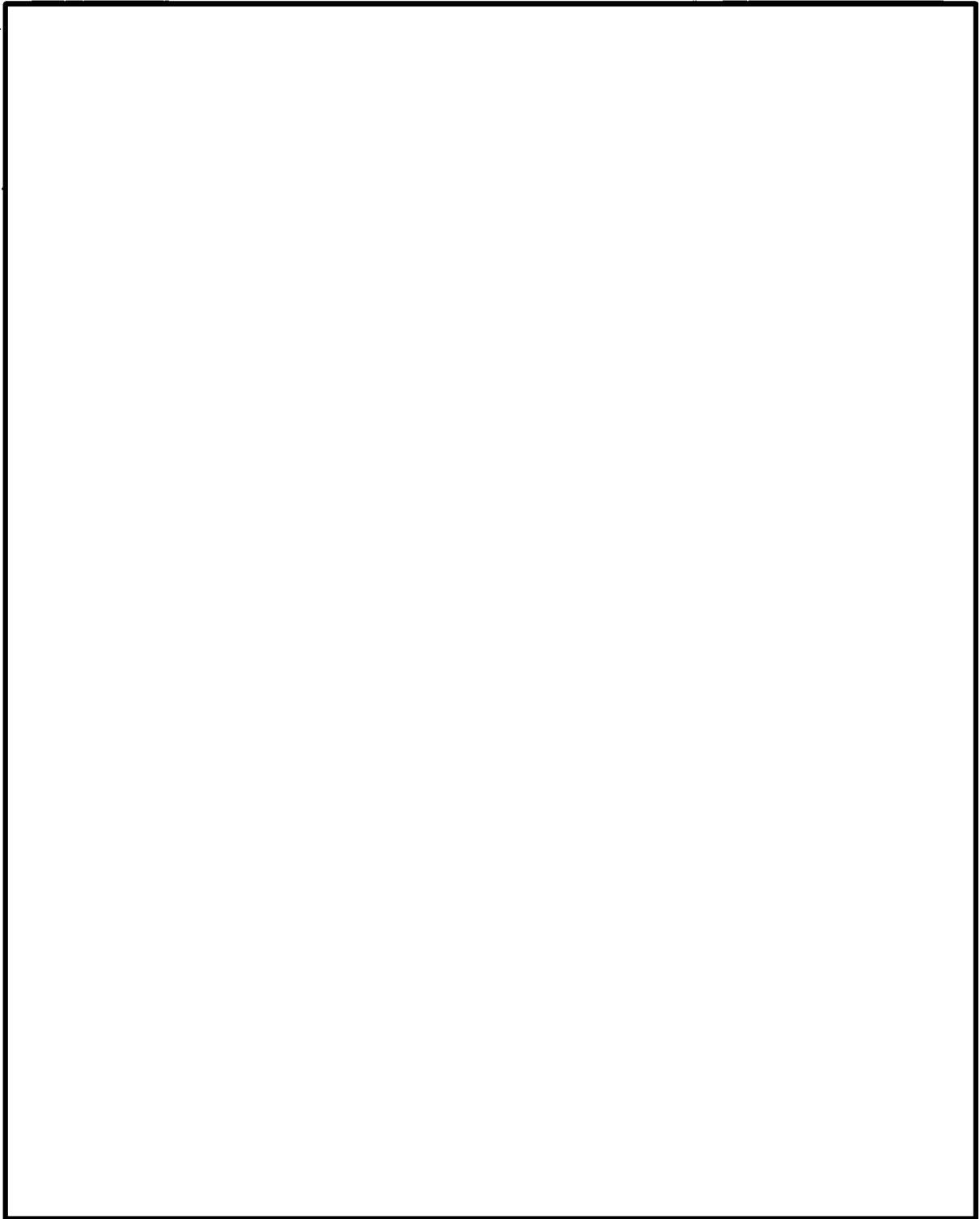
SECTION VII:

Field Resolution Process

(b)(5)

(b)(7)(e)

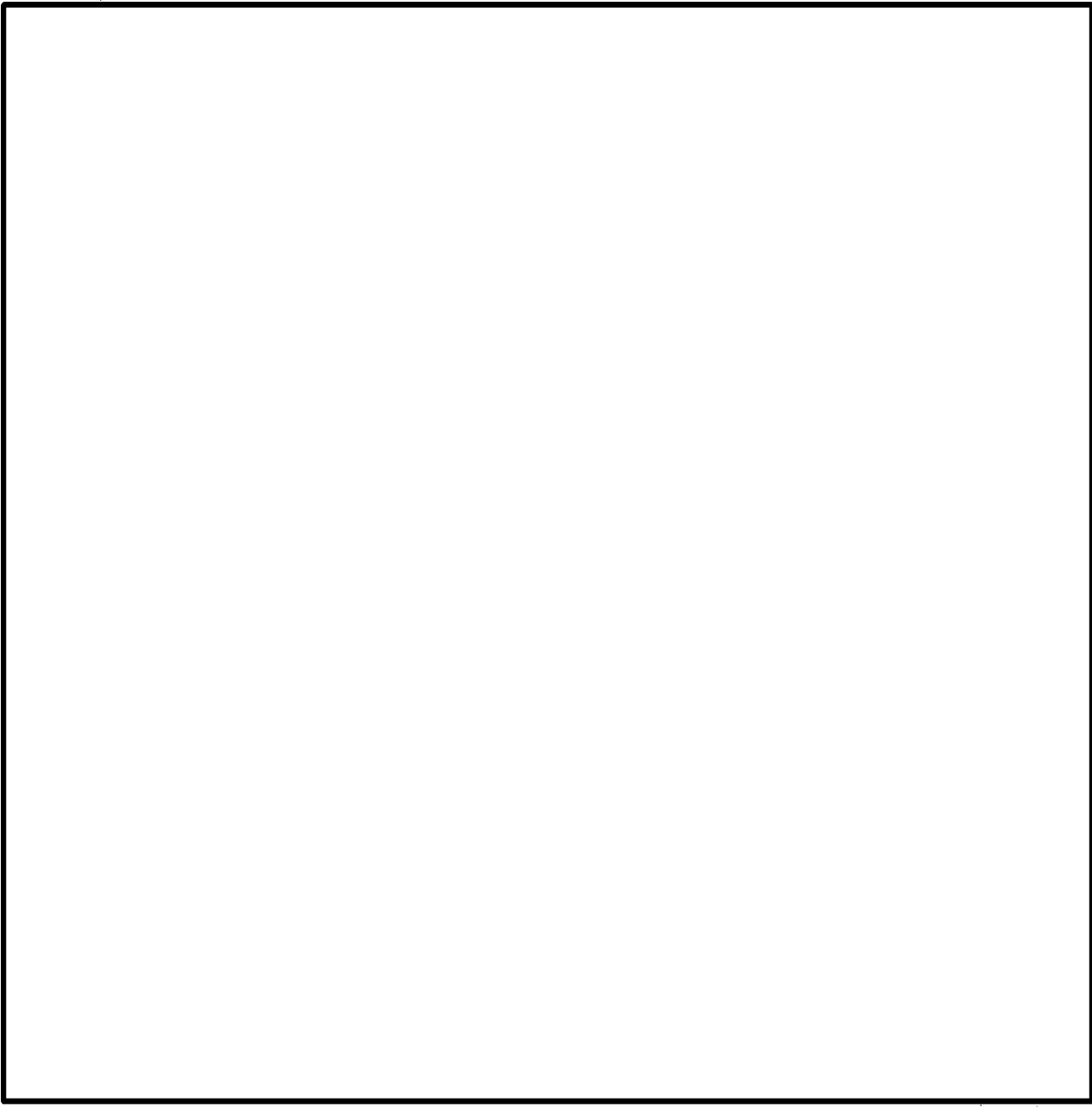
Section VII: Field Resolution Process



(b)(5)

Field Resolution Process, Continued

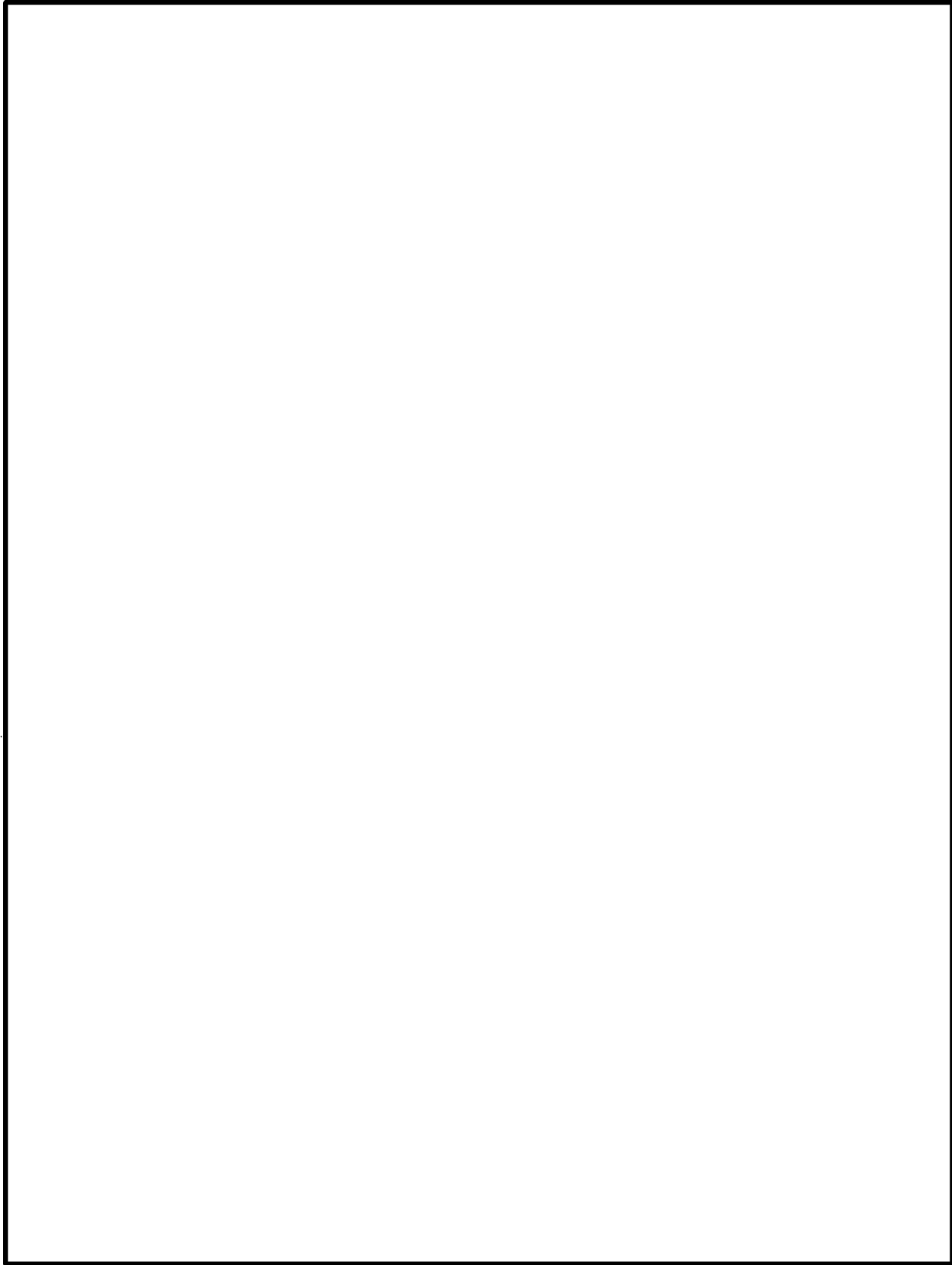
(b)(7)(e)



(b)(7)(e)

(b)(5)

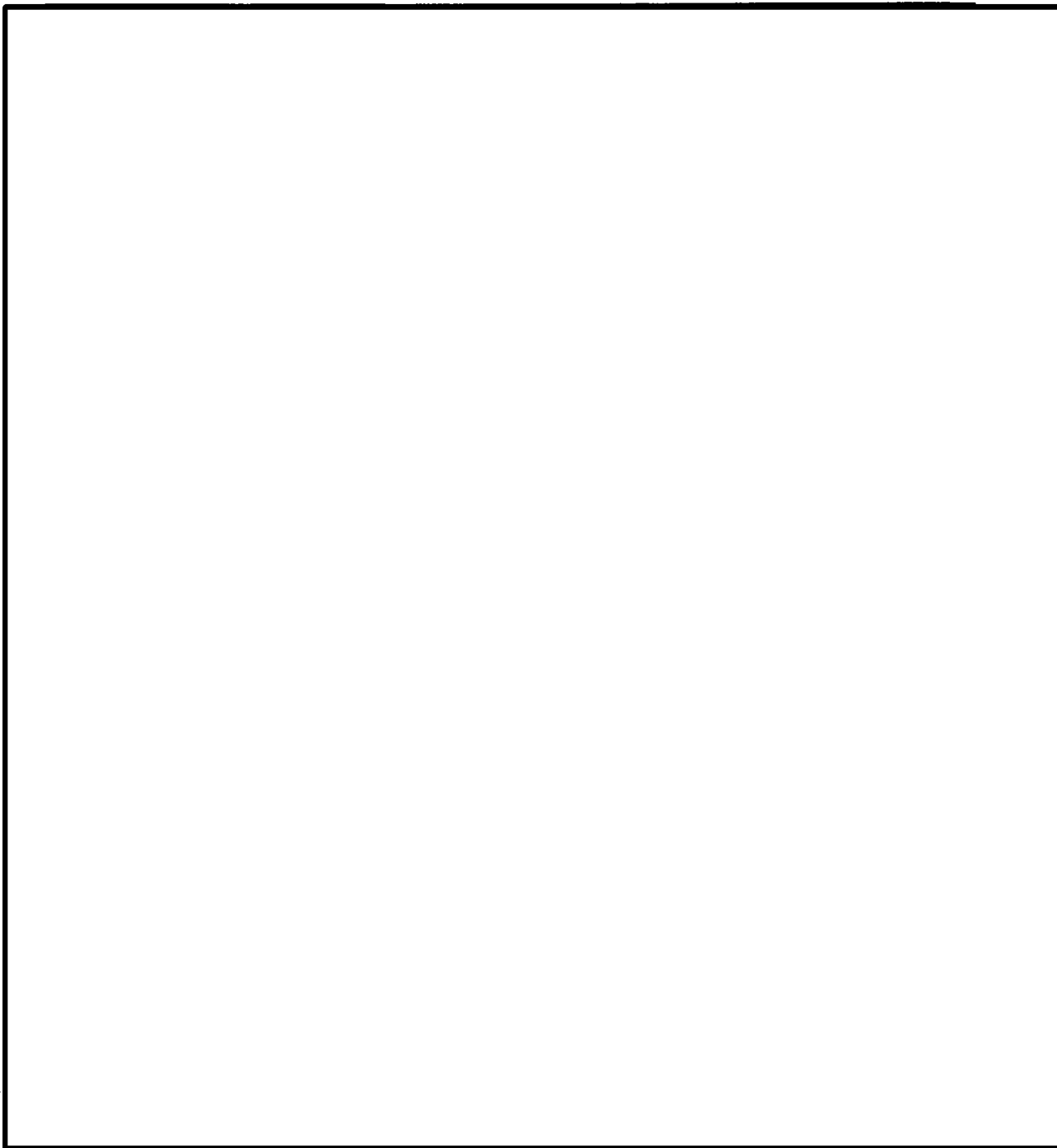
Field Resolution Process, Continued



(b)(5)

(b)(7)(e)

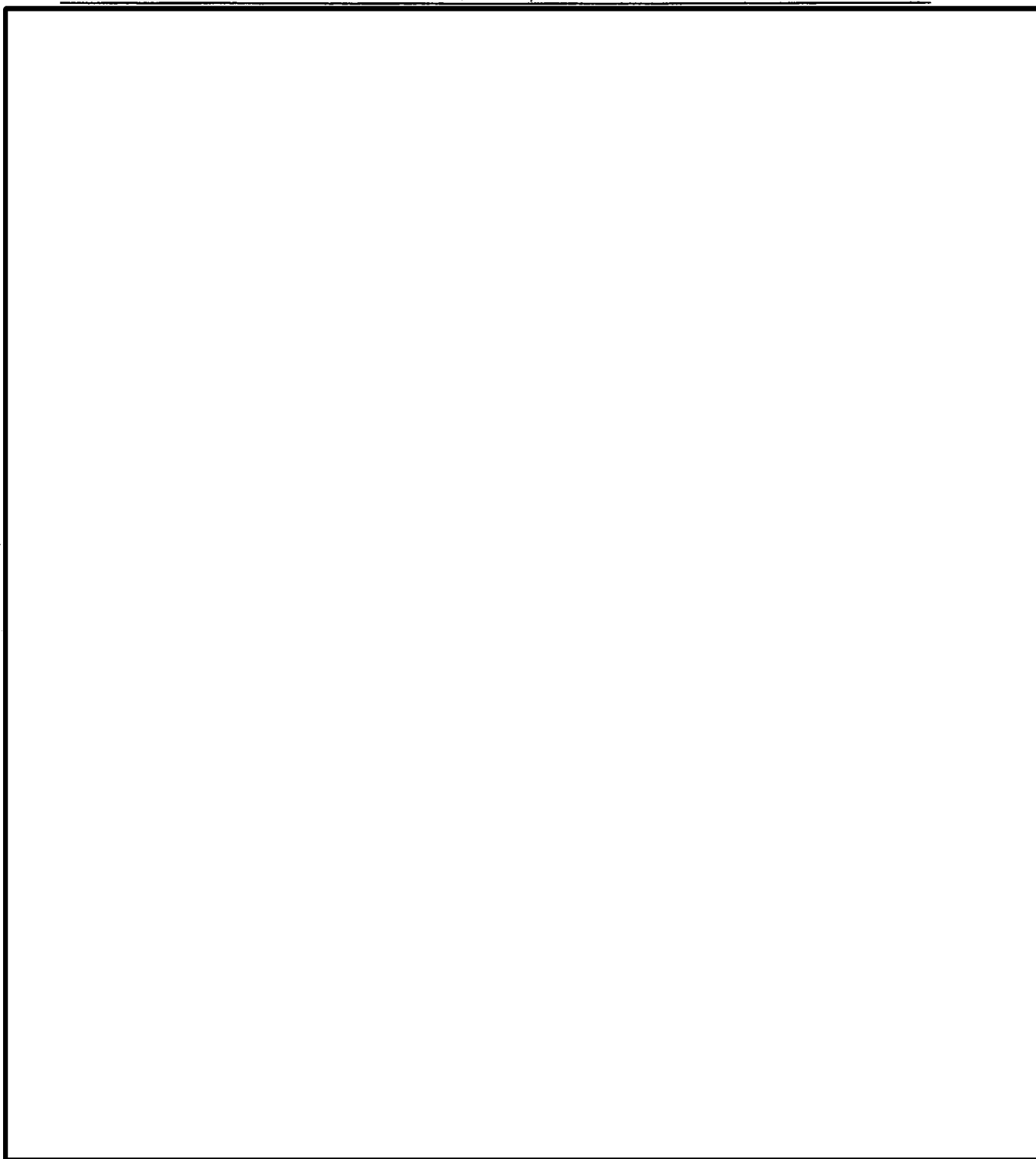
Field Resolution Process, Continued



(b)(5)

(b)(7)(e)

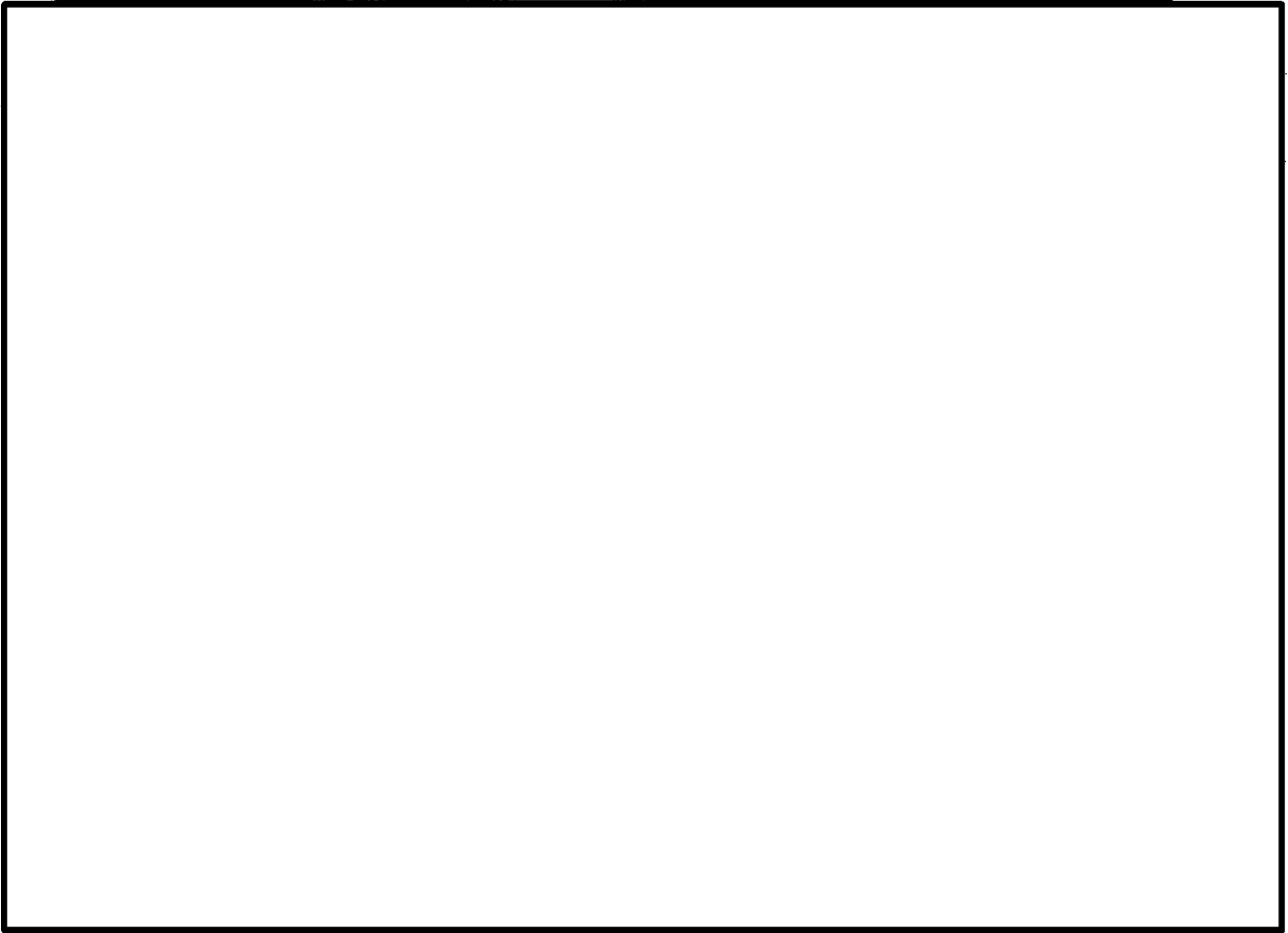
Field Resolution Process, Continued



(b)(5)

(b)(7)(e)

Field Resolution Process, Continued



Field Resolution Process, Continued

Figure VII-1: Completed ROIQ (Field)

Record of IBIS Query (ROIQ)						
A-Number or Receipt Number : <u>A12345678</u>						
#	Last Name, First Name	DOB	NO MATCH	DNR	RELATES	Resolution Memo Completed?
1	[Redacted]	2/15/78			9/1/05	<input checked="" type="checkbox"/>
		2 nd Check			1/10/06	<input checked="" type="checkbox"/>
		3 rd Check				
2		2/15/78	9/1/05 FFG			
		2 nd Check	1/10/06 SDF			
		3 rd Check				
3		6/29/76	9/1/05 FFG			
		2 nd Check	1/10/06 SDF			
		3 rd Check				
4		6/29/76		1/12/06	<input checked="" type="checkbox"/>	
		2 nd Check				
		3 rd Check				

X
 A P B D

Properly annotate IBIS results on the ROIQ:
 *Include the date of query in the appropriate box (NOMATCH, DNR, RELATES)
 *Include the initial/s or identifying number of the USCIS personnel conducting the query in the same box as the date.
 * If the hit was a RELATES and a Resolution Memo was completed, check the Resolution Memo Completed box in the last column.

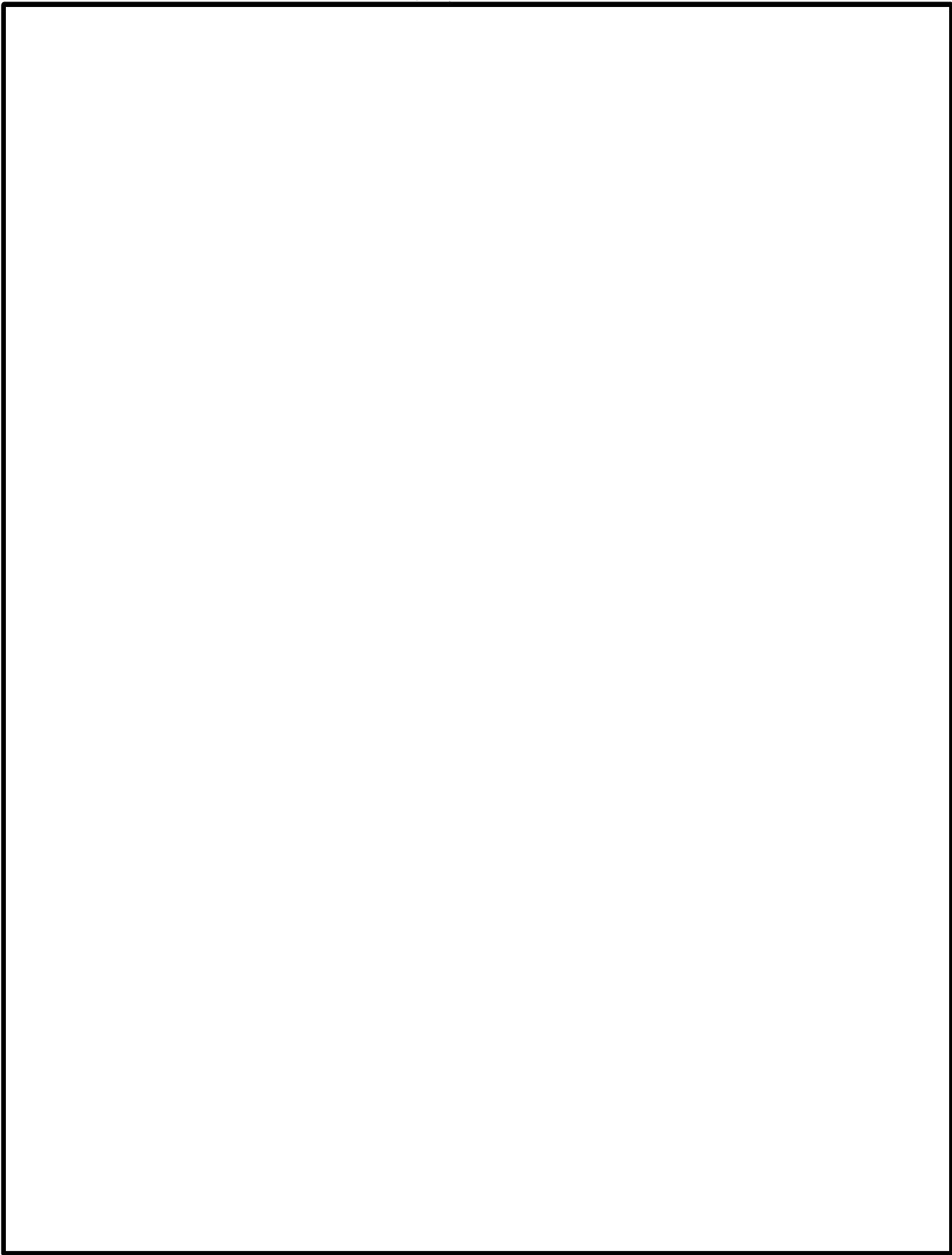
NOMATCH - No information found in IBIS
 DNR - Information found in IBIS but does not relate to the subject.
 RELATES - Information found in IBIS that relates to the subject, case referred for resolution
 A = Applicant P = Petitioner
 B = Beneficiary D = Derivative/Household Member

(b)(5)

(b)(7)(c)

Field Resolution Process, Continued

(b)(7)(e)



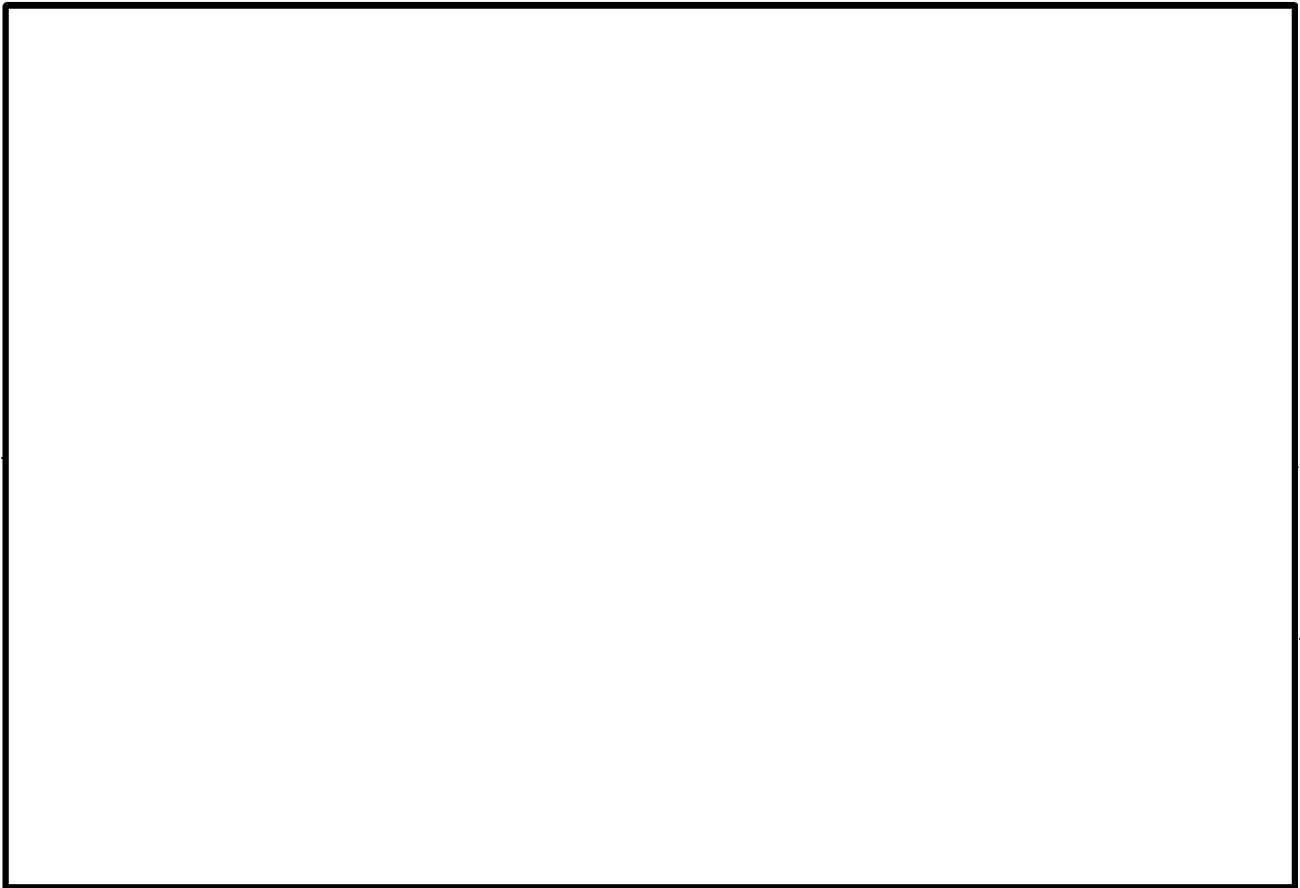
SECTION VIII:

FDU Resolution Process

(b)(5)

(b)(7)(e)

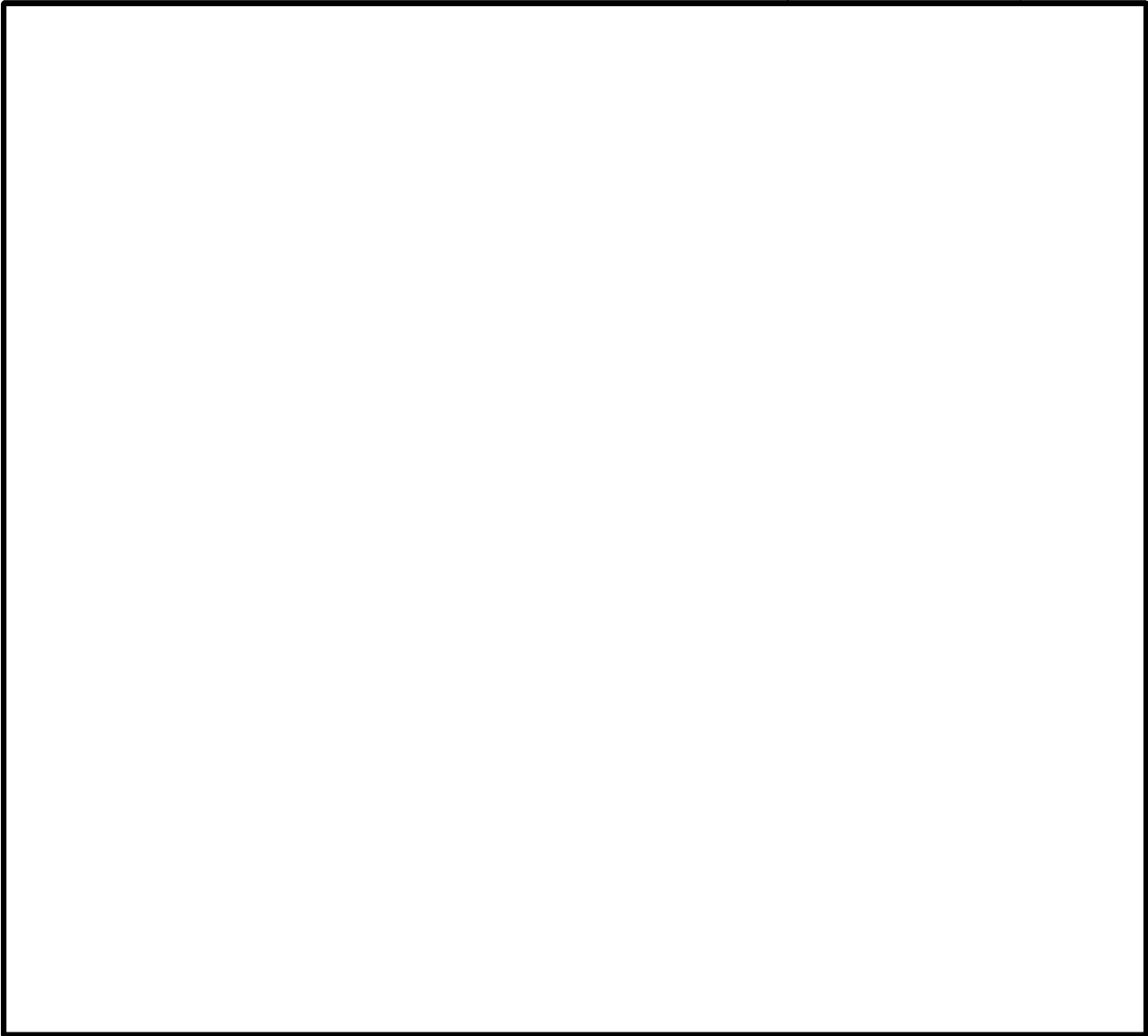
Section VIII: FDU Resolution Process



(b)(5)

(b)(7)(e)

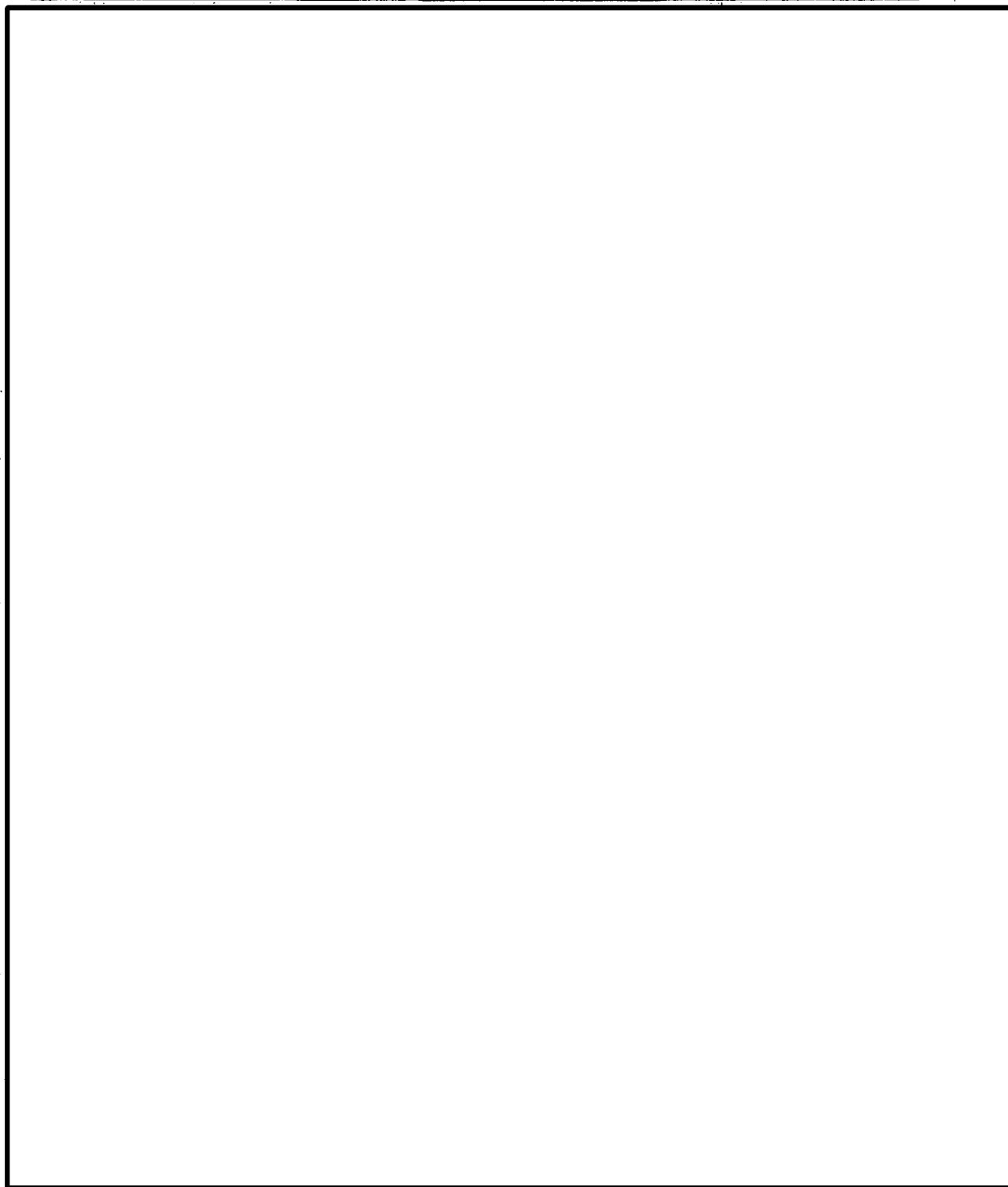
FDU Resolution Process, Continued



(b)(5)

(b)(7)(e)

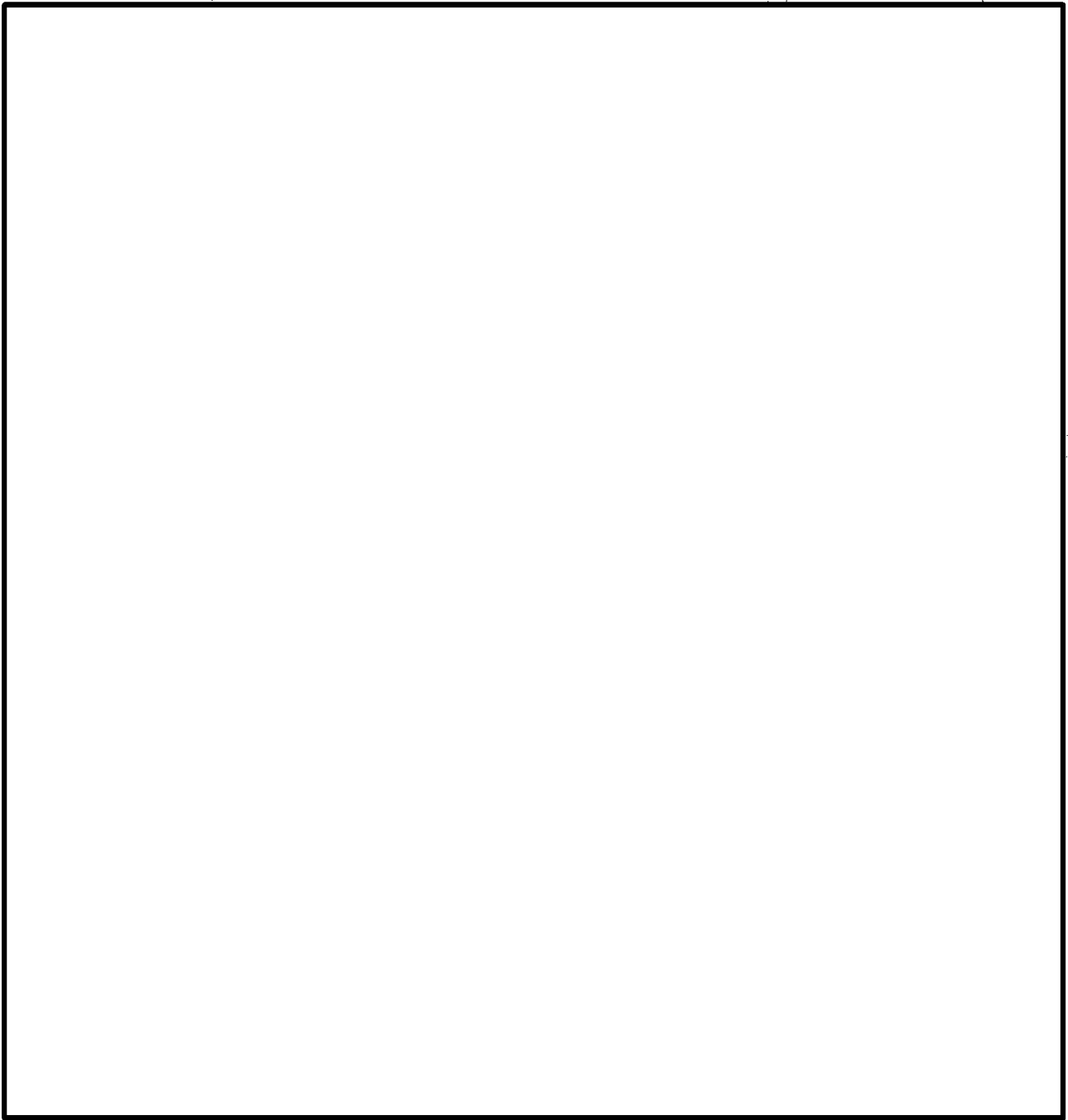
FDU Resolution Process, Continued



(b)(5)

(b)(7)(e)

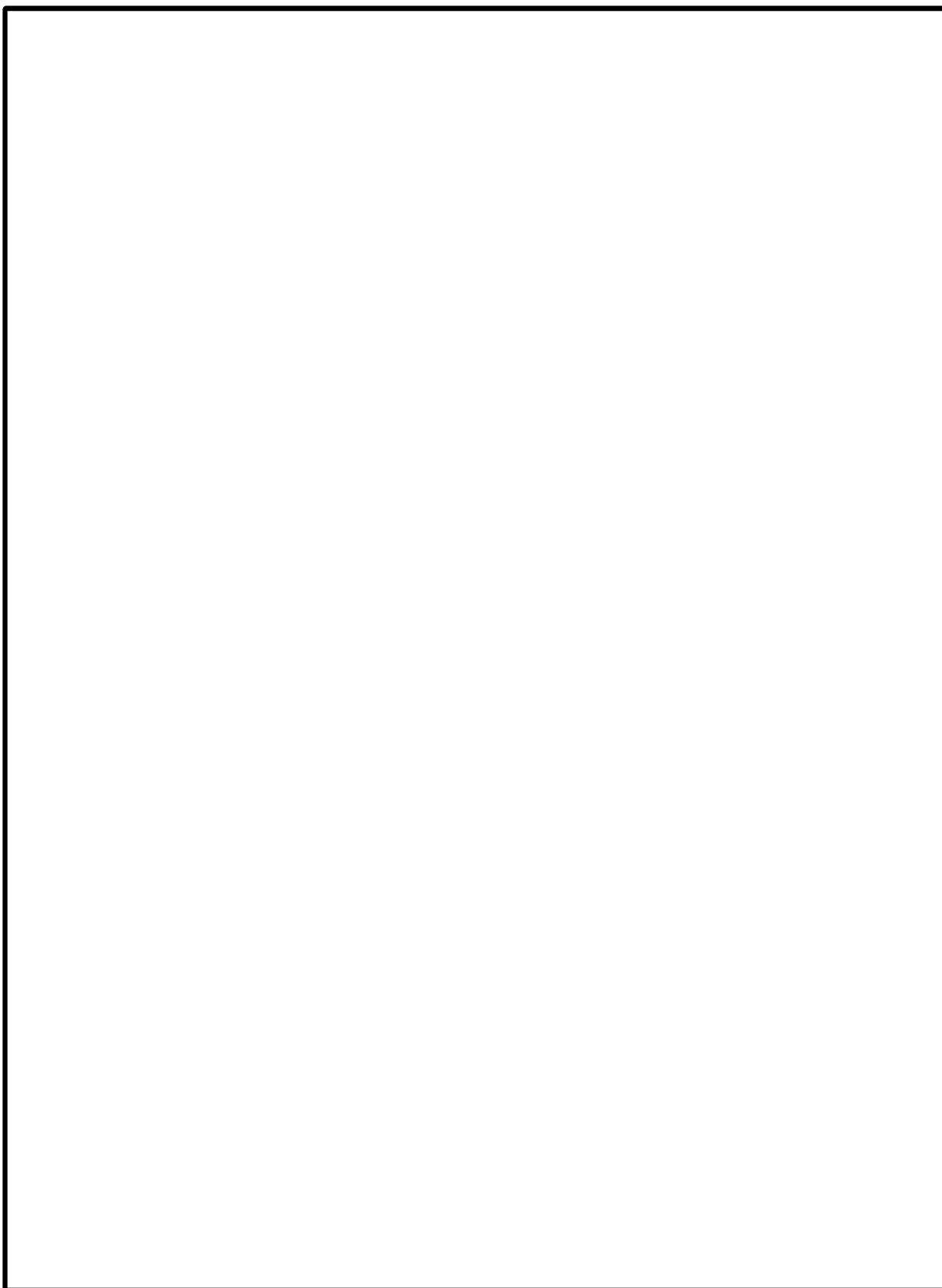
FDU Resolution Process, Continued



(b)(5)

(b)(7)(e)

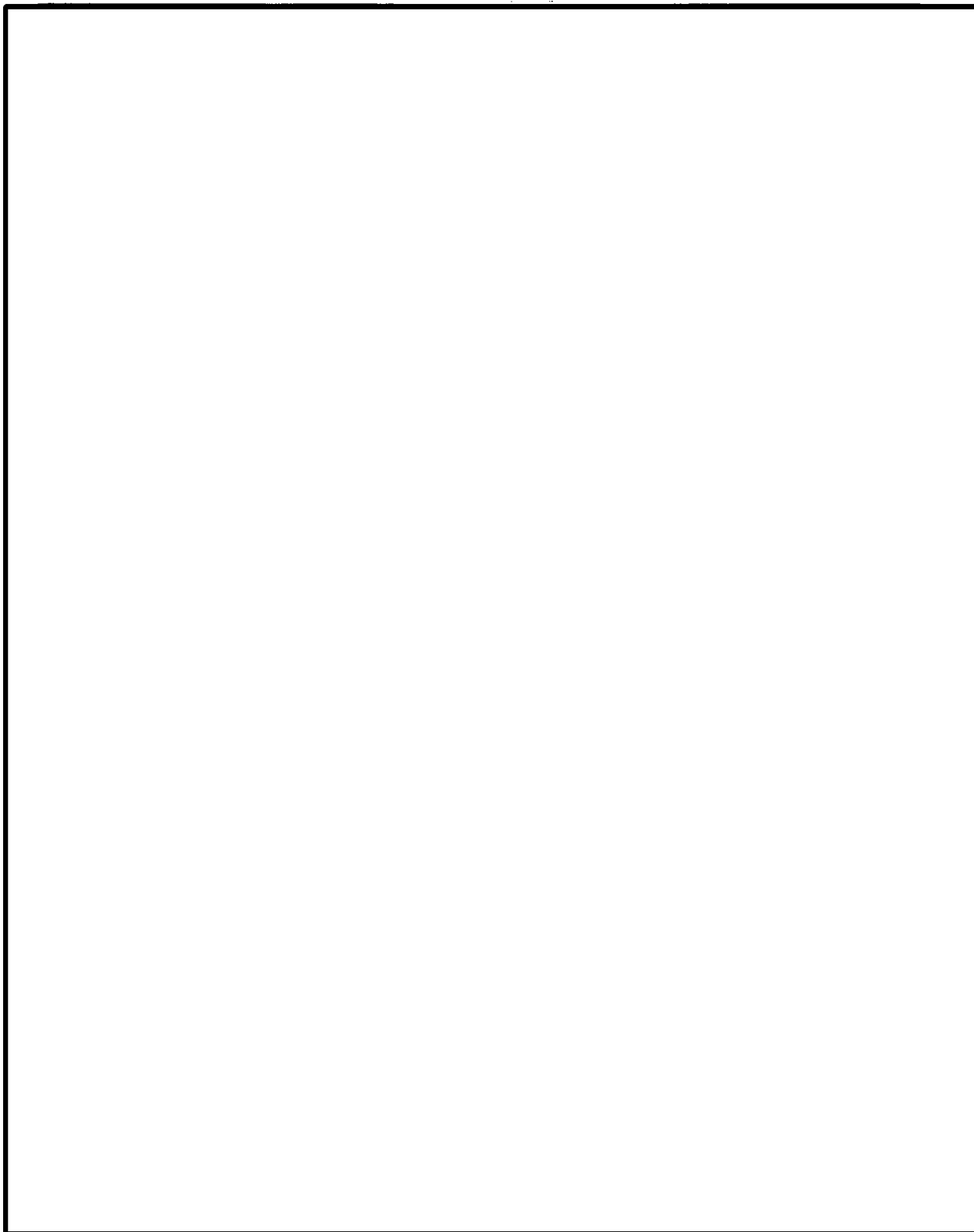
FDU Resolution Process, Continued



(b)(5)

(b)(7)(e)

FDU Resolution Process, Continued



(b)(5)

(b)(7)(e)

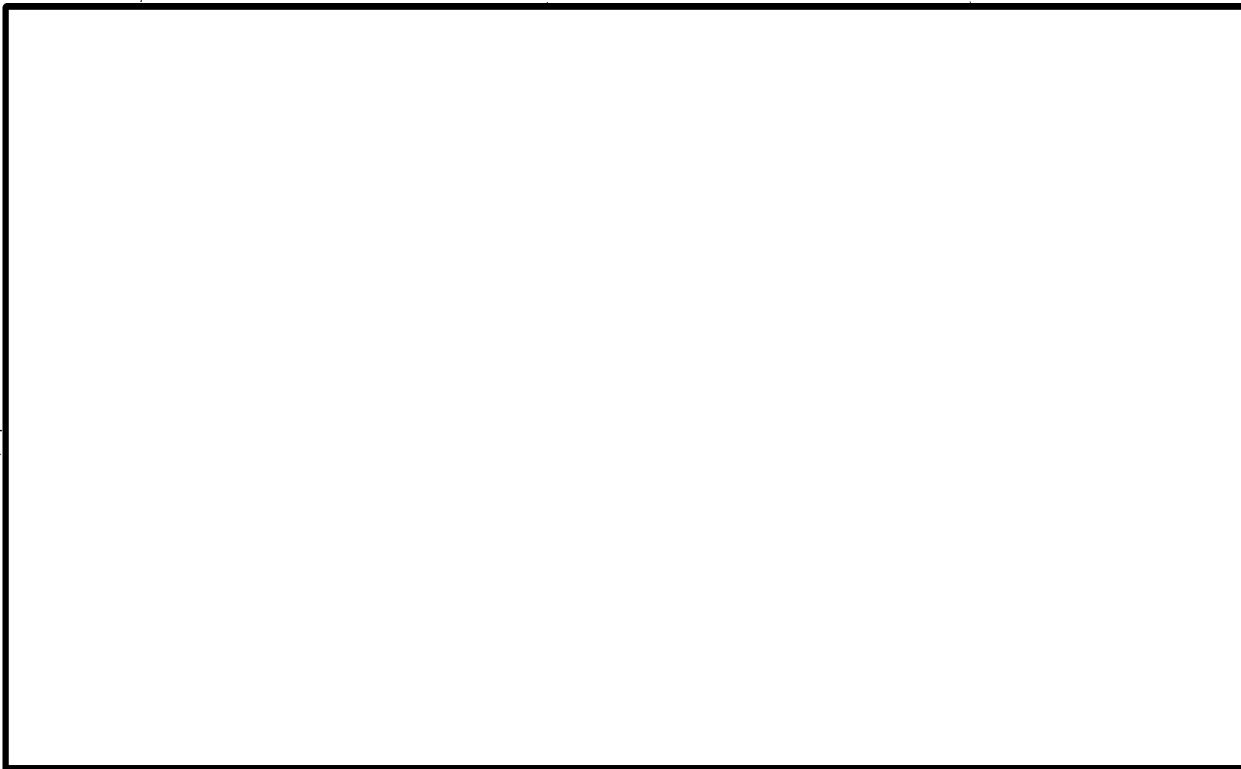
FDU Resolution Process, Continued



(b)(5)

(b)(7)(e)

FDU Resolution Process, Continued



Glossary

Glossary

About the Glossary

The following definitions are for the purpose of the IBIS SOP, in order to clearly explain the usage of these terms throughout this manual.

Glossary, Continued

Director	District Director and/or Center Director.
DOB	Date of Birth
DOS	Department of State
DNR	Does Not Relate. This annotation is used on the ROIQ if an IBIS query results in a hit that does not relate to the subject queried.
DRO	Detention and Removal Operations
EAD	Employment Authorization Document
Egregious Public Safety	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 is at least one year as defined in 101(a)(43)(F) INA; Human Rights Violators; Interpol hits; and 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.
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.
EOIR	Executive Office for Immigration Review

Glossary, Continued

FBI	Federal Bureau of Investigation	
FDNS	Headquarters Office of Fraud Detection and National Security	
FDNS-DS	Fraud Detection and National Security Data System	
FDU	Fraud Detection Unit, located at each Center.	
FDU Personnel	Intelligence Research Specialist and/or Investigative Assistant	
Field Office	District Office, Sub-Office, and/or Satellite Office.	
Final Decision	Approval, denial, abandonment denial, revocation, reaffirmation, or withdrawal of a benefit application/petition.	
FOCUS	A headquarters unit within the Office of Field Operations established to assist all USCIS offices in the adjudication of applications/petitions with identified national security and/or public safety concerns.	(b)(5) (b)(7)(e)
FPS	Federal Protective Service	



Glossary, Continued

Household Member	An individual living at the residence of an I-600 petitioner or an I-600A applicant.
HQ	Headquarters
IBIS	Interagency Border Inspection System, comprised of TECS and NCIC.
IBIS Certification Test	The online test that must be successfully completed by each user in order to obtain access to IBIS. Certification remains valid for two years, after which re-certification is required.
IBIS Hit	A record returned by IBIS in response to a query, the subject of which may or may not relate to the subject being queried. Same as System Match.
IBIS Query	A search in IBIS 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.
IBIS NSR	IBIS National Security Record
IBIS Record	A uniquely numbered and identifiable entry into TECS or NCIC made by a contributing agency.
IBIS Resolution Memo	Formal documentation of the reconciliation of a relating hit. The completion of this documentation is mandatory and must be completed before rendering a final decision.
ICE	Immigration and Customs Enforcement

Glossary, Continued

IJ	Immigration Judge
Interpol	International Criminal Police Organization, the world's largest international police organization. This organization facilitates cross-border police co-operation and supports and assists all organizations, authorities, and services whose mission is to prevent or combat international crime.
IO	Immigration Officer
IRS	Intelligence Research Specialist
ITU	IBIS Triage Unit, located at each Center.
JTTF	Joint Terrorism Task Force
KCC	Kentucky Consular Center
LPR	Lawful Permanent Resident
MOU	Memorandum of Understanding, which documents the agreement between the United States Custom Service and the Immigration and Naturalization Service for the use of IBIS, the protection of IBIS data, and the adherence to common procedures for the effective sharing of sensitive law enforcement and related information. This document applies in its entirety to USCIS.

Glossary, Continued

NACI	National Agency Check with Inquiries
NBC	National Benefits Center
NCIC	National Crime Information Center
NCIC Certification Test	The online test that must be successfully completed by each IBIS user in order to obtain access to NCIC information. Certification remains valid for two years, after which re-certification is required.
NCIC III	National Crime Information Center Interstate Identification Index
NLETS	National Law Enforcement Telecommunications System
NN-16 Query	A query of NCIC III conducted when other background check procedures indicate the subject on the application/petition may have an issue of criminality.
No Match	This annotation is used on the ROIQ if an IBIS query results in no IBIS hit.
NSEERS	National Security Entry Exit Registration System
NSN	National Security Notification

Glossary, Continued

RFI	Referral for Investigation
ROIQ	Record of IBIS Query. This form is used to record the search criteria queried and the results of those queries.
ROP	Record of Proceeding
SCO	System Control Officer, the local USCIS officer who is responsible for implementing USCIS policy for IBIS use and coordinating the designation and assignment of the IBIS access for all applicable USCIS personnel. This officer serves as the local point of contact within USCIS for general IBIS access issues.
Search Criteria	The search criteria for an SQ-11 query include last name, first name and date of birth of a subject. The search criteria for an SQ-16 query are comprised of the name of the business or school.
SEVIS	Student and Exchange Visitor Information System
SQ-11 Query	Person Subject Query
SQ-16 Query	Organization Subject Query
Supporting Documentation	Documentation provided by the applicant, petitioner, or their designee in conjunction with an application/petition. This documentation includes all USCIS required forms and documents that establish relationship or identity.
System Match	A record returned by IBIS in response to a query, the subject of which may or may not relate to the subject being queried. Same as IBIS Hit.

Glossary, Continued

(b)(7)(e) **TECS** Treasury Enforcement Communications System

(b)(5) **Terrorist** Defined in 212(a)(3) INA and 237(a)(4) INA.

USC United States Citizen

USCIS United States Citizenship and Immigration Services

USCIS Personnel A person employed by USCIS or a company or agency that entered into a contract with USCIS to perform specified functions.

Valid IBIS Query A query completed within the previous 90 days. A final adjudicative decision cannot be made if all required IBIS queries have not been conducted within the previous 90-day period.

VAWA Violence Against Women Act

Work Folder An unofficial file created at a local office for working purposes.

Appendix

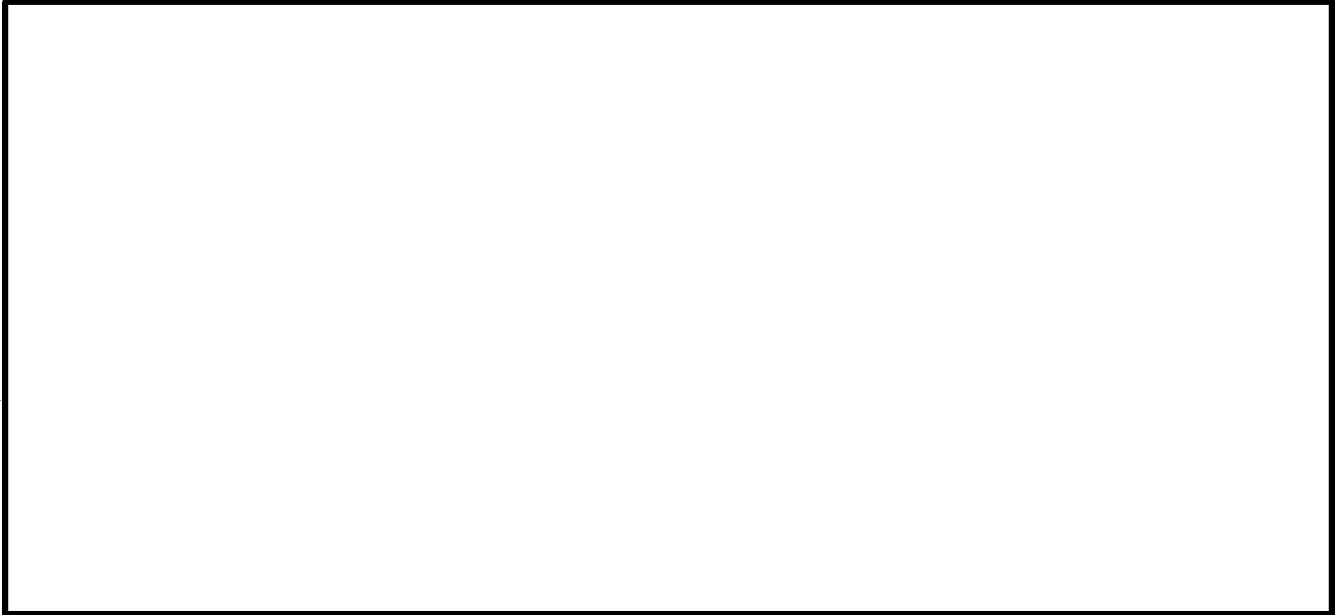
Appendix, Continued

**APPENDIX A
Guide to IBIS Hits**

(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(7)(e)

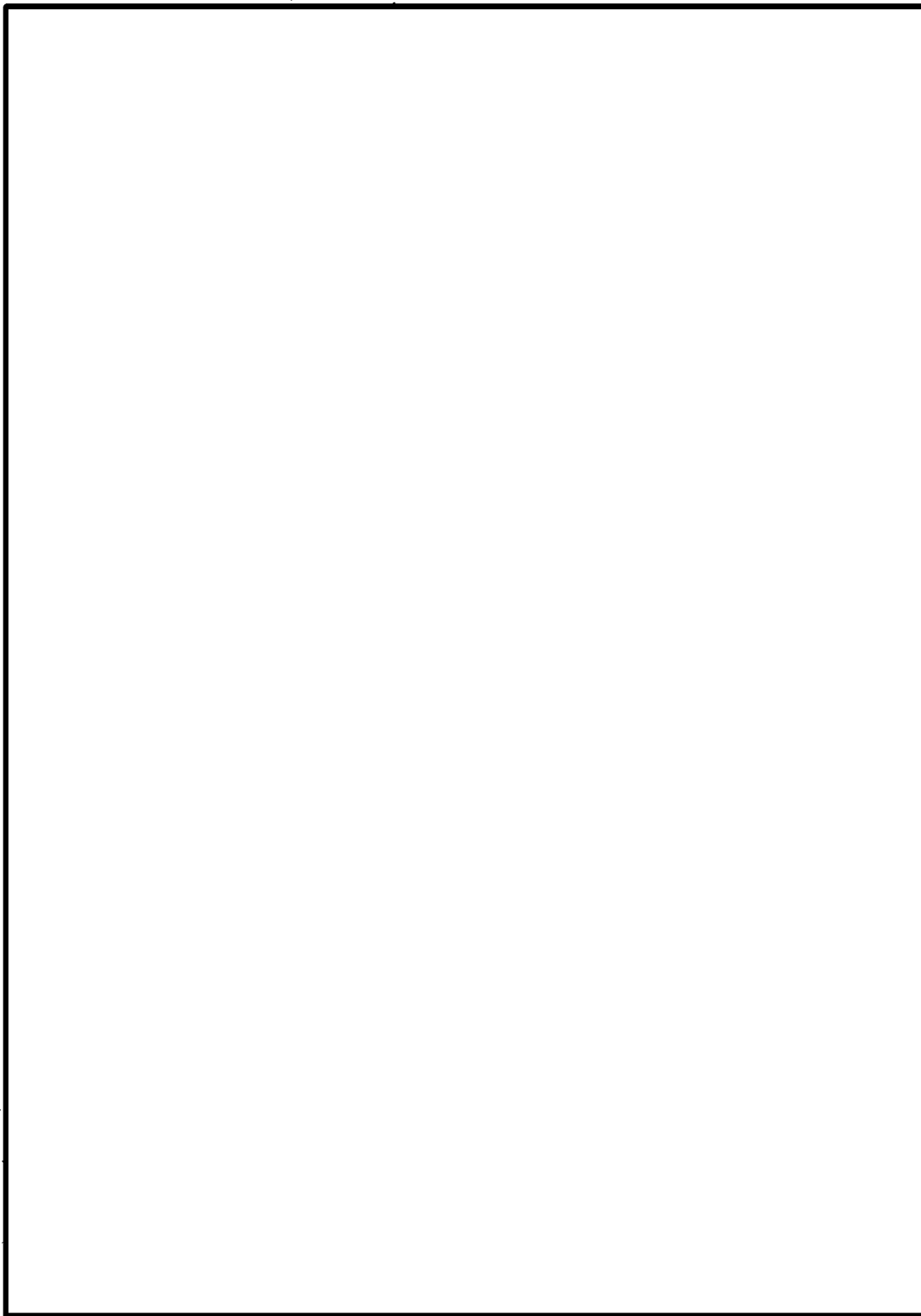
(b)(5)

Appendix, Continued

TERMS AND ACRONYMS

(b)(7)(e) (b)(5)

Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(7)(e)

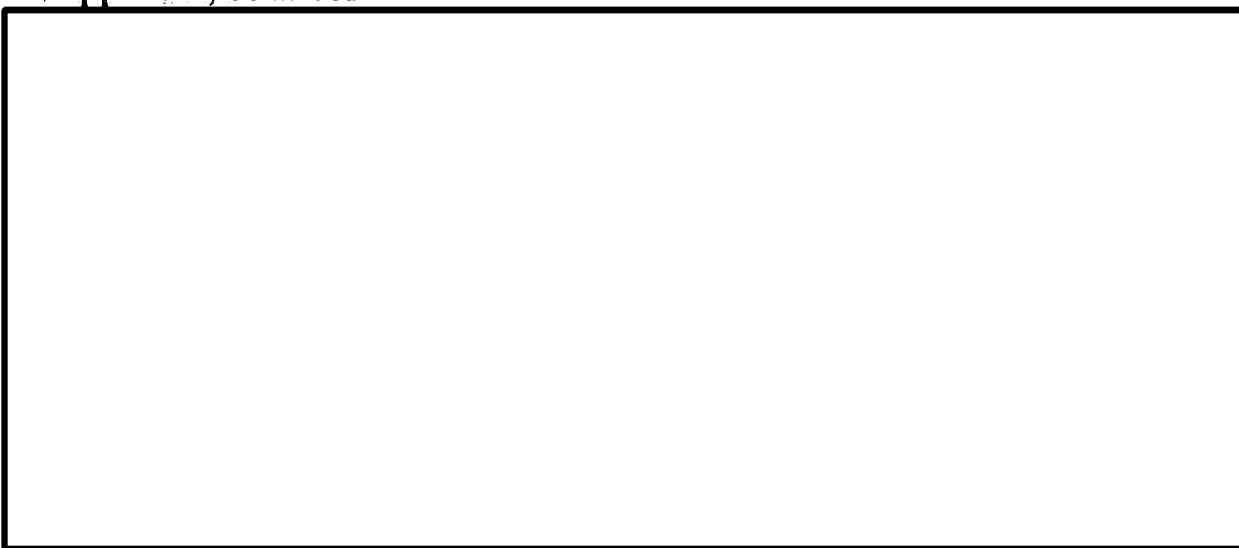
(b)(5)

Appendix, Continued

(b)(5)

(b)(7)(e)

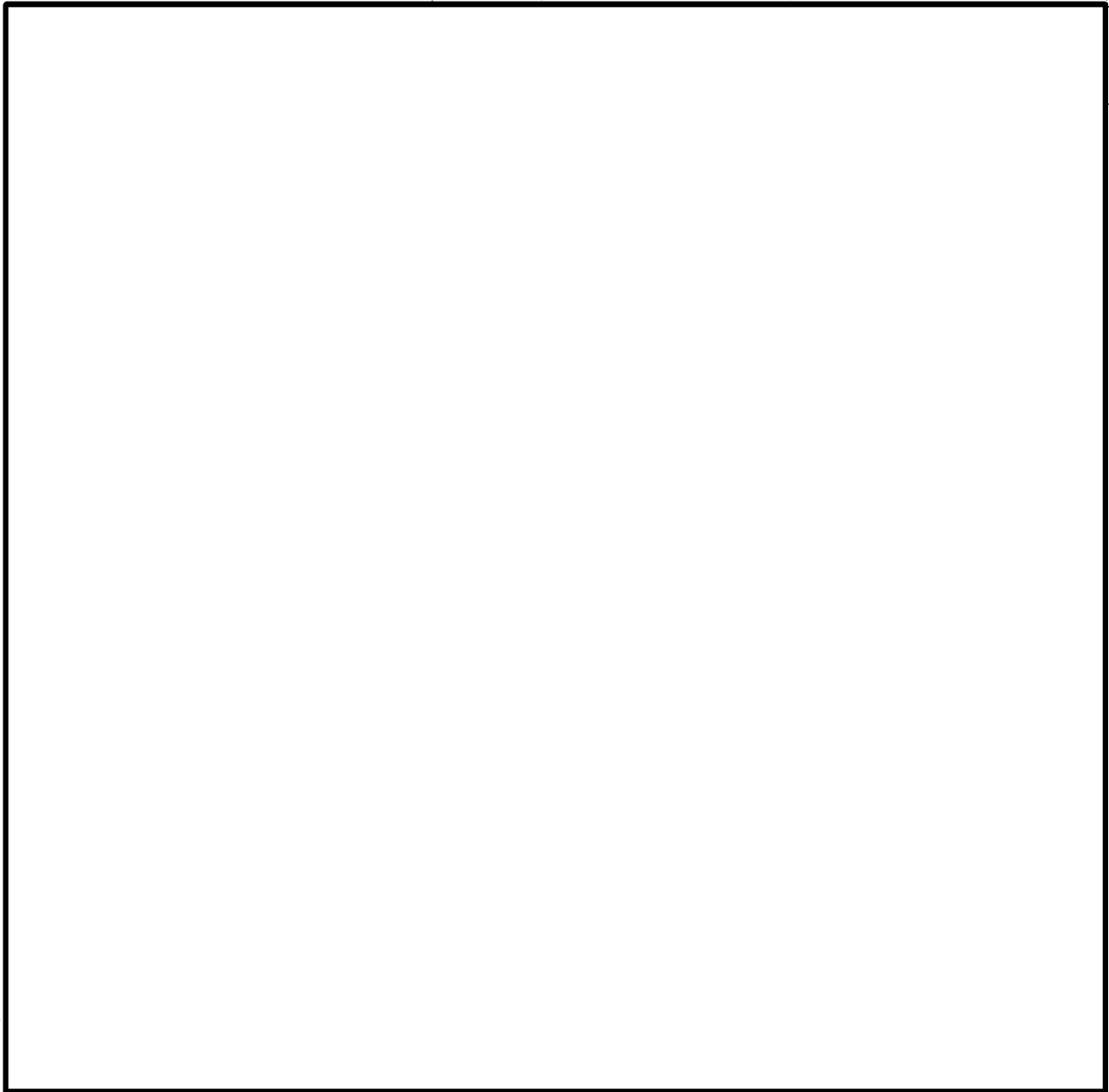
Appendix, Continued



(b)(5)

(b)(7)(e)

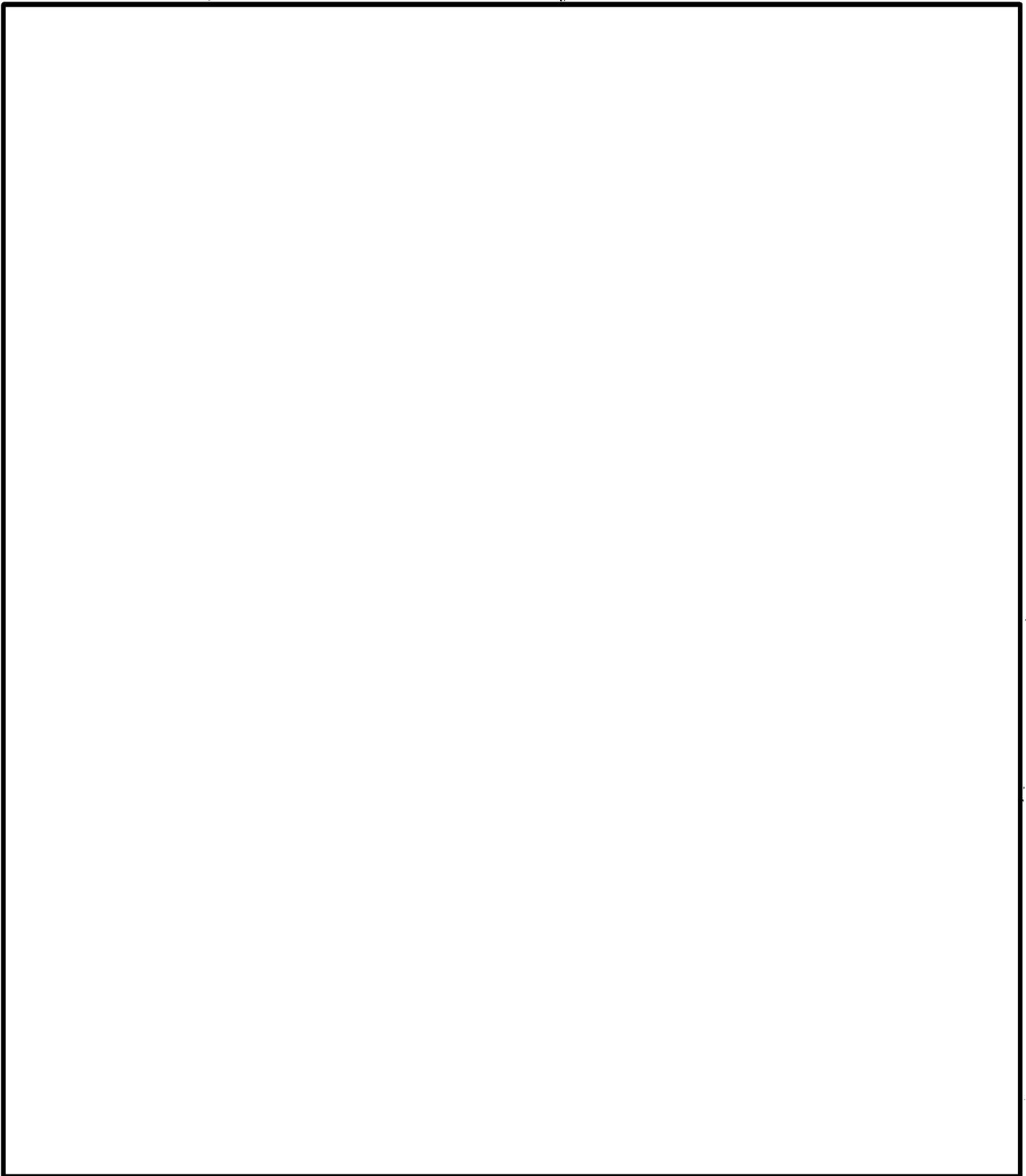
Appendix, Continued



(b)(7)(e)

(b)(5)

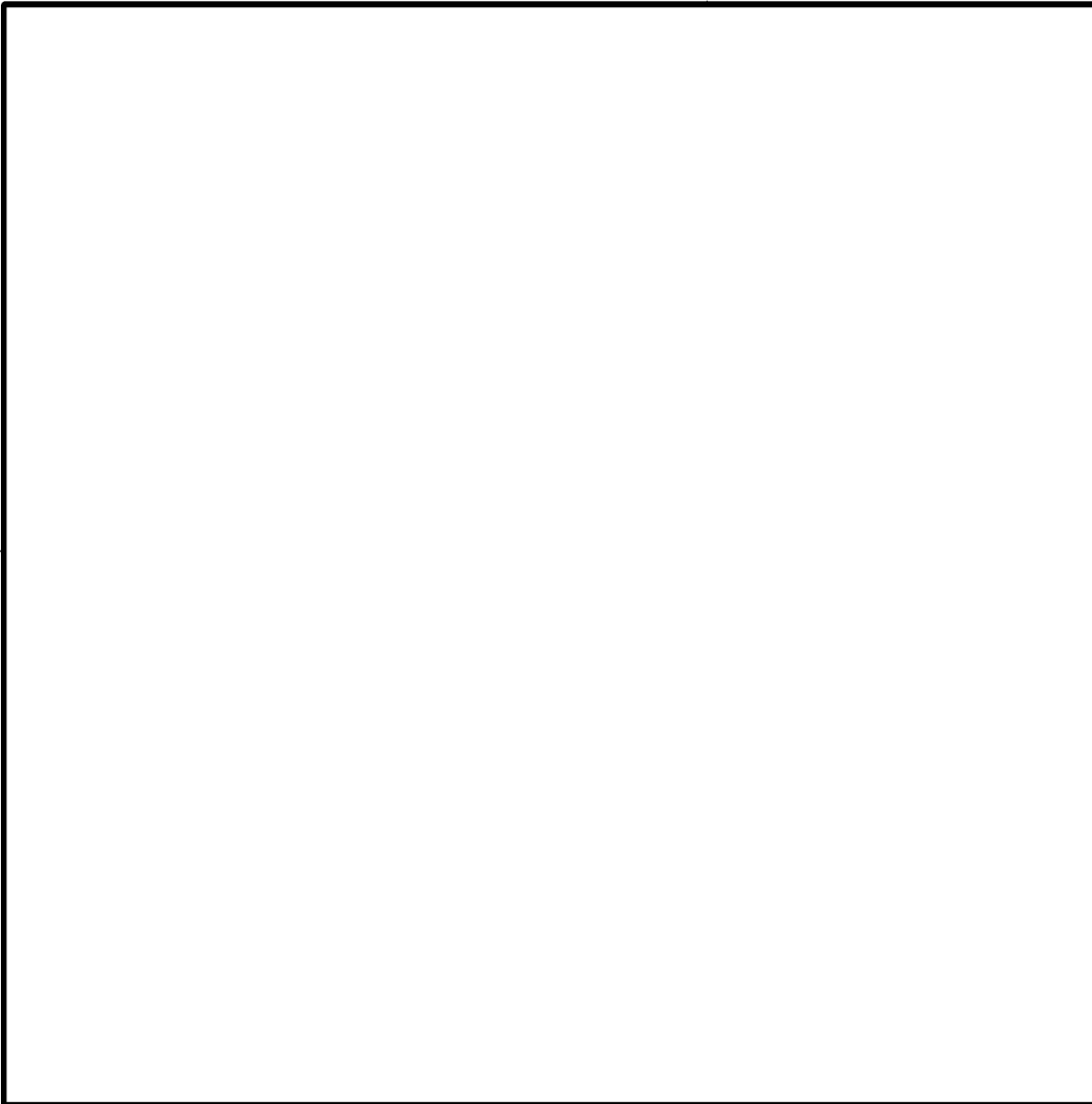
Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



Appendix, Continued

APPENDIX B
Fact Sheet: Federal Regulations Protecting the
Confidentiality of Asylum Applicants

Appendix, Continued

Prepared by the USCIS Asylum Division
Date: June 3, 2005

Fact Sheet: Federal Regulations Protecting the Confidentiality of Asylum Applicants

Synopsis

The federal regulations at 8 CFR 208.6 generally prohibit the disclosure to third parties of information contained in or pertaining to asylum applications, credible fear determinations, and reasonable fear determinations—including information contained in RAPS or APSS¹—except under certain limited circumstances. These regulations safeguard information that, if disclosed publicly, could 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 members who may still be residing in the country of origin. Moreover, public disclosure might, albeit in rare circumstances², 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.

According to established guidance, confidentiality is breached when information contained in or pertaining to an asylum application (including information contained in RAPS or APSS) is disclosed to a third party in violation of the regulations, and the unauthorized disclosure is of a nature that allows the third party to link the identity of the applicant to: (1) the fact that the applicant has applied for asylum; (2) specific facts or allegations pertaining to the individual asylum claim contained in an asylum application; or (3) facts or allegations that are sufficient to give rise to a reasonable inference that the applicant has applied for asylum. The same principles generally govern the disclosure of information related to credible fear and reasonable fear determinations, as well as to applications for withholding or deferral of removal under Article 3 of the Convention Against Torture, which are encompassed within the asylum application.

In the absence of the asylum applicant's written consent or the Secretary of Homeland Security's³ specific authorization, disclosure may be made only to United States government officials or contractors and United States federal or state courts on a need to know basis related to certain administrative, law enforcement, and civil actions. In some instances, interagency arrangements have been established – such as the arrangement between the former INS and the FBI -- to facilitate the proper disclosure of asylum-related information to United States agencies pursuant to the regulations. The release of information relating to an asylum application,

¹RAPS is the system for maintenance of records concerning aliens who affirmatively seek asylum by applying for the benefit with USCIS. APSS is the system for maintenance of records concerning aliens referred to a USCIS asylum officer for a credible fear or reasonable fear screening determination after having expressed a fear of return to the intended country of removal because of fear of persecution or torture during the expedited removal process under INA sec. 235(b) or administrative removal processes under INA sec. 238(b) or INA sec. 241(a)(5).

²Public disclosure alone will rarely be sufficient to establish *sur place* protection claims under U.S. asylum laws. The applicant would have to establish, in light of this disclosure, that he or she has a well-founded fear of persecution on account of one of the protected grounds.

³By operation of section 1512(d) of the Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135, 2310, the Attorney General's authority under 8 C.F.R. § 208.6(a) to authorize disclosure of confidential asylum information held by the former Immigration and Naturalization Service (INS)—and now held by the Department of Homeland Security (DHS)—was transferred to the Secretary of DHS.

Appendix, Continued

Prepared by the USCIS Asylum Division
Date: June 3, 2005

credible fear determination, or reasonable fear determination (including information contained in RAPS or APSS) to an official of another government or to any entity for purposes not specifically authorized by the regulations without the written consent of the claimant requires the express permission of the Secretary of Homeland Security.

Code of Federal Regulations, Title 8

Sec. 208.6 Disclosure to third parties.

(a) Information contained in or pertaining to any asylum application, records pertaining to any credible fear determination conducted pursuant to § 208.30, and records pertaining to any reasonable fear determination conducted pursuant to § 208.31, shall not be disclosed without the written consent of the applicant, except as permitted by this section or at the discretion of the Attorney General [now the Secretary of DHS].

(b) The confidentiality of other records kept by the [Immigration and Naturalization] Service [now DHS] and the Executive Office for Immigration Review that indicate that a specific alien has applied for asylum, received a credible fear or reasonable fear interview, or received a credible fear or reasonable fear review shall also be protected from disclosure. The Service [now DHS] will coordinate with the Department of State to ensure that the confidentiality of those records is maintained if they are transmitted to Department of State offices in other countries.

(c) This section shall not apply to any disclosure to:

(1) Any United States Government official or contractor having a need to examine information in connection with:

(i) The adjudication of asylum applications;

(ii) The consideration of a request for a credible fear or reasonable fear interview, or a credible fear or reasonable fear review;

(iii) The defense of any legal action arising from the adjudication of, or failure to adjudicate, the asylum application, or from a credible fear determination or reasonable fear determination under § 208.30 or § 208.31;

(iv) The defense of any legal action of which the asylum application, credible fear determination, or reasonable fear determination is a part; or

(v) Any United States Government investigation concerning any criminal or civil matter; or

(2) Any Federal, State, or local court in the United States considering any legal action:

(i) Arising from the adjudication of, or failure to adjudicate, the asylum application, or from a credible fear or reasonable fear determination under § 208.30 or § 208.31; or (ii) Arising from the proceedings of which the asylum application, credible fear determination, or reasonable fear determination is a part.

Frequently Asked Questions

1. Q: Why do the regulations protect asylum-related information from disclosure?

A: Public disclosure of asylum-related 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 members who may still be residing in the country of origin. Moreover, public disclosure might, albeit in rare circumstances (see footnote #2), 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.

Appendix, Continued

Prepared by the USCIS Asylum Division
Date: June 3, 2005

2. Q: Under what specific circumstances can asylum-related information be disclosed to third parties?

A: In general, asylum-related information must not be shared with third parties without the asylum applicant's written consent or the Secretary of Homeland Security's specific authorization. However, this general prohibition does not apply to the following limited circumstances as established by the regulations at 8 CFR 208.6:

"(1) Any United States Government official or contractor having a need to examine information in connection with:

- (i) The adjudication of asylum applications;
 - (ii) The consideration of a request for a credible fear or reasonable fear interview, or a credible fear or reasonable fear review;
 - (iii) The defense of any legal action arising from the adjudication of, or failure to adjudicate, the asylum application, or from a credible fear determination or reasonable fear determination under § 208.30 or § 208.31;
 - (iv) The defense of any legal action of which the asylum application, credible fear determination, or reasonable fear determination is a part; or
 - (v) Any United States Government investigation concerning any criminal or civil matter; or
- (2) Any Federal, State, or local court in the United States considering any legal action:
- (i) Arising from the adjudication of, or failure to adjudicate, the asylum application, or from a credible fear or reasonable fear determination under § 208.30 or § 208.31; or
 - (ii) Arising from the proceedings of which the asylum application, credible fear determination, or reasonable fear determination is a part."

3. Q: To what extent may asylum-related information be disclosed to personnel within the Department of Homeland Security (DHS), such as the Immigration and Customs Enforcement (ICE) or Customs or Border Protection (CBP) personnel?

A: Protected asylum-related information may be disclosed to CBP and ICE, as they are not considered "third parties" for purposes of 208.6 and, therefore, requesters from those former INS components need not demonstrate a "need to examine" protected asylum information. Information may also be disclosed to offices within the direct policy and legal chains of command of DHS, such as DHS Office of General Counsel, the Office of the Undersecretary for Border and Transportation Security (BTS), Office of the Deputy Secretary, and the Office of the Secretary.

4. Q: If none of the regulatory exceptions applies, what information about an asylum applicant, if any, may be shared with third parties without breaching confidentiality?

A: According to established guidance, confidentiality is breached when information contained in or pertaining to an asylum application is disclosed to a third party in violation of the regulations, and the unauthorized disclosure is of a nature that allows the third party to link the identity of the applicant to: (1) the fact that the applicant has applied for asylum; (2) specific facts or allegations pertaining to the individual asylum claim contained in an asylum application; or (3) facts or allegations that are sufficient to give rise to a reasonable inference that the applicant has applied for asylum. The same principles govern the disclosure of information related to credible fear and reasonable fear determinations. They also generally apply to

Appendix, Continued

Prepared by the USCIS Asylum Division
Date: June 3, 2005

applications for withholding or deferral of removal under Article 3 of the Convention Against Torture, which are encompassed within the asylum application.

5. Q: Under the regulation's exceptions, can asylum-related information be disclosed to state law enforcement agencies or other state agencies?

A: No. The confidentiality regulations do not allow disclosure of asylum-related information to state agencies, including state law enforcement agencies, except with the asylum applicant's written consent or the Secretary of Homeland Security's specific authorization. The regulations at 208.6(c)(2) do, however, allow for disclosure to state or local courts in certain circumstances.

6. Q: How can a United States Government official or contractor, who is seeking asylum-related information and to whom asylum-related information may be disclosed under the regulations, obtain asylum-related information from USCIS?

A: Unless there is a pre-existing interagency arrangement or protocol (such as the arrangement between the former INS and the FBI), federal agency officials or contractors should request asylum-related information about specific aliens directly from the appropriate United States Citizenship and Immigration Services (USCIS) Asylum Office Director with jurisdiction over the alien's application. Requests for asylum-related information concerning groups of aliens that match certain identified criteria must be made to the Director of the Asylum Division of USCIS by the appropriate official in the requesting agency.

7. Q: If asylum-related information is properly disclosed to a third party pursuant to the regulations, what is the third party's obligation with respect to confidentiality?

A: As the new custodian of the asylum-related information, the third-party recipient is bound by the confidentiality regulations under 8 CFR 208.6. The recipient must not disclose the asylum-related information to other parties, except pursuant to the regulations. When making an authorized disclosure of asylum-related information to a third party, USCIS officials should alert the third party to the confidentiality requirements of 8 CFR 208.6.

8. Q: What are the obligations of U.S. government officials or contractors who work with or are responsible for maintaining asylum-related data in U.S. government systems?

A: U.S. government officials or contractors who encounter asylum-related data in their work are bound by the confidentiality regulations under 8 CFR 208.6. These handlers of asylum-related data must not disclose the asylum-related information to third parties, except in keeping with the regulations.

9. Q: Are non-USCIS custodians of asylum-related information required to obtain authorization from USCIS before disclosing the asylum-related information to another party pursuant to the regulations?

A: No. However, the transmitter of information should take reasonable steps to ensure that the new recipient of information is aware of the confidentiality rules described in this document to prevent unauthorized disclosure by the new recipient. In fact, it might be prudent to provide the new recipient this document for that purpose.

10. Q: What is the special arrangement between the FBI and USCIS concerning the disclosure of asylum-related information?

Appendix, Continued

Prepared by the USCIS Asylum Division
Date: June 3, 2005

A: As established in an October 8, 2001 memorandum, the Attorney General has used his discretionary authority under 8 CFR 208.6 (now belonging to the Secretary of Homeland Security) to provide the FBI access to asylum applications filed with USCIS for the purpose of gathering foreign counterintelligence or international terrorism information unrelated to pending criminal or civil litigation. Where the request relates to a specific alien, the request should be made to the Director of the appropriate USCIS Asylum Office and be approved by the FBI Field Office Special Agent in Charge or an appropriate Assistant Special Agent in Charge. Where the request relates to an explicitly identified group of aliens, the request will be made to the Director of the Asylum Division of USCIS and be approved by the FBI Field Office Special Agent in Charge or an appropriate Assistant Special Agent in Charge.

11. Q: Can asylum-related information be shared with foreign governments or international organizations (such as INTERPOL)?

A: Asylum-related information cannot be shared with foreign governments or international organizations without the written consent of the asylum applicant, except at the discretion of the Secretary of Homeland Security. To date, the Secretary has exercised his discretion to permit regular sharing of asylum-related information with a foreign government only with respect to Canada. The arrangement is in the form of a *Statement of Mutual Understanding on Information Sharing* (SMU) and an Annex to the SMU, which together permit Canada's Department of Citizenship and Immigration Canada (CIC) and USCIS to exchange asylum-related records on both a case-by-case and systematic basis.

12. Q: Why is there a special information-sharing agreement with Canada?

A: Sharing information on asylum seekers was included as an initiative in the agreement signed by Attorney General Ashcroft and former Minister of Citizenship and Immigration Caplan on December 2, 2001. It is also one of the thirty initiatives included in the Ridge-Manley Smart Border Action Plan. In furtherance of this initiative, the United States and Canadian governments entered into a formal arrangement in 2003 that permits USCIS and CIC to systematically share information on individuals seeking asylum in Canada and the United States. By gaining access to this key information, USCIS and CIC will enhance their abilities to prevent abuse of the asylum process in their respective countries and to make accurate asylum eligibility determinations, thereby strengthening the integrity of both countries' asylum systems.

13. Q: What is the status of the implementation of the information-sharing arrangement with Canada?

A: USCIS and CIC have already begun to share information on asylum seekers on a case-by-case basis. With regard to the systematic sharing of information, USCIS and CIC and their technical specialists are working together to develop protocols for the process of comparing and matching biometrically shared data sets.

14. Q: Has the Secretary of Homeland Security exercised his discretion to authorize disclosure of information to third parties in other instances (besides disclosure to the FBI and to Canada)?

A: Yes. In 2002, the Attorney General authorized the Asylum Division to disclose to the Office of Refugee Resettlement (ORR) of the Department of Health and Human Services (HHS) biographical information on individuals granted asylum to enable ORR to meet congressional

Appendix, Continued

Prepared by the USCIS Asylum Division
Date: June 3, 2005

reporting requirements and generate statistical reports used to allocate funding for asylee social benefits. In addition, in 2001 the Attorney General authorized the Asylum Division to disclose to HHS certain biographical information on asylees to enable ORR and the Center for Disease Control (CDC) to provide emergency relief to qualified asylees. The Attorney General and the Secretary have, in rare circumstances, also authorized disclosure on specific asylum seekers on a case-by-case basis for state law enforcement agencies, foreign governments, and members of Congress.

15. Q: May protected asylum-related information be shared with congressional offices?

A: If the Chairman of a congressional committee with competent jurisdiction submits a written request for protected asylum-related information, then the requested information will generally be provided without regard to the regulation. Written requests for asylum-related by individual Members of Congress or their respective staff members will be considered on a case-by-case basis.

16. Q: What information can be shared with the press when the applicant has gone public with the asylum claim?

A: Because the regulation currently requires the applicant's "written consent," we generally do not recognize implicit waivers of confidentiality, even when the asylum-related material is a matter of public record.

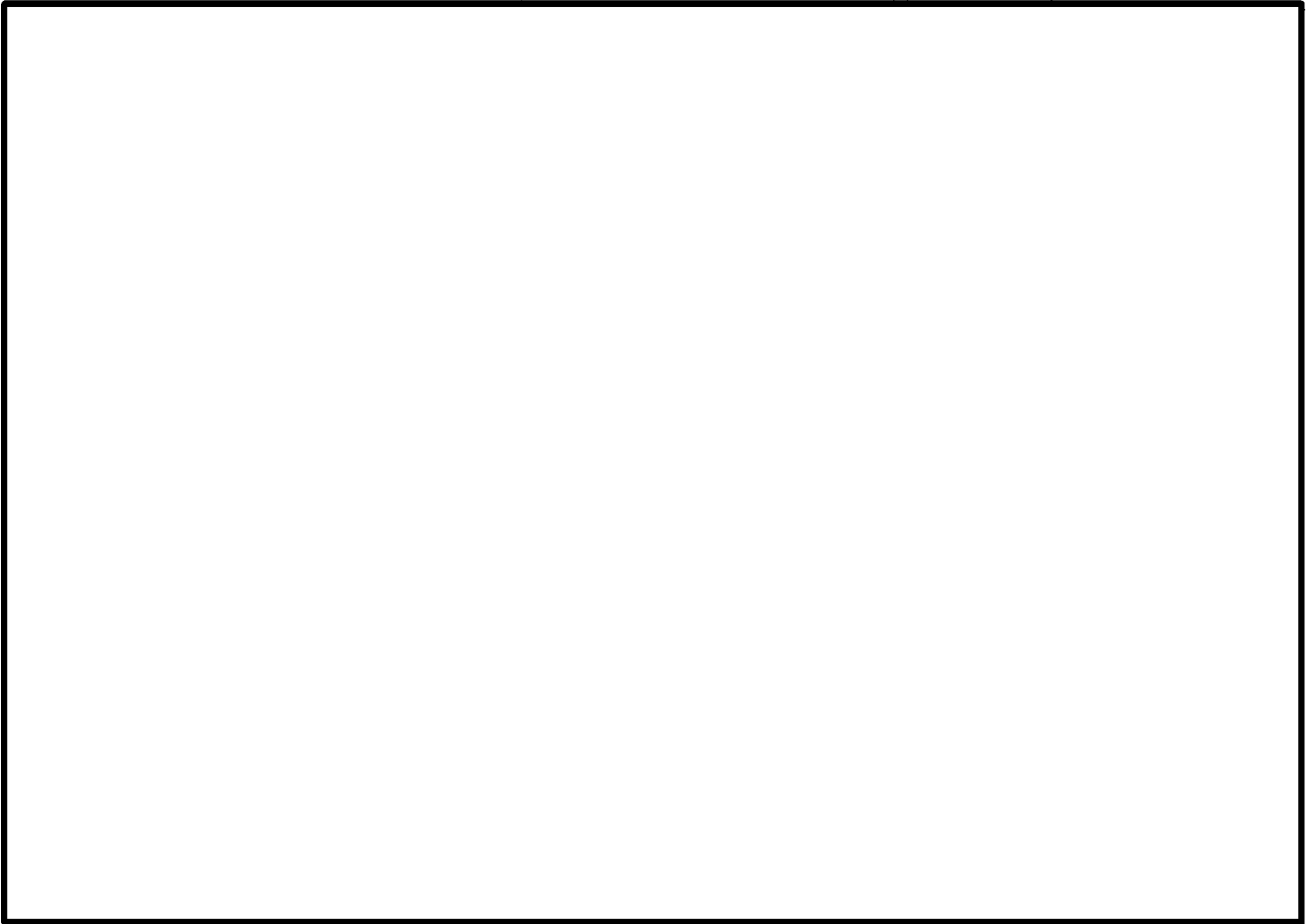
If you have any questions regarding these policies, please contact Ted Kim at 202.272.1615.

Appendix, Continued

APPENDIX C
Reading an NCIC Query Response

(b)(5)

(b)(7)(e) **Appendix, Continued**



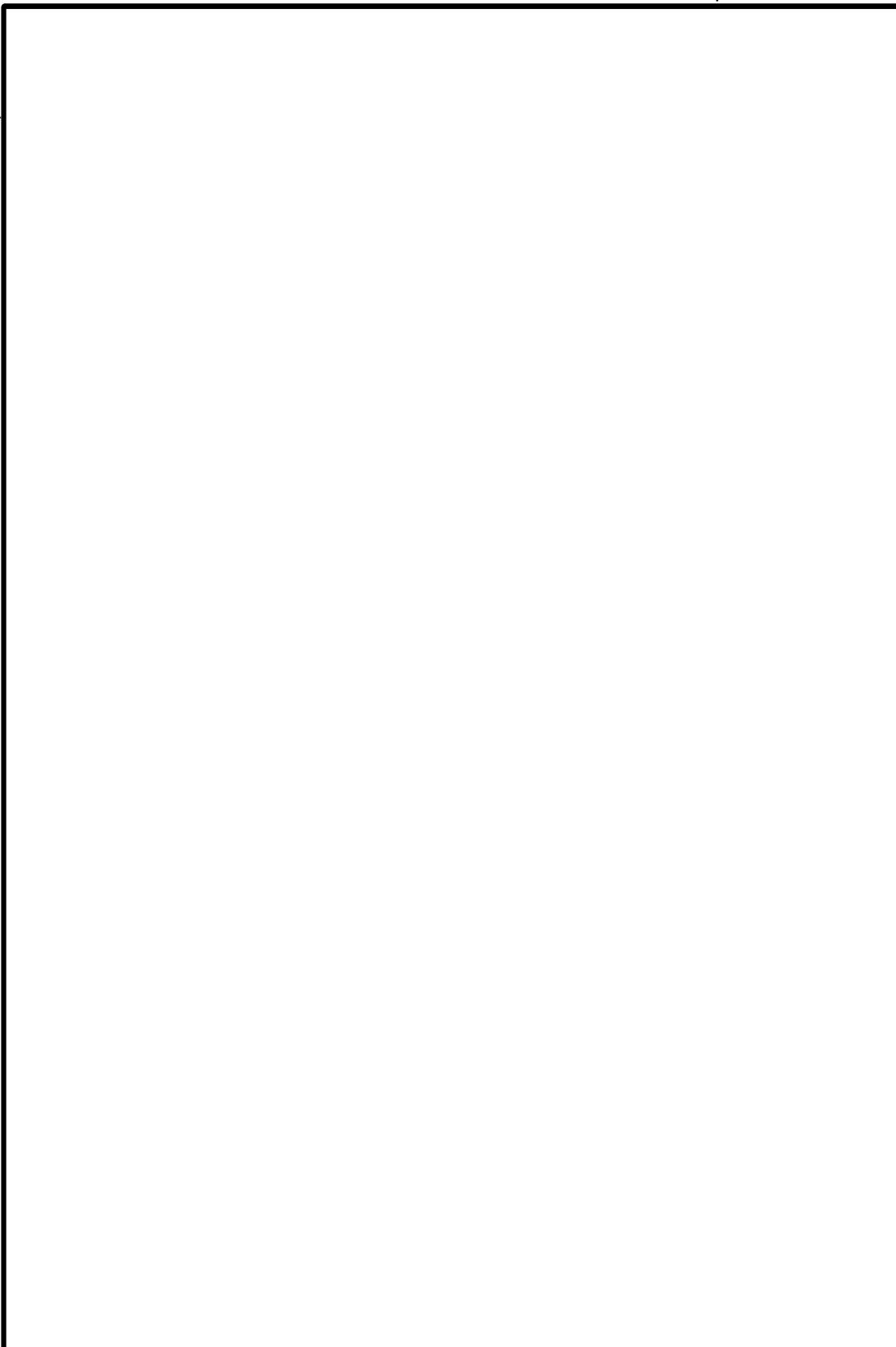
Appendix, Continued

APPENDIX D
DACS NCIC Offense Codes

(b)(5)

Appendix, Continued

(b)(7)(e)



(b)(5)

(b)(7)(e)

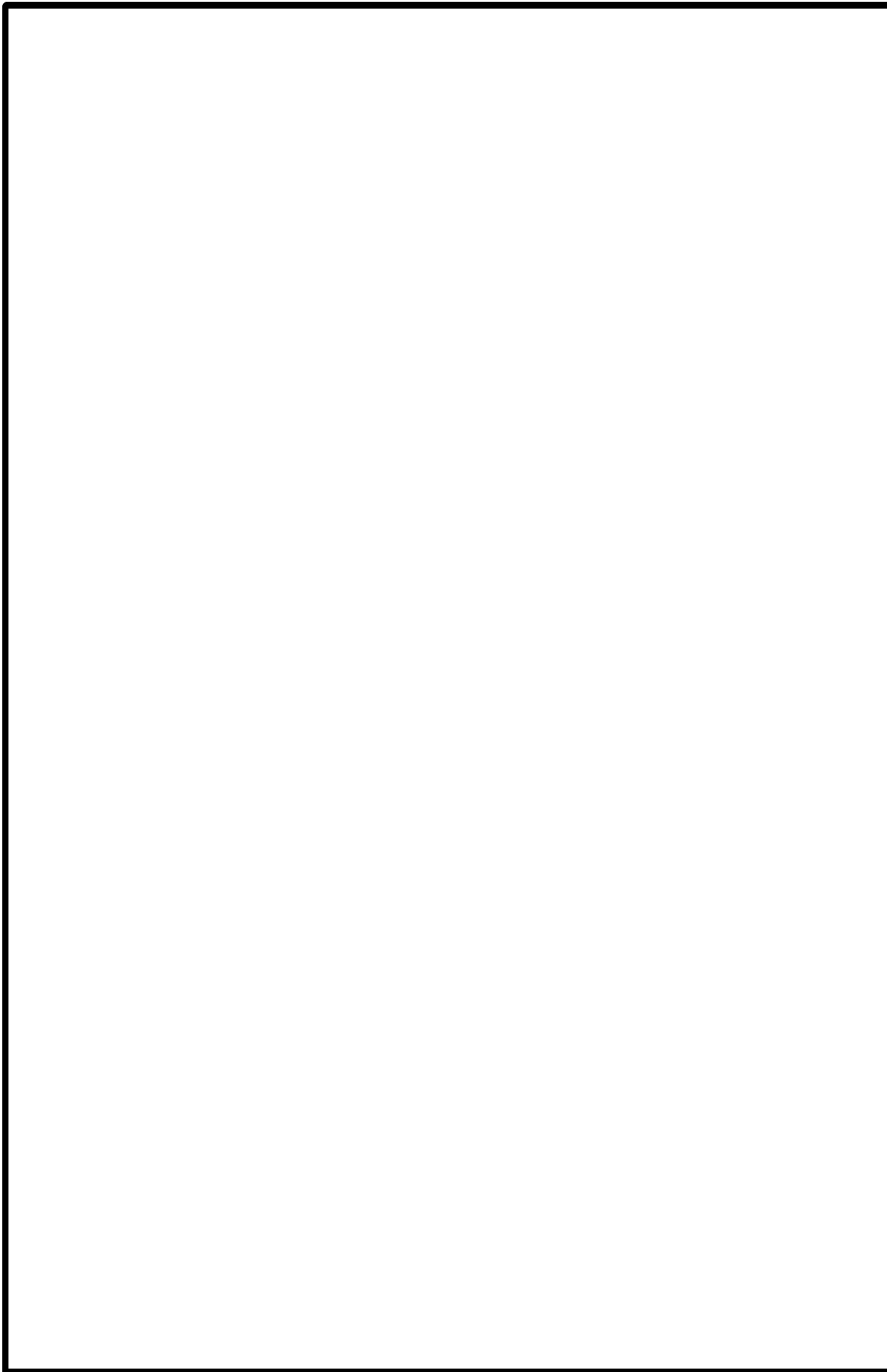
Appendix, Continued



(b)(7)(e)

(b)(5)

Appendix, Continued



(b)(5)

(b)(7)(e)

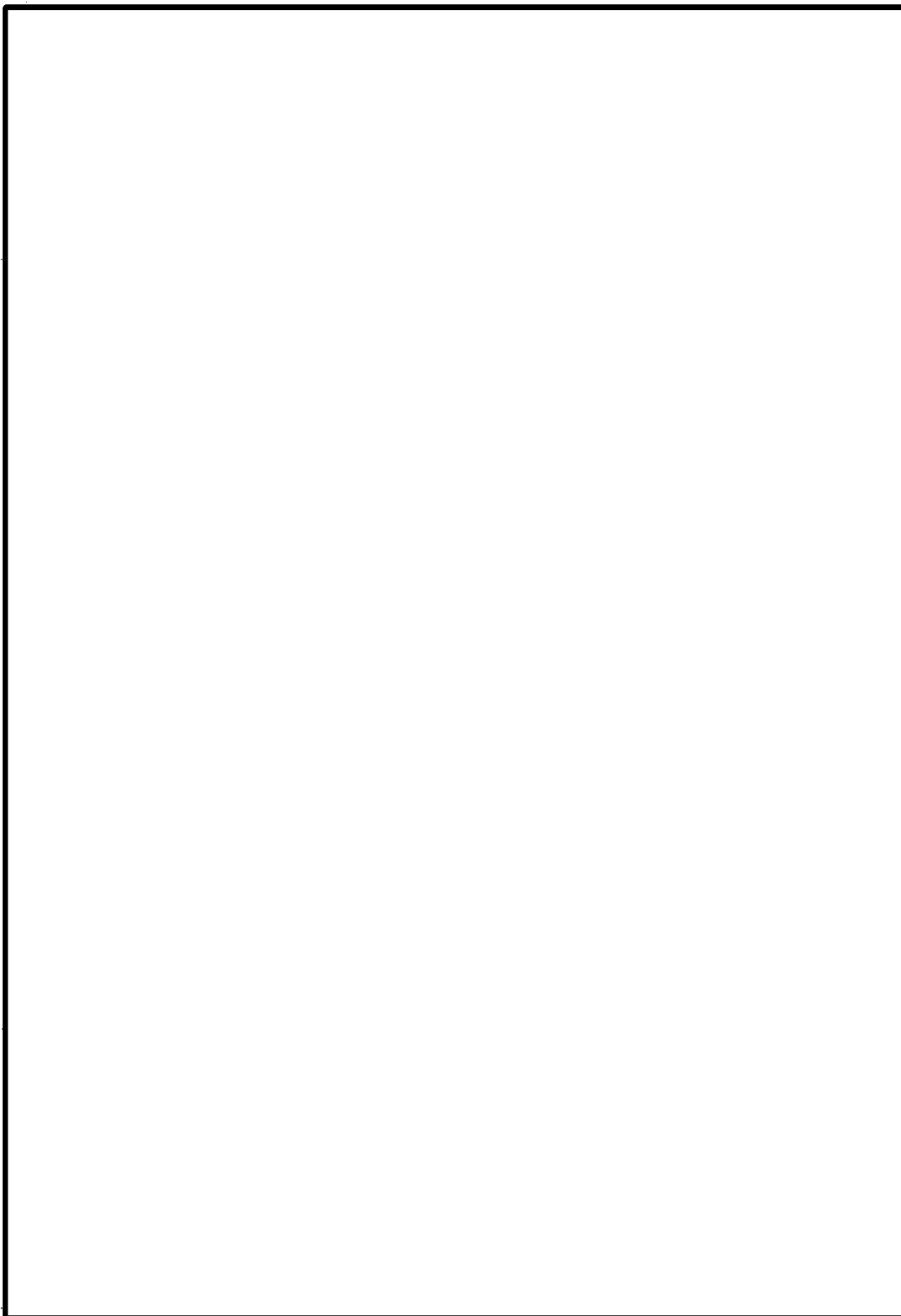
Appendix, Continued



(b)(7)(e)

(b)(5)

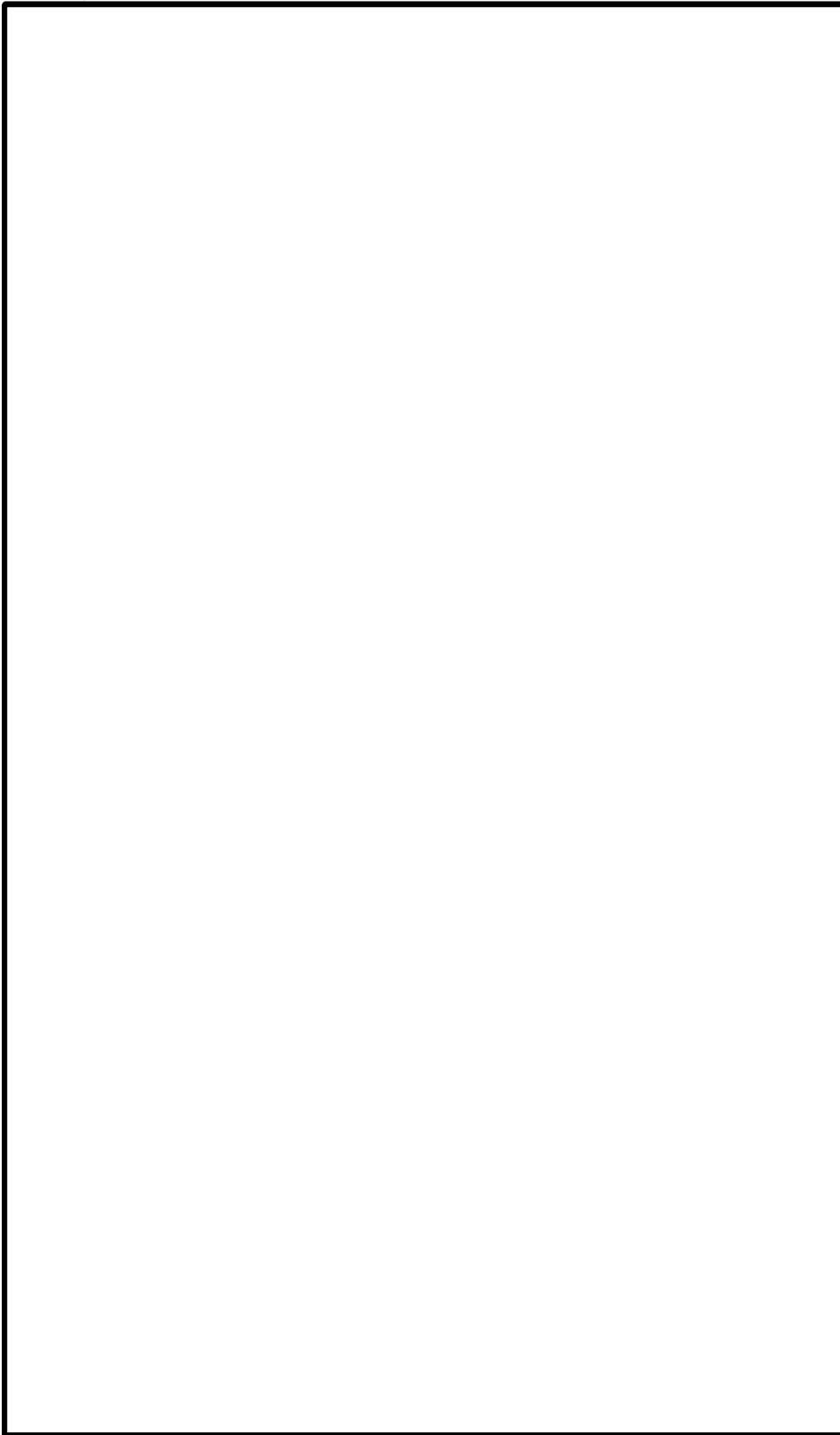
Appendix, Continued



(b)(5)

(b)(7)(e)

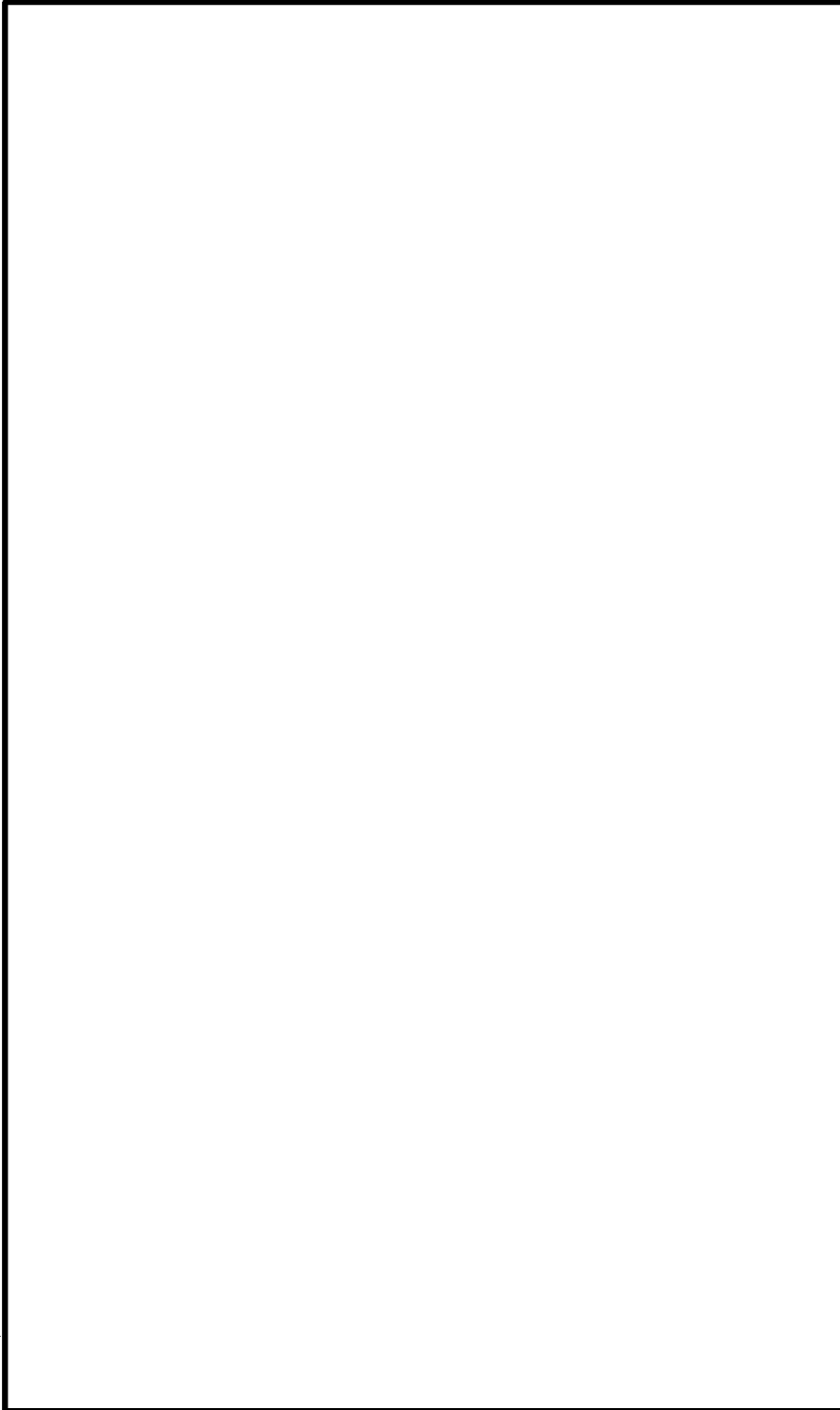
Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(5)

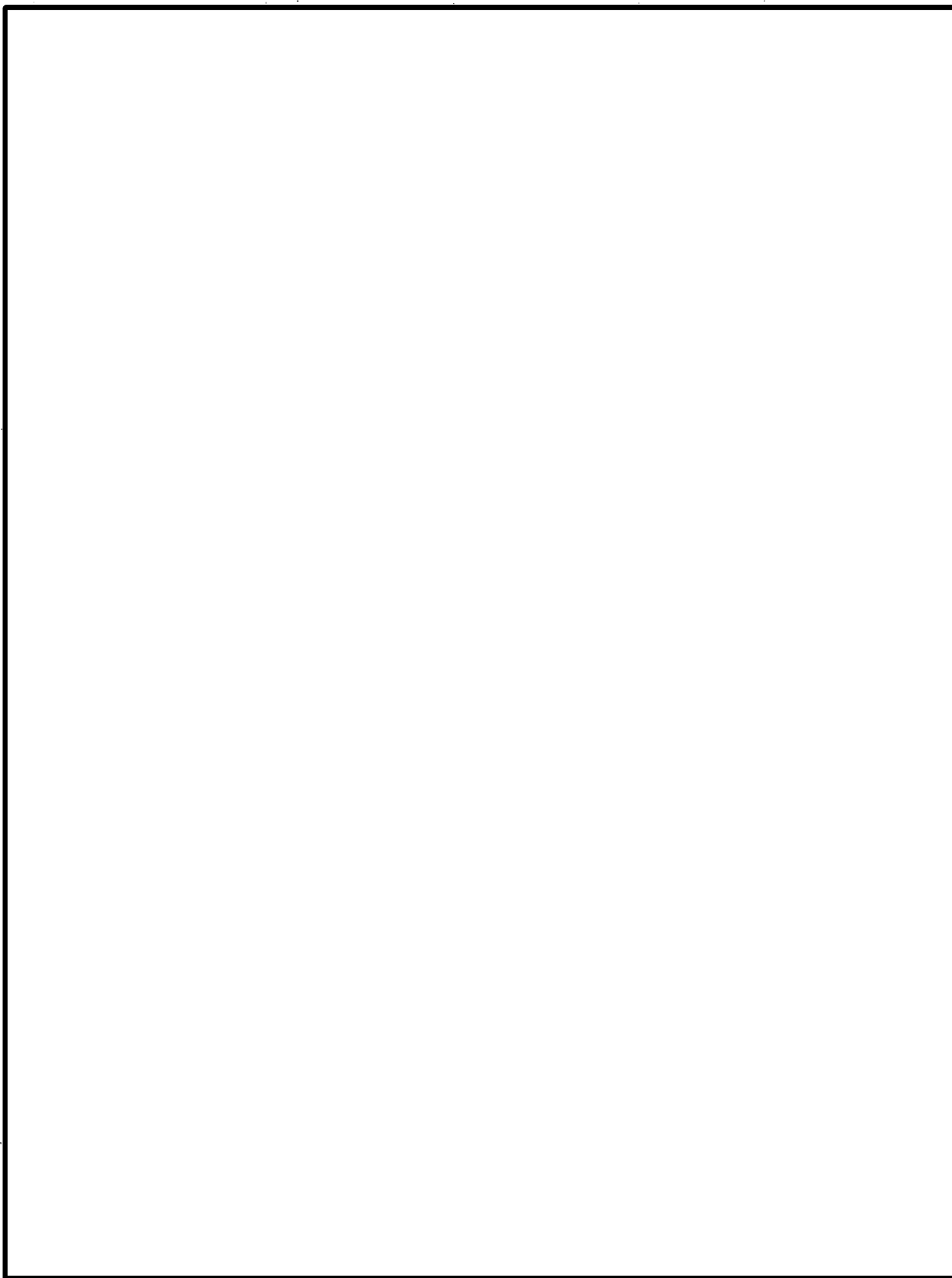
(b)(7)(e) **Appendix, Continued**



(b)(5)

(b)(7)(e)

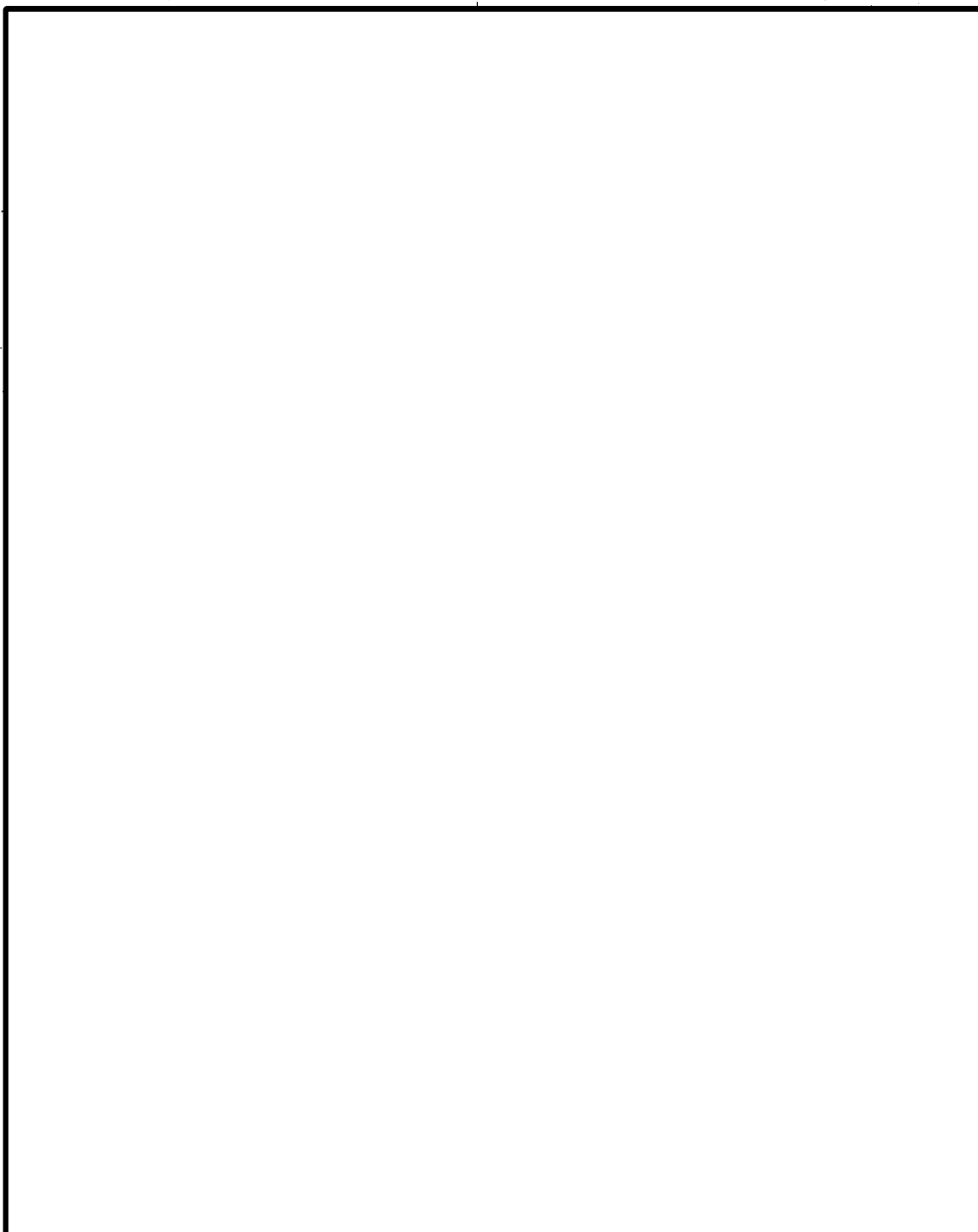
Appendix, Continued



(b)(7)(e)

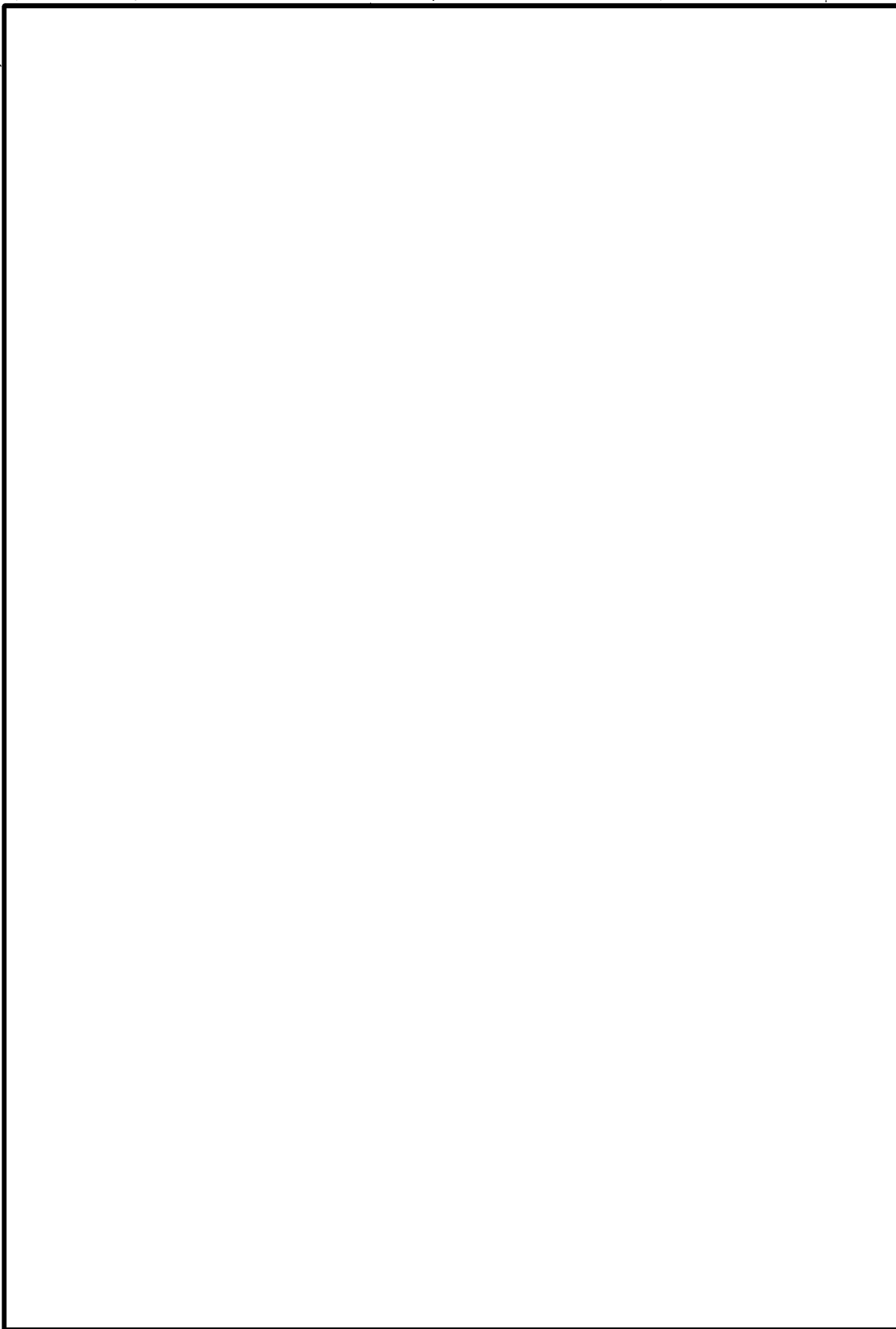
(b)(5)

Appendix, Continued



(b)(5)

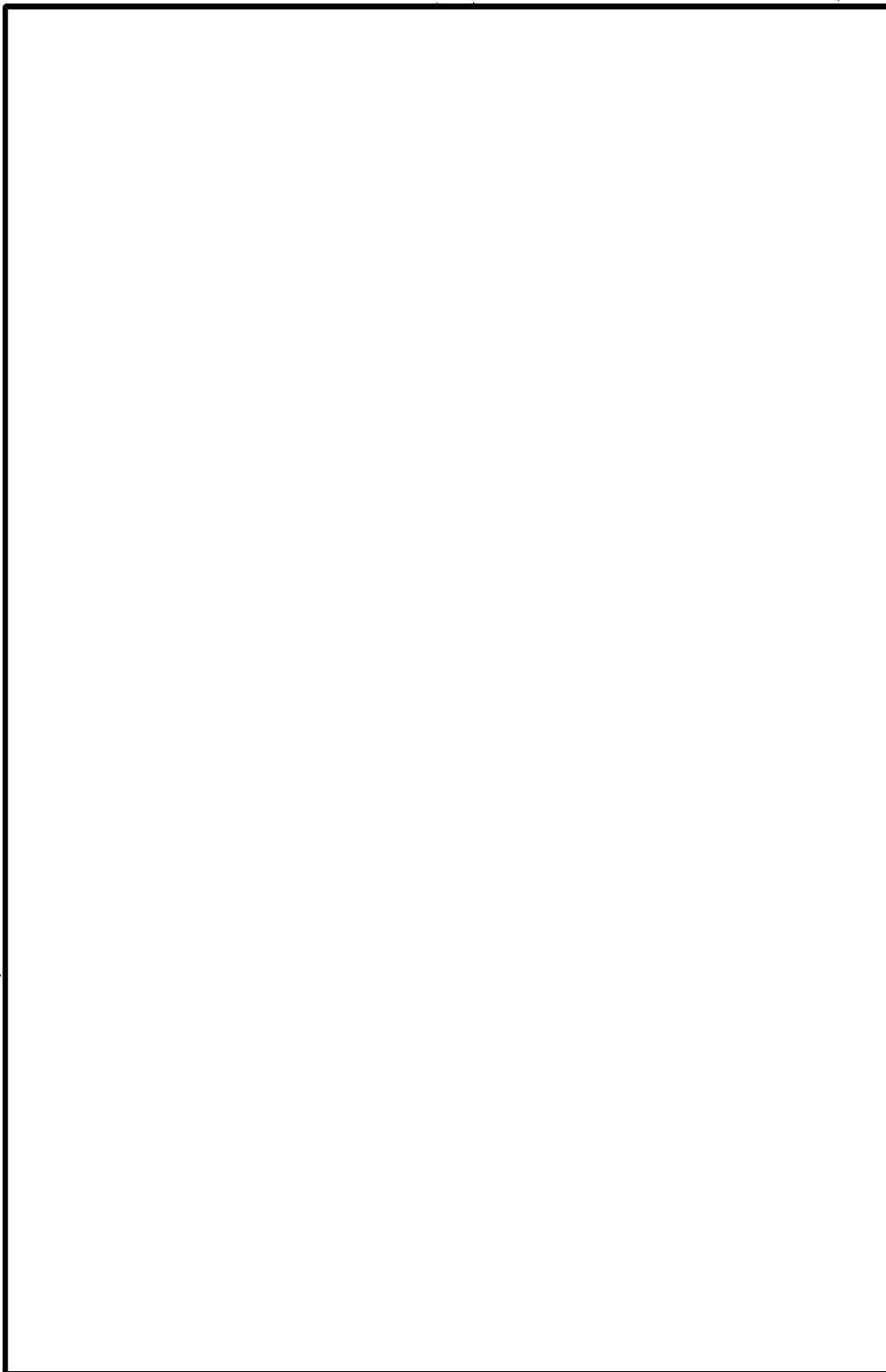
(b)(7)(e)



(b)(7)(e)

(b)(5)

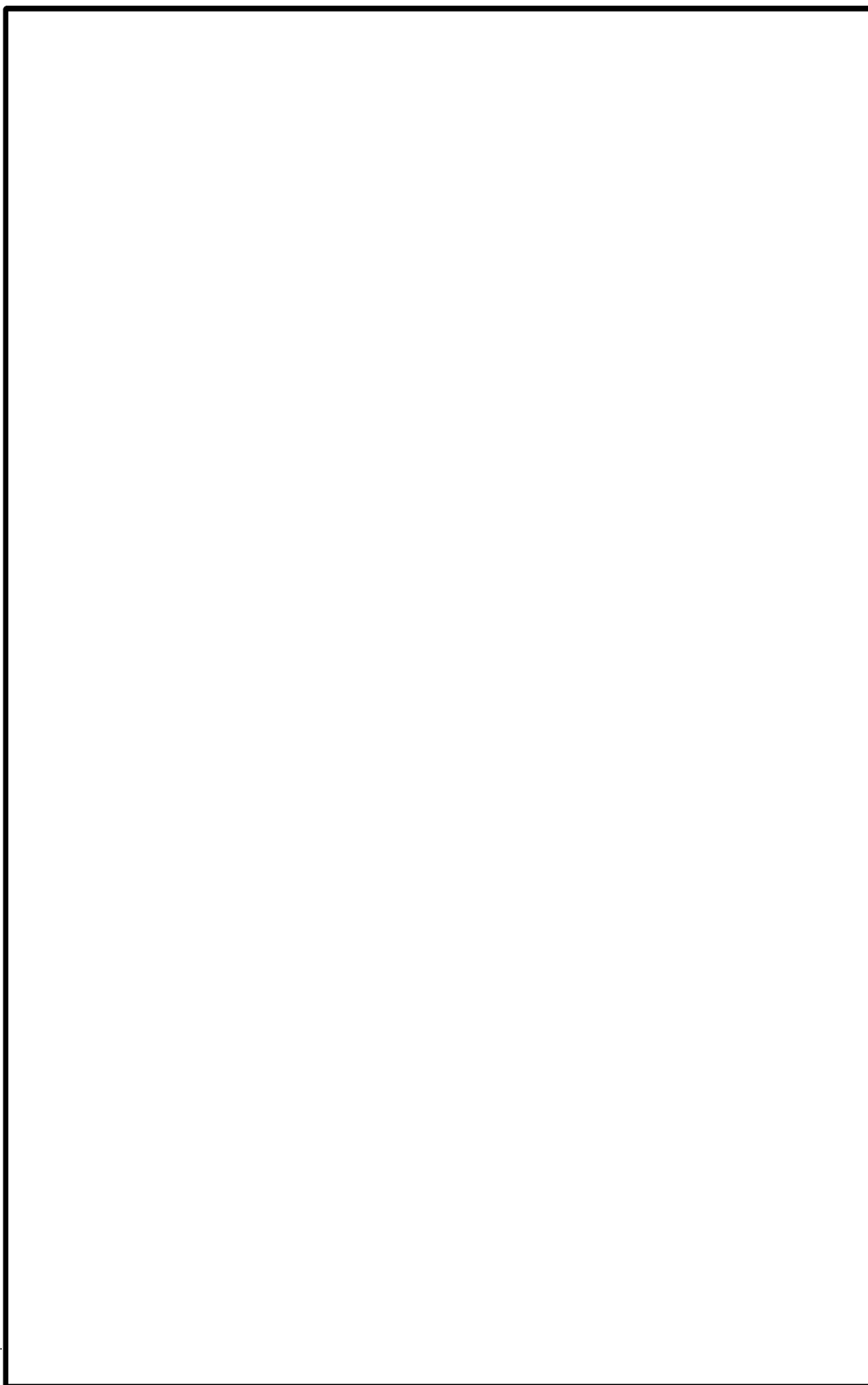
Appendix, Continued



(b)(5)

(b)(7)(e)

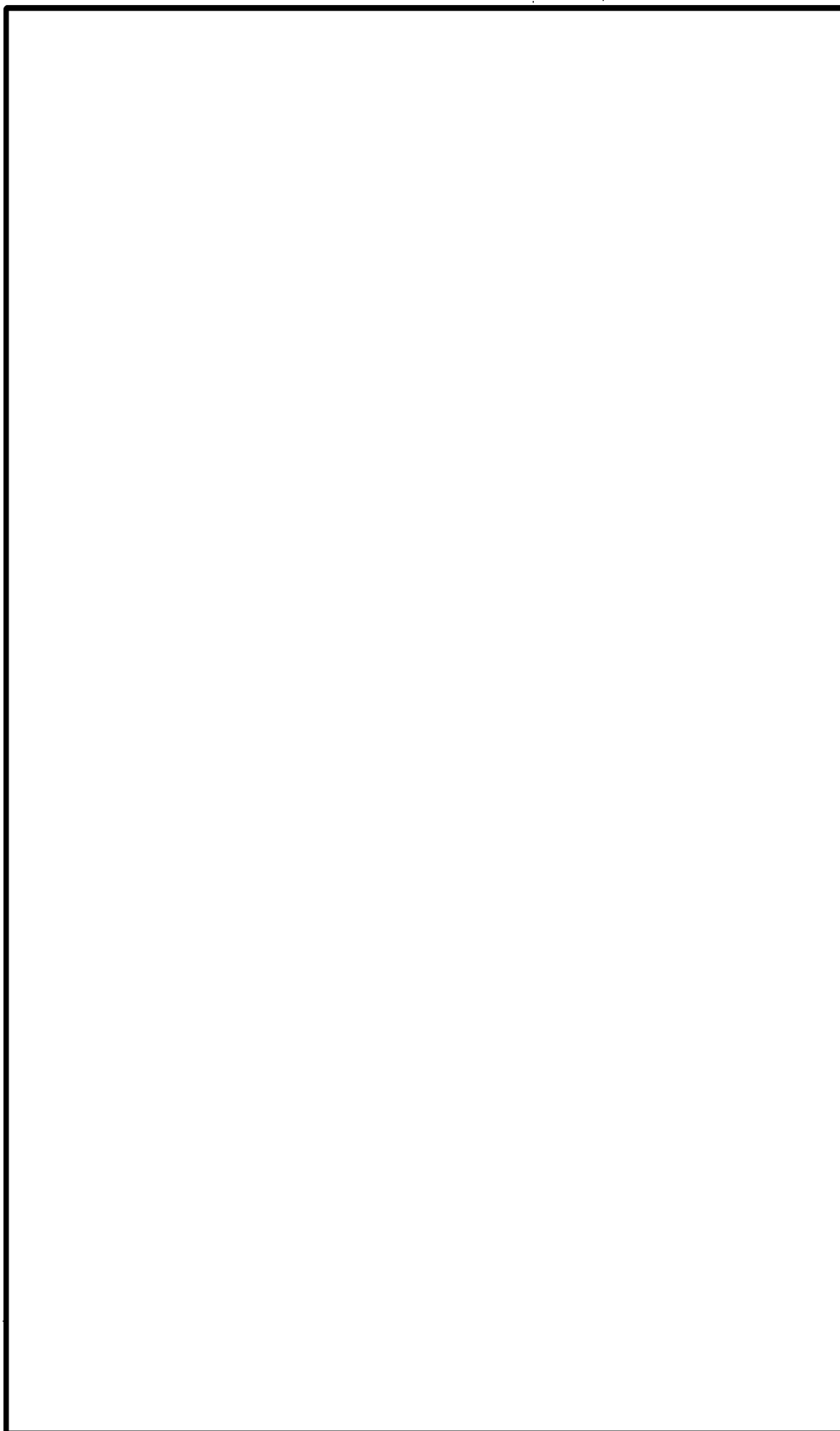
Appendix, Continued



(b)(7)(e)

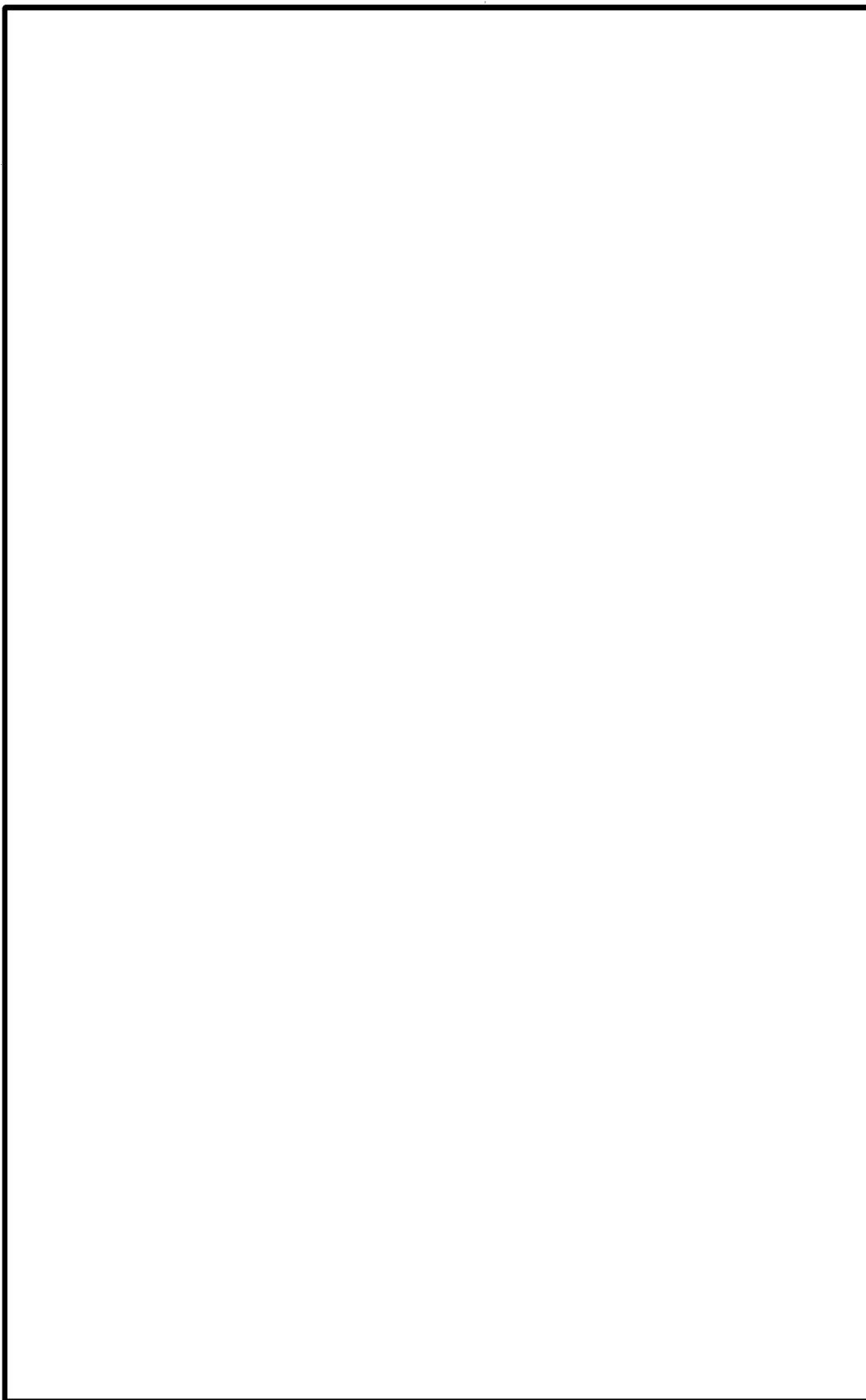
(b)(5)

Appendix, Continued



(b)(5)

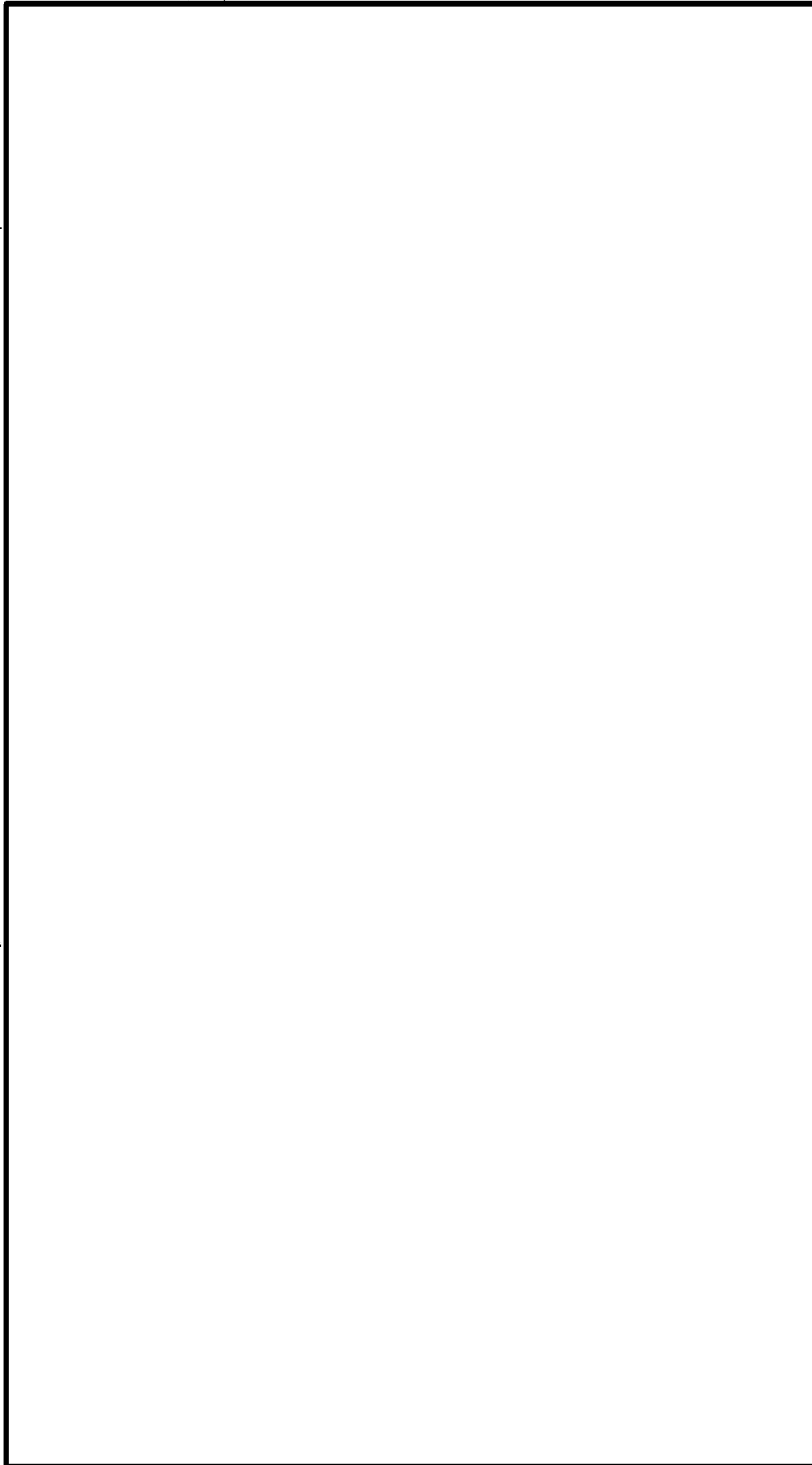
(b)(7)(e) **Appendix, Continued**



(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(7)(e)

(b)(5)

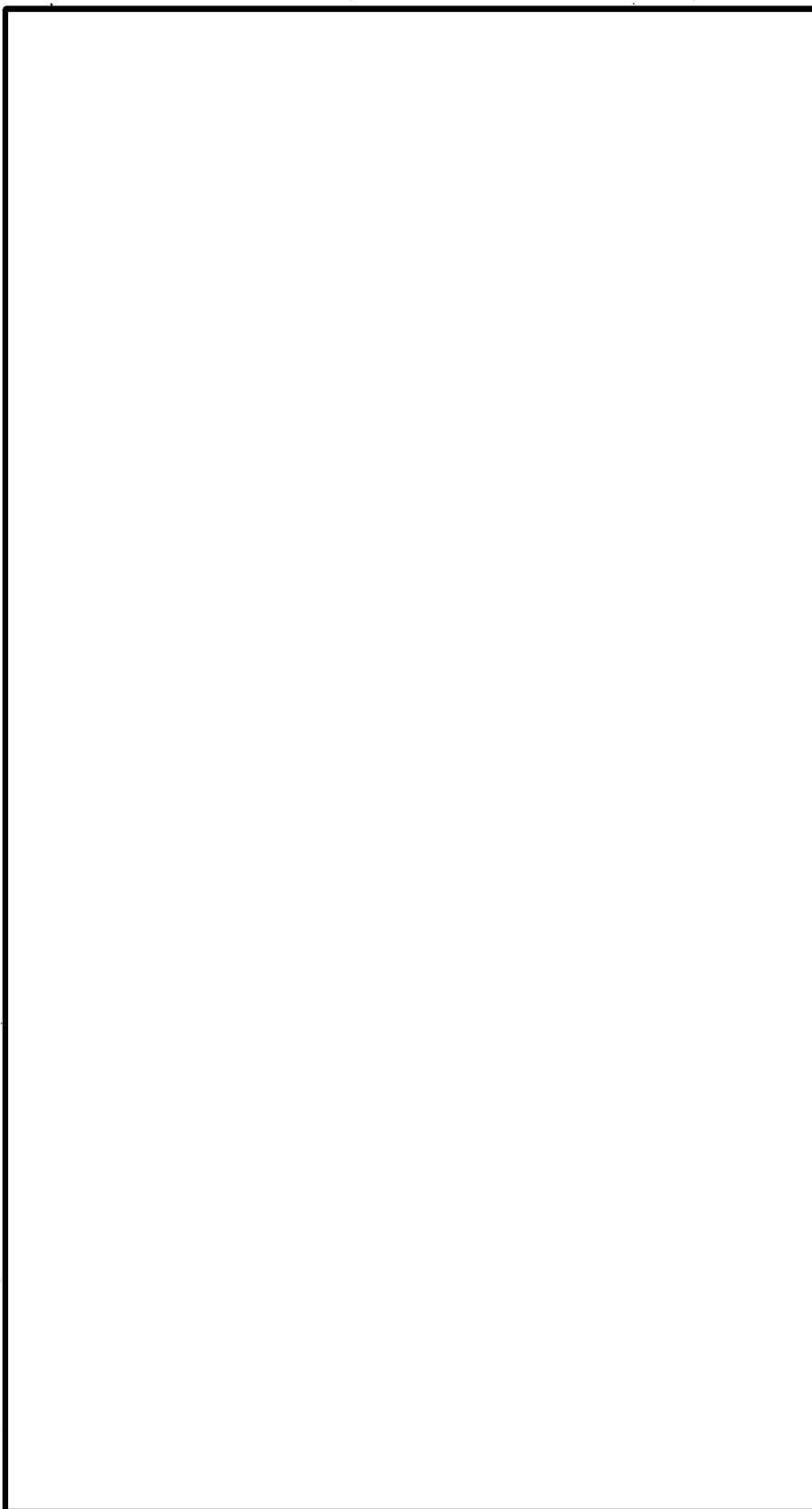
Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(7)(e)

(b)(5)

Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



Appendix, Continued

(b)(5)

(b)(7)(e)



Appendix, Continued

**APPENDIX E
DACS Charge Codes**

(b)(7)(e)

(b)(5)

Appendix, Continued

Inadmissibility Charge Codes—IIRAIRA

Effective April 1, 1997

Section of INA	Description
212(a)(1)(A)(i)	Communicable disease of public health significance
212(a)(1)(A)(ii)	Lacks immunization against vaccine-preventable disease
212(a)(1)(A)(iii)	Physical or mental disorder with associated harmful behavior
212(a)(1)(A)(iv)	Drug abuser or addict
212(a)(2)(A)(i)(I)	Conviction for one CIMT
212(a)(2)(A)(i)(II)	Controlled substance violation (includes U.S. or foreign laws)
212(a)(2)(B)	Conviction for two or more CIMTs, sentenced to 5 years or more
212(a)(2)(C)	Controlled substance traffickers
212(a)(2)(D)	Prostitution and commercialized vice
212(a)(2)(E)	Criminal who asserted immunity from prosecution
212(a)(3)(A)	Espionage, sabotage, or export of sensitive technology/information
212(a)(3)(B)(i)(I)	Alien who has engaged in a terrorist activity
212(a)(3)(B)(i)(II)	Alien who is engaged in or likely to engage in terrorist activity
212(a)(3)(B)(i)(III)	Alien who has incited terrorist activity
212(a)(3)(B)(i)(IV)	Representative of foreign terrorist organization
212(a)(3)(B)(i)(V)	Member of foreign terrorist organization
212(a)(3)(C)	Adverse foreign policy consequences for the United States
212(a)(3)(D)	Membership in communist or any other totalitarian party
212(a)(3)(E)	Assisted in Nazi persecution or engaged in genocide
212(a)(4)	Likely to become a public charge
212(a)(5)(A)	No approved labor certification
212(a)(5)(B)	Unqualified physicians
212(a)(5)(C)	Uncertified foreign health-care workers
212(a)(6)(A)	Alien present in the United States who was not admitted or paroled or arriving in the United States at a time or place not designated by the AG
212(a)(6)(B)	Alien who did not appear for or remain at removal proceedings and attempts to enter within five years of departure or removal
212(a)(6)(C)(i)	Willful misrepresentation of a material fact
212(a)(6)(C)(ii)	False claim to U.S. citizenship
212(a)(6)(D)	Stowaways
212(a)(6)(E)	Alien smugglers
212(a)(6)(F)	Subject of final order for violation of Section 274C INA
212(a)(6)(G)	Student visa abusers
212(a)(7)(A)(i)(I)	Immigrant not in possession of valid entry documents
212(a)(7)(A)(i)(II)	Immigrant visa issued without compliance with Section 203 INA
212(a)(7)(B)(i)(I)	Nonimmigrant without valid passport
212(a)(7)(B)(i)(II)	Nonimmigrant without valid visa
212(a)(8)(A)	Immigrant who is permanently ineligible to citizenship
212(a)(8)(B)	Draft evaders
212(a)(9)(A)(i)	Any alien previously removed as inadmissible who seeks reentry within 5 years (20 years if subsequent removal or ag felon)
212(a)(9)(A)(ii)	Any alien previously removed after being ordered removed or who departed while an order of removal was outstanding and seeks reentry within 10 years (20 years if subsequent removal or ag felon)

(b)(5)

(b)(7)(e)

Appendix, Continued

Section of INA	Description
212(a)(9)(B)(1)(I)	Any alien (other than LPR) who departed voluntarily after being unlawfully present in the United States for more than 180 days but less than one year and seeks to reenter within 3 years
212(a)(9)(B)(1)(II)	Any alien (other than LPR) who was unlawfully present in the United States for more than one year who seeks to reenter within 10 years
212(a)(9)(C)(1)(I)	Any alien who has been unlawfully present in the United States for an aggregate period of more than one year and who enters or attempts to enter the United States without being admitted
212(a)(9)(C)(1)(II)	Any alien who has been ordered removed under section 235(b)(1) or section 240 INA, or any other provision of law, who enters or attempts to enter the United States without being admitted
212(a)(10)(A)	Immigrant coming to practice polygamy
212(a)(10)(B)	Guardian required to accompany a helpless alien
212(a)(10)(C)	International child abductor
212(a)(10)(D)	Any alien who has unlawfully voted
212(a)(10)(E)	Former citizen who renounced citizenship to avoid taxation

(b)(7)(e)

(b)(5)

Appendix, Continued

Removable (Inadmissible at Time of Entry)—IIRAIRA

Effective April 1, 1997

Section of INA	Description
237(a)(1)(A)	Communicable disease of public health significance – (212)(a)(1)(A)(i)
237(a)(1)(A)	Lacks immunization against vaccine-preventable disease – (212)(a)(1)(A)(ii)
237(a)(1)(A)	Physical or mental disorder with associated harmful behavior – (212)(a)(1)(A)(iii)
237(a)(1)(A)	Drug abuser or drug addict – (212)(a)(1)(A)(iv)
237(a)(1)(A)	Conviction for one CIMT – (212)(a)(2)(A)(i)(I)
237(a)(1)(A)	Controlled substance violation (includes U.S. or foreign laws) – (212)(a)(2)(A)(i)(II)
237(a)(1)(A)	Conviction for two or more CIMTs, sentenced to five years or more – (212)(a)(2)(B)
237(a)(1)(A)	Controlled substance traffickers – (212)(a)(2)(C)
237(a)(1)(A)	Prostitution and commercialized vice – (212)(a)(2)(D)
237(a)(1)(A)	Criminal who asserted immunity from prosecution – (212)(a)(2)(E)
237(a)(1)(A)	Espionage, sabotage, or export of sensitive technology/information – (212)(a)(3)(A)
237(a)(1)(A)	Alien who has engaged in a terrorist activity – (212)(a)(3)(B)(i)(I)
237(a)(1)(A)	Alien who is engaged in or likely to engage in terrorist activities – (212)(a)(3)(B)(i)(II)
237(a)(1)(A)	Alien who has incited terrorist activity – (212)(a)(3)(B)(i)(III)
237(a)(1)(A)	Representative of foreign terrorist organization – (212)(a)(3)(B)(i)(IV)
237(a)(1)(A)	Member of foreign terrorist organization – (212)(a)(3)(B)(i)(V)
237(a)(1)(A)	Adverse foreign policy consequences for the United States – (212)(a)(3)(C)
237(a)(1)(A)	Membership in communist or any other totalitarian party – (212)(a)(3)(D)
237(a)(1)(A)	Assisted in Nazi persecution or engaged in genocide – (212)(a)(3)(E)
237(a)(1)(A)	Likely to become a public charge – (212)(a)(4)
237(a)(1)(A)	No approved labor certification – (212)(a)(5)(A)
237(a)(1)(A)	Unqualified physicians – (212)(a)(5)(B)
237(a)(1)(A)	Uncertified foreign health-care workers – (212)(a)(5)(C)
237(a)(1)(A)	Alien present in the United States who was not admitted or paroled or arriving in the United States at a time or place not designated by the AG – (212)(a)(6)(A)
237(a)(1)(A)	Aliens who did not appear for or remain at removal proceedings and attempts to enter within five years of departure or removal – (212)(a)(6)(B)
237(a)(1)(A)	Willful misrepresentation of a material fact – (212)(a)(6)(C)(i)
237(a)(1)(A)	False claim to U.S. citizenship – (212)(a)(6)(C)(ii)
237(a)(1)(A)	Stowaways – (212)(a)(6)(D)
237(a)(1)(A)	Alien smugglers – (212)(a)(6)(E)
237(a)(1)(A)	Subject of final order for violation of Section 274C INA – (212)(a)(6)(F)
237(a)(1)(A)	Student visa abusers – (212)(a)(6)(G)
237(a)(1)(A)	Immigrant not in possession of valid entry documents – (212)(a)(7)(A)(i)(I)
237(a)(1)(A)	Immigrant visa issued without compliance with section 203 INA – (212)(a)(7)(A)(i)(II)
237(a)(1)(A)	Nonimmigrant not in possession of valid passport – (212)(a)(7)(B)(i)(I)
237(a)(1)(A)	Nonimmigrant not in possession of valid visa – (212)(a)(7)(B)(i)(II)
237(a)(1)(A)	Immigrant who is permanently ineligible to citizenship – (212)(a)(8)(A)
237(a)(1)(A)	Draft evaders – (212)(a)(8)(B)

(b)(5)

(b)(7)(e)

Appendix, Continued

Section of INA	Description
237(a)(1)(A)	Any alien previously removed as inadmissible who seeks reentry within 5 years (20 years if subsequent removal or ag felon) – (212)(a)(9)(A)(i)
237(a)(1)(A)	Any alien previously removed after being ordered removed or who departed while an order of removal was outstanding and seeks reentry within 10 years (20 years if subsequent removal or ag felon) – (212)(a)(9)(A)(ii)
237(a)(1)(A)	Any alien (other than LPR) who departed voluntarily after being unlawfully present in the United States for more than 180 days but less than one year and seeks to reenter within 3 years – (212)(a)(9)(B)(i)(I)
237(a)(1)(A)	Any alien (other than LPR) who was unlawfully present in the United States for more than one year who seeks to reenter within 10 years – (212)(a)(9)(B)(i)(II)
237(a)(1)(A)	Any alien who has been unlawfully present in the United States for an aggregate period of more than one year and who enters or attempts to enter the United States without being admitted – (212)(a)(9)(C)(i)(I)
237(a)(1)(A)	Any alien who has been ordered removed under Section 235(b)(1) or section 240 INA, or any other provision of law, who enters or attempts to enter the United States without being admitted – (212)(a)(9)(C)(i)(II)
237(a)(1)(A)	Immigrant coming to practice polygamy – (212)(a)(10)(A)
237(a)(1)(A)	Guardian required to accompany a helpless alien – (212)(a)(10)(B)
237(a)(1)(A)	International child abductor – (212)(a)(10)(C)
237(a)(1)(A)	Any alien who has unlawfully voted – (212)(a)(10)(D)
237(a)(1)(A)	Former citizen who renounced citizenship to avoid taxation – (212)(a)(10)(E)

(b)(7)(e)

(b)(5) **Appendix, Continued**

Removal Charge Codes—IIRAIRA

Effective April 1, 1997

Section of INA	Description
237(a)(1)(B)	Any alien present in the United States in violation of law
237(a)(1)(C)(i)	Nonimmigrant status violator
237(a)(1)(C)(ii)	Violators of conditions of entry imposed under Section 212(g) INA
237(a)(1)(D)(i)	Termination of conditional permanent resident status
237(a)(1)(E)	Alien smuggling
237(a)(1)(G)(i)	Marriage fraud – terminated within 2 years after admission
237(a)(1)(G)(ii)	Alien fails or refuses to fulfill marital agreement
237(a)(2)(A)(i)	Convicted of one CIMT and one year sentence may be imposed
237(a)(2)(A)(ii)	Convicted of two or more CIMTs
237(a)(2)(A)(iii)	Convicted of an aggravated felony
237(a)(2)(A)(iv)	Convicted of high speed flight to avoid immigration checkpoint
237(a)(2)(B)(i)	Convicted of controlled substance violation
237(a)(2)(B)(ii)	Drug abusers and addicts
237(a)(2)(C)	Convicted of firearms offense
237(a)(2)(D)(i)	Convicted of espionage, treason, or sedition
237(a)(2)(D)(ii)	Convicted of 18 USC 871 or 960
237(a)(2)(D)(iii)	Convicted of violation of Military Selective Service Act or Trading with the Enemy Act
237(a)(2)(D)(iv)	Convicted of violation of Section 215 or 278 INA
237(a)(2)(E)(i)	Convicted of domestic violence, stalking, child abuse, child neglect or child abandonment
237(a)(2)(E)(ii)	Violation of protection order
237(a)(3)(A)	Change of address violation
237(a)(3)(B)(i)	Convicted under Section 266(c) INA or section 36(c) of the Alien Registration Act of 1940
237(a)(3)(B)(ii)	Convicted under Foreign Agents Registration Act of 1938 (22 USC 611)
237(a)(3)(B)(iii)	Convicted of fraud, misuse of visas, permits and other entry documents (18 USC 1546)
237(a)(3)(C)(i)	Alien subject of final order for violation of Section 274C INA – document fraud
237(a)(3)(D)	False claim to U.S. citizenship
237(a)(4)(A)(i)	Engaged in espionage, sabotage, or violation of law prohibiting export of goods, technology or sensitive information
237(a)(4)(A)(ii)	Engaged in criminal activity which endangers public safety or national security
237(a)(4)(A)(iii)	Activity in opposition to or control or overthrow of the U.S. Government by force, violence or other unlawful means
237(a)(4)(B)	Engaged in terrorist activity
237(a)(4)(C)	Adverse foreign policy consequences for the United States
237(a)(4)(D)	Assisted in Nazi persecution or engaged in genocide
237(a)(5)	Has become a public charge within five years of entry
237(a)(6)	Any alien who has unlawfully voted

(b)(5)

(b)(7)(e)

Appendix, Continued

Deportation Charge Codes—IMMACT '90

(Order to Show Cause Issued Between March 1, 1991, and March 31, 1997)
Deportable as Excludable at Time of Entry

Section of INA	Description
241(a)(1)(A)	Communicable disease – 212(a)(1)(A)(i)
241(a)(1)(A)	Physical or mental disorder – 212(a)(1)(A)(ii)
241(a)(1)(A)	Drug abuser or addict – 212(a)(1)(A)(iii)
241(a)(1)(A)	Conviction for one CIMT – 212(a)(2)(A)(i)(I)
241(a)(1)(A)	Controlled substance violators – 212(a)(2)(A)(i)(2)
241(a)(1)(A)	Multiple criminal convictions – 212(a)(2)(B)
241(a)(1)(A)	Controlled substance traffickers – 212(a)(2)(C)
241(a)(1)(A)	Prostitution (within 10 years) – 212(a)(2)(D)(i)
241(a)(1)(A)	Pimps (within 10 years) – 212(a)(2)(D)(ii)
241(a)(1)(A)	Unlawful commercialized vice – 212(a)(2)(D)(iii)
241(a)(1)(A)	Abuse of diplomatic privilege – 212(a)(2)(E)
241(a)(1)(A)	Espionage or sabotage – 212(a)(3)(A)(i)
241(a)(1)(A)	Any other unlawful activity – 212(a)(3)(A)(ii)
241(a)(1)(A)	Activity to overthrow U.S. Govt. – 212(a)(3)(A)(iii)
241(a)(1)(A)	Engaged in terrorist activity – 212(a)(3)(B)(i)
241(a)(1)(A)	Likely to participate in terrorist activity – 212(a)(3)(B)(ii)
241(a)(1)(A)	Foreign policy – 212(a)(3)(C)
241(a)(1)(A)	Membership in a totalitarian party – 212(a)(3)(D)
241(a)(1)(A)	Assisted in Nazi persecution – 212(a)(3)(E)(i)
241(a)(1)(A)	Engaged in genocide – 212(a)(3)(E)(ii)
241(a)(1)(A)	Likely to become a public charge – 212(a)(4)
241(a)(1)(A)	No labor certification – 212(a)(5)(A)(i)
241(a)(1)(A)	Unqualified physician – 212(a)(5)(B)
241(a)(1)(A)	Previously excluded – 212(a)(6)(A)
241(a)(1)(A)	Previously deported – 212(a)(6)(B)
241(a)(1)(A)	Fraud or misrepresentation – 212(a)(6)(C)
241(a)(1)(A)	Stowaway – 212(a)(6)(D)
241(a)(1)(A)	Alien smuggler – 212(a)(6)(E)
241(a)(1)(A)	Subject of civil penalty – 212(a)(6)(F)
241(a)(1)(A)	Immigrant without visa – 212(a)(7)(A)(i)
241(a)(1)(A)	Immigrant visa outside numerical limits – 212(a)(7)(A)(ii)
241(a)(1)(A)	No valid passport – 212(a)(7)(B)(i)
241(a)(1)(A)	No valid nonimmigrant visa – 212(a)(7)(B)(ii)
241(a)(1)(A)	Ineligible to citizenship – 212(a)(8)(A)
241(a)(1)(A)	Draft evader – 212(a)(8)(B)
241(a)(1)(A)	Practicing polygamist – 212(a)(9)(A)
241(a)(1)(A)	Accompanying excluded alien – 212(a)(9)(B)
241(a)(1)(A)	International child abduction – 212(a)(9)(C)

(b)(7)(e)

(b)(5) **Appendix, Continued**

Deportation Charge Codes—IMMACT '90

(Order to Show Cause Issued Between March 1, 1991, and March 31, 1997)
Deportable—Other Deportation Charges

Section of INA	Description
241(a)(1)(B)	Entered without inspection
241(a)(1)(C)(i)	Nonimmigrant status violator
241(a)(1)(C)(ii)	Violated conditions of entry
241(a)(1)(D)	Termination of conditional residence
241(a)(1)(E)	Alien smuggling
241(a)(1)(F)	Failure to maintain employment
241(a)(1)(G)(i)	Marriage fraud – terminated early
241(a)(1)(G)(ii)	Marriage fraud – failure to fulfill marital agreement
241(a)(2)(A)(i)	Convicted of one CIMT
241(a)(2)(A)(ii)	Convicted of more than one CIMT
241(a)(2)(A)(iii)	Convicted of an aggravated felony
241(a)(2)(B)(i)	Controlled substance conviction
241(a)(2)(B)(ii)	Drug abusers and addicts
241(a)(2)(C)	Firearms offenses
241(a)(2)(D)(i)	Conviction for espionage or treason
241(a)(2)(D)(ii)	Convicted under 18 USC 871 or 960
241(a)(2)(D)(iii)	Convicted of Selective Service violation
241(a)(2)(D)(iv)	Conviction under Section 215 or 278 INA
241(a)(3)(A)	Change of address violation
241(a)(3)(B)(i)	Failure to register
241(a)(3)(B)(ii)	Violation of Foreign Agent Act
241(a)(3)(B)(iii)	Falsification of documents
241(a)(3)(C)	Conviction under Section 274C INA for document fraud
241(a)(4)(A)(i)	Sabotage or exporting goods
241(a)(4)(A)(ii)	Endangering public safety
241(a)(4)(A)(iii)	Opposition or overthrow the government
241(a)(4)(B)	Terrorist activities
241(a)(4)(C)	Adverse foreign policy consequences for the United States
241(a)(4)(D)	Assisted in Nazi persecution or engaged in genocide
241(a)(5)	Likely to become a public charge

Appendix, Continued

(b)(5)

EXCLUSION CHARGE CODES—IMMACT '90

(b)(7)(e)

(I-110/122 Issued Between June 1, 1991, and March 31, 1997)

Section of INA	Description
212(a)(1)(A)(1)	Communicable disease
212(a)(1)(A)(2)	Physical or mental disorder
212(a)(1)(A)(3)	Drug abuser or addict
212(a)(2)(A)(1)(i)	Conviction for one CIMT
212(a)(2)(A)(1)(ii)	Controlled substance violators
212(a)(2)(B)	Convictions for more than one CIMT
212(a)(2)(C)	Controlled substance traffickers
212(a)(2)(D)(i)	Prostitution (within 10 years)
212(a)(2)(D)(ii)	Pimps (within 10 years)
212(a)(2)(D)(iii)	Unlawful commercialized vice
212(a)(2)(E)	Abuse of diplomatic privilege
212(a)(3)(A)(i)	Espionage or sabotage
212(a)(3)(A)(ii)	Any other unlawful activity
212(a)(3)(A)(iii)	Activity to overthrow the U.S. Government
212(a)(3)(B)(i)	Engaged in terrorist activity
212(a)(3)(B)(ii)	Likely to participate in terrorist activity
212(a)(3)(C)	Adverse foreign policy consequences for the United States
212(a)(3)(D)	Membership in a totalitarian party
212(a)(3)(E)(i)	Assisted in Nazi persecution
212(a)(3)(E)(ii)	Engaged in genocide
212(a)(4)	Likely to become a public charge
212(a)(5)(A)(i)	No labor certification
212(a)(5)(B)	Unqualified physician
212(a)(6)(A)	Previously excluded
212(a)(6)(B)	Previously deported
212(a)(6)(C)	Fraud or misrepresentation
212(a)(6)(D)	Stowaway
212(a)(6)(E)	Alien smuggler
212(a)(6)(F)	Subject of civil penalty
212(a)(7)(A)(i)	Immigrant without visa
212(a)(7)(A)(ii)	Immigrant visa outside numerical limits
212(a)(7)(B)(i)	Nonimmigrant without valid passport
212(a)(7)(B)(ii)	Nonimmigrant without valid visa
212(a)(8)(A)	Immigrant who is permanently ineligible to citizenship
212(a)(8)(B)	Draft evader
212(a)(9)(A)	Practicing polygamist
212(a)(9)(B)	Accompanying excluded alien
212(a)(9)(C)	International child abductor

(b)(7)(e)

(b)(5)

Appendix, Continued

Deportation Charge Codes

Effective Prior to March 1, 1991

Section of INA	Description
241(a)(1)	Feebleminded ⁴
241(a)(1)	Insane ⁴
241(a)(1)	One or more prior attacks of insanity ⁴
241(a)(1)	Afflicted with epilepsy ⁴
241(a)(1)	Afflicted with psychopathic personality ⁴
241(a)(1)	Afflicted with a mental defect ⁴
241(a)(1)	Narcotic drug addict ⁴
241(a)(1)	Chronic alcoholic ⁴
241(a)(1)	Afflicted with tuberculosis ⁴
241(a)(1)	Afflicted with leprosy ⁴
241(a)(1)	Afflicted with a dangerous contagious disease ⁴
241(a)(1)	Afflicted with a physical defect or disease affecting the ability to earn a living ⁴
241(a)(1)	Pauper ⁴
241(a)(1)	Professional beggar ⁴
241(a)(1)	Vagrant ⁴
241(a)(1)	Convicted of CIMT ⁴
241(a)(1)	Admits commission of CIMT ⁴
241(a)(1)	Admits commission of elements of CIMT ⁴
241(a)(1)	Convicted of two or more CIMT, five or more years imposed ⁴
241(a)(1)	One who is a polygamist ⁴
241(a)(1)	A practicing polygamist ⁴
241(a)(1)	Advocate of the practice of polygamy ⁴
241(a)(1)	Prostitutes ⁴
241(a)(1)	Have engaged in prostitution ⁴
241(a)(1)	Coming to engage in prostitution ⁴
241(a)(1)	Procure or attempt to procure a prostitute ⁴
241(a)(1)	Have procured or imported for prostitution ⁴
241(a)(1)	Supported by the proceeds of prostitution ⁴
241(a)(1)	Have been supported by the proceeds of prostitution ⁴
241(a)(1)	Coming to the United States to engage in commercialized vice ⁴
241(a)(1)	Coming to the United States to engage in an immoral sexual act ⁴
241(a)(1)	Seeking to enter to perform skilled or unskilled labor ⁴
241(a)(1)	Who is likely to become a public charge ⁴
241(a)(1)	Previously excluded ⁴
241(a)(1)	Previously deported ⁴
241(a)(1)	Previously removed as a distressed alien ⁴
241(a)(1)	Previously removed as an alien enemy ⁴
241(a)(1)	Previously removed in lieu of deportation ⁴
241(a)(1)	Stowaway ⁴
241(a)(1)	Seek to procure visa or other document by fraud ⁴
241(a)(1)	Have sought to procure visa or other document by fraud ⁴
241(a)(1)	Have procured visa or document by fraud ⁴
241(a)(1)	Seek to enter the United States by fraud or misrepresentation ⁴
241(a)(1)	Immigrant not in possession of valid entry documents ⁴
241(a)(1)	Immigrant not in possession of valid passport ⁴
241(a)(1)	Immigrant with faulty visa ⁴

(b)(5)

(b)(7)(e)

Appendix, Continued

Section of INA	Description
241(a)(1)	Ineligible to citizenship ⁴
241(a)(1)	Draft evaders ⁴
241(a)(1)	Conviction for trafficking in narcotic drugs ⁴
241(a)(1)	Conviction for any narcotic drugs law or regulation ⁴
241(a)(1)	Known drug traffickers ⁴
241(a)(1)	Arrival via nonsignatory line ⁴
241(a)(1)	Illiterate ⁴
241(a)(1)	Nonimmigrant not in possession of valid passport ⁴
241(a)(1)	Nonimmigrant not in possession of valid visa ⁴
241(a)(1)	Accompanying helpless excluded alien ⁴
241(a)(1)	Alien smuggling ⁴
241(a)(1)	Mentally retarded ¹
241(a)(1)	Afflicted with a sexual deviation ¹
241(a)(1)	No labor certification ¹
241(a)(1)	Visa not properly charged to foreign state ¹
241(a)(1)	Not an immediate relative as defined ¹
241(a)(1)	Not a special immigrant as defined ¹
241(a)(1)	Idiot ¹³
241(a)(1)	Imbecile ¹³
241(a)(1)	Feeble minded ¹³
241(a)(1)	Epileptic ¹³
241(a)(1)	Insane ¹³
241(a)(1)	Prior insanity ¹³
241(a)(1)	Constitutional psychopathic inferiority ¹³
241(a)(1)	Chronic alcoholic ¹³
241(a)(1)	Pauper ¹³
241(a)(1)	Professional beggar ¹³
241(a)(1)	Vagrant ¹³
241(a)(1)	Afflicted with tuberculosis ¹³
241(a)(1)	Afflicted with loathsome or dangerous contagious disease ¹³
241(a)(1)	Mental defective ¹³
241(a)(1)	Physical defect affecting ability to earn ¹³
241(a)(1)	Draft evader ¹³
241(a)(1)	Convicted of one CIMT ¹³
241(a)(1)	Admits having committed CIMT ¹³
241(a)(1)	Polygamist ¹³
241(a)(1)	Advocates of polygamy ¹³
241(a)(1)	Prostitute ¹³
241(a)(1)	Coming to engage in prostitution ¹³
241(a)(1)	Coming for immoral purpose ¹³
241(a)(1)	Procuring for prostitution ¹³
241(a)(1)	Imports a person for the purpose of prostitution ¹³
241(a)(1)	Supported by proceeds of prostitution ¹³
241(a)(1)	Contract laborer (offer or promise) ¹³
241(a)(1)	Contract laborer (agreement) ¹³
241(a)(1)	Contract laborer (advertisement) ¹³
241(a)(1)	Person likely to become a public charge ¹³
241(a)(1)	Previously excluded ¹³
241(a)(1)	Assisted alien to enter the United States by other than corporation ¹³
241(a)(1)	Assisted alien to enter the United States by a corporation ¹³

Appendix, Continued

Section of INA	Description
241(a)(1)	Stowaway ¹³
241(a)(1)	Unaccompanied alien under 16 years old ¹³
241(a)(1)	Barred zone native – from Asiatic Islands ¹³
241(a)(1)	Barred zone native – from mainland of Asia ¹³
241(a)(1)	Previously excluded as a prostitute ¹³
241(a)(1)	Illiterate ¹³
241(a)(1)	Laborer with limited passport ¹³
241(a)(1)	Previously excluded as procurer ¹³
241(a)(1)	Previously excluded as connected with prostitution ¹³
241(a)(1)	Previously excluded as person connected with the business of importation for prostitution ¹³
241(a)(1)	Previously excluded as prostitute ¹³
241(a)(1)	Previously deported as procurer ¹³
241(a)(1)	Previously deported as connected with the business of prostitution ¹³
241(a)(1)	Previously deported as connected with the business of importation for prostitution ¹³
241(a)(1)	Accompanying helpless excluded alien ¹³
241(a)(1)	Previously removed as distressed alien ¹³
241(a)(1)	Nonpossession of valid passport (nonseaman) ¹²
241(a)(1)	Nonpossession of valid passport (seaman) ¹²
241(a)(1)	Entry prejudicial to the interests of the United States ¹²
241(a)(1)	Previously excluded or deported as anarchist – entry prior to 9/23/50 ¹¹
241(a)(1)	Previously excluded or deported as anarchist – entry between 9/23/50 and 12/23/52 ¹¹
241(a)(1)	Previously deported as wartime undesirable alien ¹⁰
241(a)(1)	Immigrant not in possession of valid visa ⁹
241(a)(1)	Immigrant not in possession of valid non-quota visa ⁹
241(a)(1)	Not non-quota immigrant as specified ⁹
241(a)(1)	Immigrant not preference quota as specified in the visa ⁹
241(a)(1)	Immigrant not of nationality specified in the visa ⁹
241(a)(1)	Immigrant visa procured by fraud ⁹
241(a)(1)	Ineligible to citizenship ⁹
241(a)(1)	Arrival via nonsignatory line ⁹
241(a)(1)	Previously deported and returned within one year ⁸
241(a)(1)	Previously deported and returned without consent ⁸
241(a)(1)	Alien without visa, reentry permit or border crossing card ⁷
241(a)(1)	Fraudulent certificate of identity ⁶
241(a)(2)	Entry without inspection ⁵
241(a)(2)	Entry at time not designated ⁵
241(a)(2)	Entry at place not designated ⁵
241(a)(2) and 241(C)	Marriage fraud – marriage terminated ⁴
241(a)(2)	Entry without proper documents – Suspension of deportation cases only ⁴
241(a)(2) and 241(C)	Marriage fraud – nonfulfillment of marital agreement ⁴
241(a)(3)	Institutionalized because of mental disease within 5 years ⁵
241(a)(4)	Convicted of CIMT committed within 5 years after entry ⁵
241(a)(4)	Convicted of CIMT committed within 5 years after entry, confined one year or more ⁵
241(a)(4)	Convicted of two CIMTs after entry ⁵
241(a)(5)	Failure to furnish alien registration information ⁵
241(a)(5)	Convicted of false or fraudulent statements in alien registration information ⁵

(b)(5)

(b)(7)(e)

Appendix, Continued

Section of INA	Description
241(a)(5)	Convicted of false or fraudulent statements in alien registration information, 1940 Act ⁵
241(a)(5)	Convicted for violating Foreign Agents Registration Act ⁵
241(a)(5)	Convicted for visa fraud ⁵
241(a)(1)	Subversive – entry prior to 12/24/52 – 1918 Act ¹¹
241(a)(1)	Subversive – entry prior to 12/24/52 – 1918 Act, as amended ⁴
241(a)(1)	Subversive – entry on or after 12/24/52 ⁴
241(a)(1)	Have been subversive after entry ⁴
241(a)(8)	Became public charge within five years of entry ³
241(a)(9)	Failure to maintain nonimmigrant status ⁴
241(a)(9)(B)	Petition filed to remove conditional basis of status contained untrue facts and information
241(a)(9)	Failure to maintain nonimmigrant status ⁹
241(a)(9)	Failure to maintain or comply with changed nonimmigrant status ⁴
241(a)(2)	Nonimmigrant – remained longer ⁴
241(a)(2)	Nonimmigrant – remained longer ⁹
241(a)(2)	Nonimmigrant: Crewman refused permission to land ⁴
241(a)(9)(B)	Qualifying marriage judicially annulled or terminated other than through death of spouse
241(a)(9)(B)	A fee or other consideration was given for the filing of a petition on alien's behalf
241(a)(2)	Ag. Worker failed to maintain status ⁴
241(a)(9)(B)	Marriage entered into to procure admission as an immigrant
241(a)(2)	Ag. Worker failed to comply with conditions ⁴
241(a)(2)	Ag. Worker remained longer ⁴
241(a)(9)	Claim to nationality – failed to comply with conditions ⁷
241(a)(9)	Claim to nationality – failed to maintain nonimmigrant status ⁷
241(a)(10)	Arrival on nonsignatory line ⁵
241(a)(11)	Narcotic drug addicts ⁵
241(a)(11)	Narcotic drug addict after entry ⁵
241(a)(11)	Conviction for narcotic drug trafficking ⁵
241(a)(11)	Conviction – violation of narcotic drug law or regulation ⁵
241(a)(12)	Became a prostitute after entry ⁵
241(a)(12)	Engaged in prostitution after entry ⁵
241(a)(12)	Procured or attempted to procure prostitutes after entry ⁵
241(a)(12)	Imported or attempted to import prostitutes after entry ⁵
241(a)(12)	Supported by proceeds of prostitution after entry ⁵
241(a)(12)	Manager of house of prostitution after entry ⁵
241(a)(12)	Connected with management of house of prostitution after entry ⁵
241(a)(13)	Smuggling for gain, prior to entry ⁵
241(a)(13)	Smuggling for gain at time of entry ⁵
241(a)(13)	Smuggling for gain after entry ⁵
241(a)(14)	Conviction for misuse of firearms (sawed-off shotgun) ⁵
241(a)(15)	Convicted once of violating the Alien Registration Act ⁵
241(a)(16)	Convicted more than once of violating the Alien Registration Act ⁵
241(a)(17)	Conviction under wartime laws as undesirable resident ⁵
241(a)(18)	Convicted of importation for prostitution ⁵
241(a)(18)	Convicted of importation for prostitution (prior act) ⁵
241(a)(9)	Failed to maintain student status ⁹
241(a)(9)	Failed to maintain changed nonimmigrant status ⁹
241(a)(17)	Previously deported – reinstatement of prior order of deportation ⁴

(b)(7)(e)

(b)(5)

Appendix, Continued

Section of INA	Description
241(a)(9)(B)	Failed to appear for interview or file a petition to remove conditional basis of status
241(a)(1)	Not of status specified in nonimmigrant visa ¹
241(a)(1)	Immigrant visa not in compliance with Section 203 INA ¹
241(a)(1)	Immigrant visa not properly charged to quota specified ⁴
241(a)(1)	Immigrant visa not non-quota as specified ⁴
241(a)(1)	Immigrant visa not of proper status under quota as specified ⁴
241(a)(1)	Not entitled to special non-quota immigrant visa issued under Sec. 4(a) Refugee Relief Act of 1953 ⁴
241(a)(1)	Not entitled to non-quota immigrant visa as a refugee ⁴
241(a)(1)	Not entitled to non-quota immigrant visa as an escapee ⁴
241(a)(1)	Convicted of conspiracy trafficking in narcotic drugs ⁴
241(a)(1)	Convicted of possession of narcotic drugs ³
241(a)(1)	Convicted of conspiracy to possess narcotic drugs ³
241(a)(1)	Convicted of conspiracy to violate any narcotic drug law or regulation ³
241(a)(11)	Convicted of conspiracy to violate any law relating to trafficking in narcotic drugs ²
241(a)(11)	Convicted for possession of narcotic drugs ²
241(a)(11)	Convicted of conspiracy to possess narcotic drugs ³
241(a)(11)	Convicted of conspiracy to violate any narcotic drug law or regulation ³

Appendix, Continued

- 1 Effective 12/01/65
- 2 Effective 07/14/60
- 3 Effective 07/19/56
- 4 Effective 12/24/52
- 5 Effective 06/27/52
- 6 Effective 10/14/40
- 7 Effective 06/28/40
- 8 Effective 03/24/29
- 9 Effective 05/26/24
- 10 Effective 05/10/20
- 11 Effective 10/16/18
- 12 Effective 05/22/18
- 13 Effective 02/05/17

(b)(5)

(b)(7)(e)

Appendix, Continued

Exclusion Charge Codes

Effective Prior to June 1, 1991

Section of INA	Description
212(a)(1)	Mental Retardation
212(a)(2)	Insane
212(a)(3)	Attack of Insanity
212(a)(4)	Deviates
212(a)(5)	Addicts
212(a)(6)	Contagious Disease
212(a)(7)	Physical Disease
212(a)(8)	Paupers and beggars
212(a)(9)	Convicted of one CIMT
212(a)(10)	Convicted of two or more CIMT offenses
212(a)(11)	Polygamy
212(a)(12)	Prostitution
212(a)(13)	Immoral sexual act
212(a)(14)	Immigrant without labor certification
212(a)(15)	Likely to become a public charge
212(a)(16)	Previously excluded
212(a)(17)	Previously deported
212(a)(18)	Stowaway
212(a)(19)	Fraud
212(a)(20)	Immigrant without visa
212(a)(21)	Immigrant, wrong class on visa
212(a)(22)	Ineligible to citizenship
212(a)(23)	Narcotics
212(a)(24)	Arrival on non-signatory line
212(a)(25)	Illiterate
212(a)(26)	Nonimmigrant without documents
212(a)(27)	Prejudicial to the interests of the United States
212(a)(28)	Communist
212(a)(29)	Espionage, etc.
212(a)(30)	Accompanying excluded alien
212(a)(31)	Alien smuggler
212(a)(32)	Unqualified Physician
212(a)(33)	Assisted in Nazi Persecution

Appendix, Continued

**APPENDIX G
DOS Refusal Codes**

(b)(5)

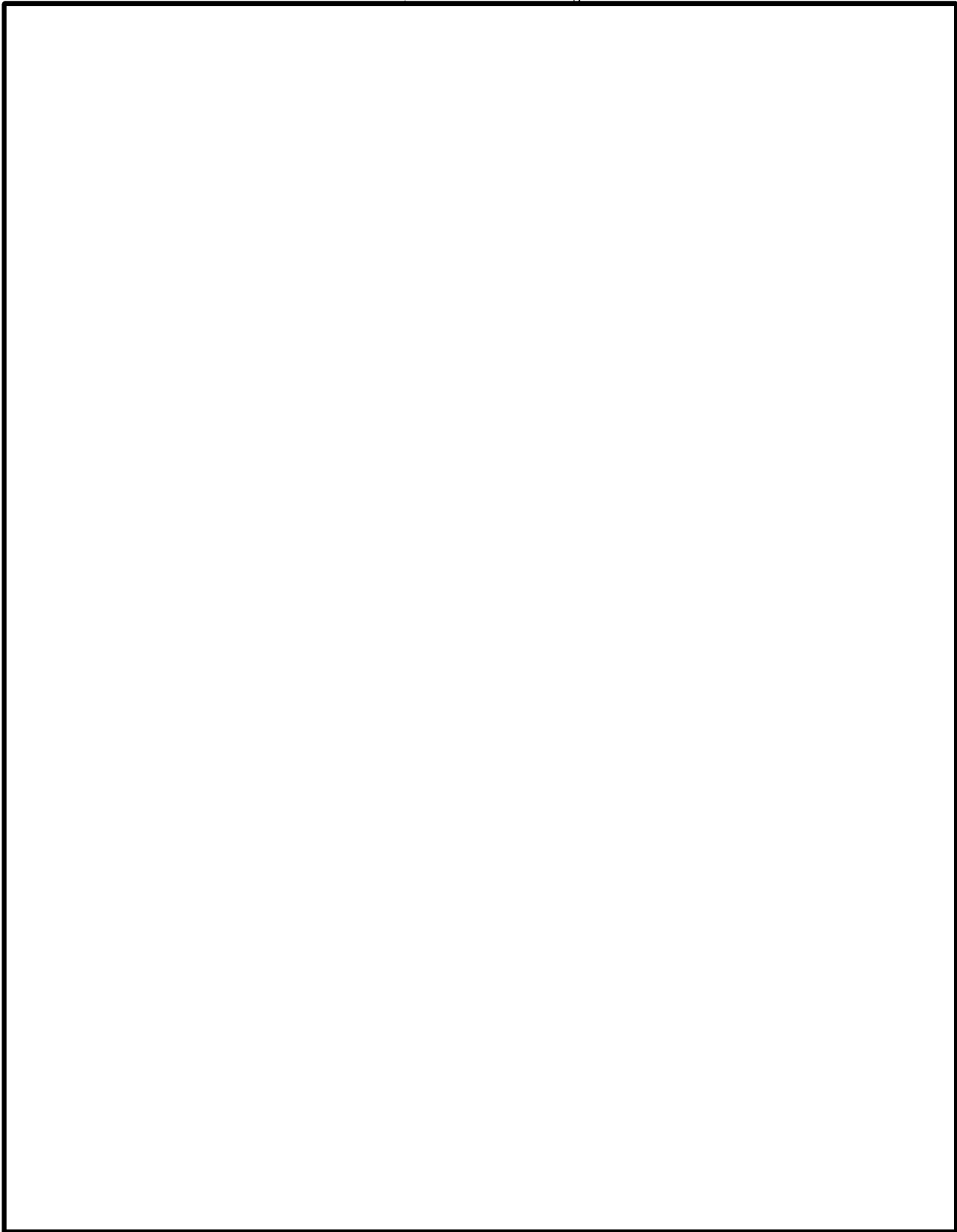
Appendix, Continued

(b)(7)(e)

DOS REFUSAL CODES

(b)(5)

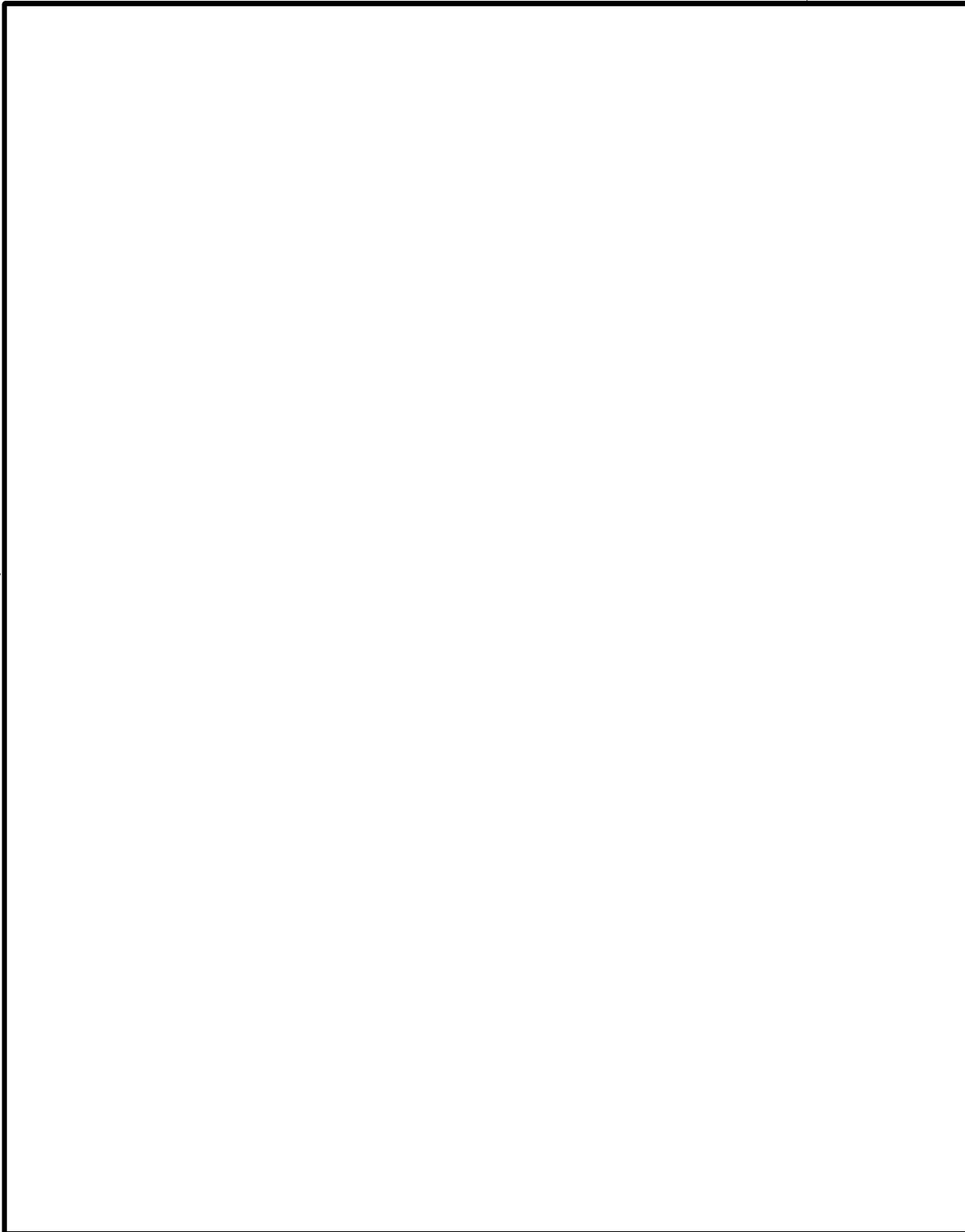
(b)(7)(e) **Appendix, Continued**



(b)(5)

(b)(7)(e)

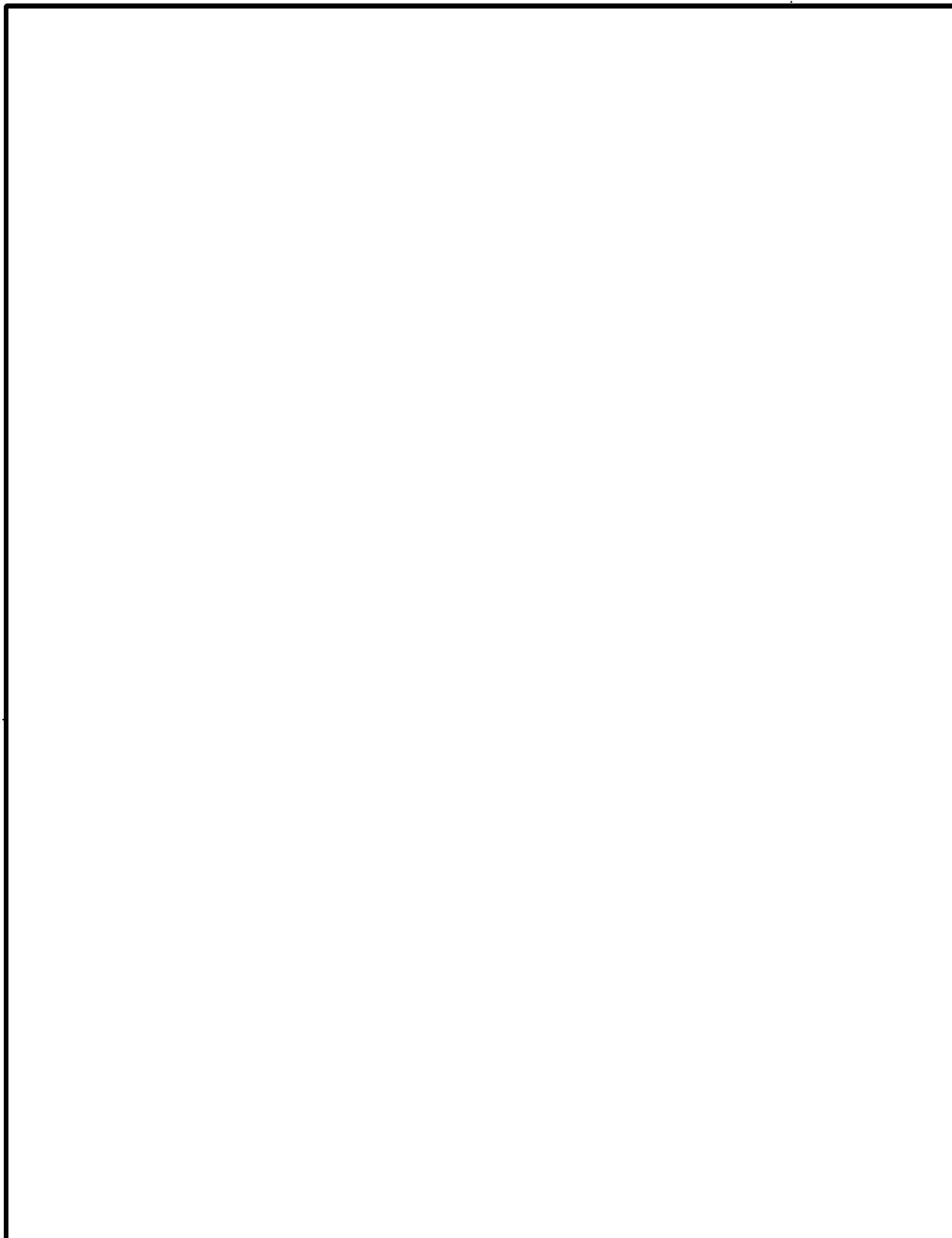
Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(5)

(b)(7)(e)

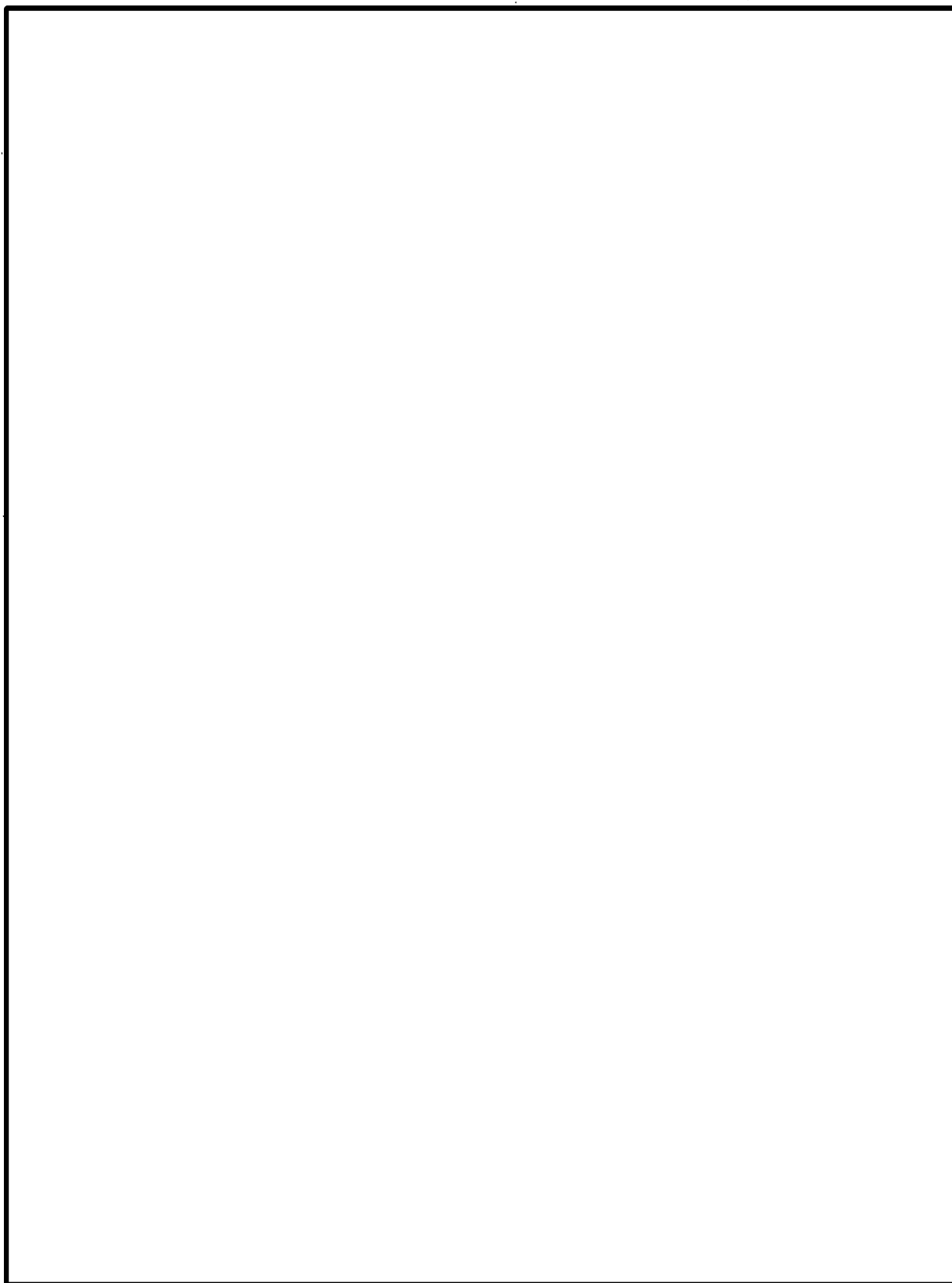
Appendix, Continued



(b)(7)(e)

(b)(5)

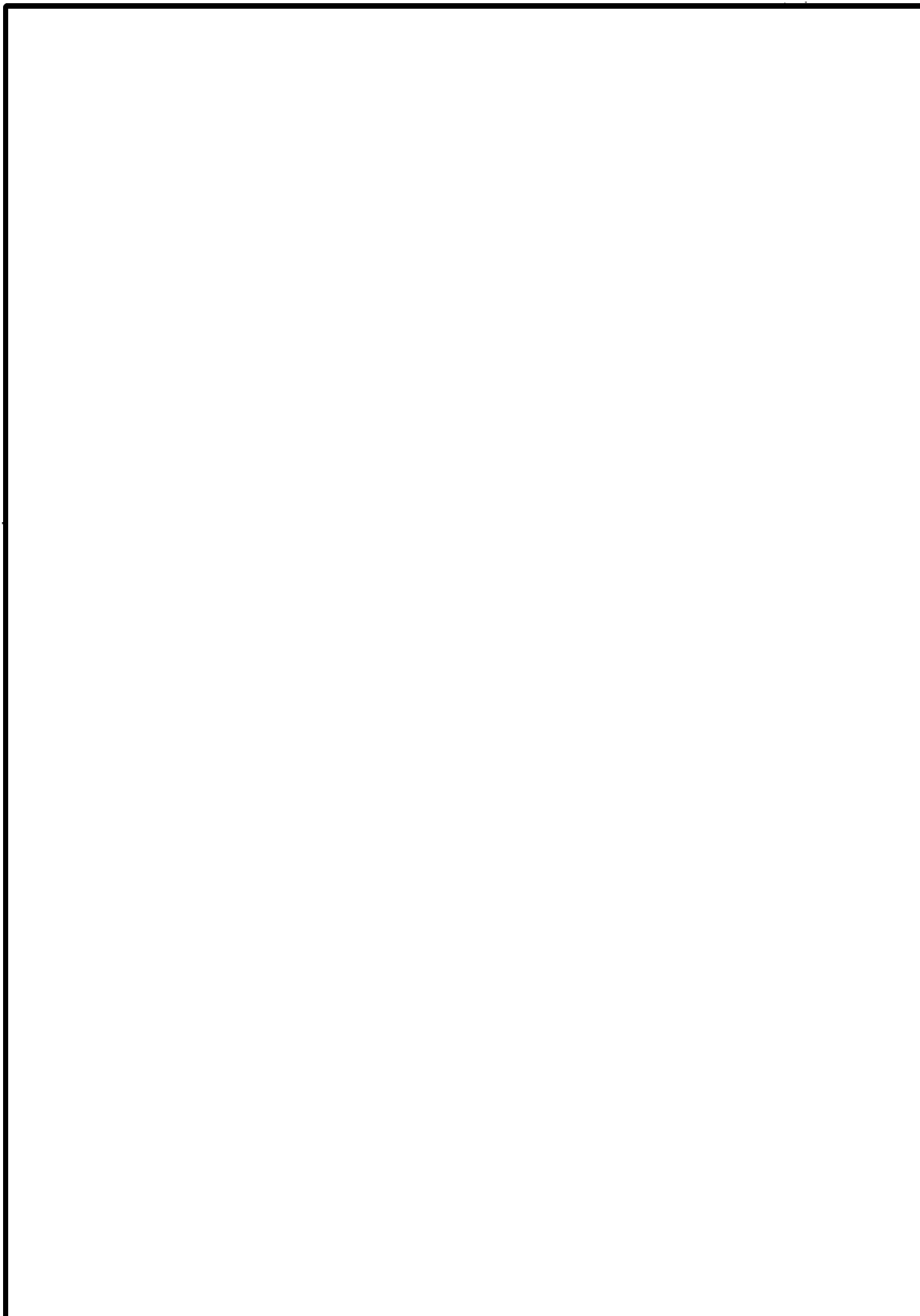
Appendix, Continued



(b)(5)

(b)(7)(e)

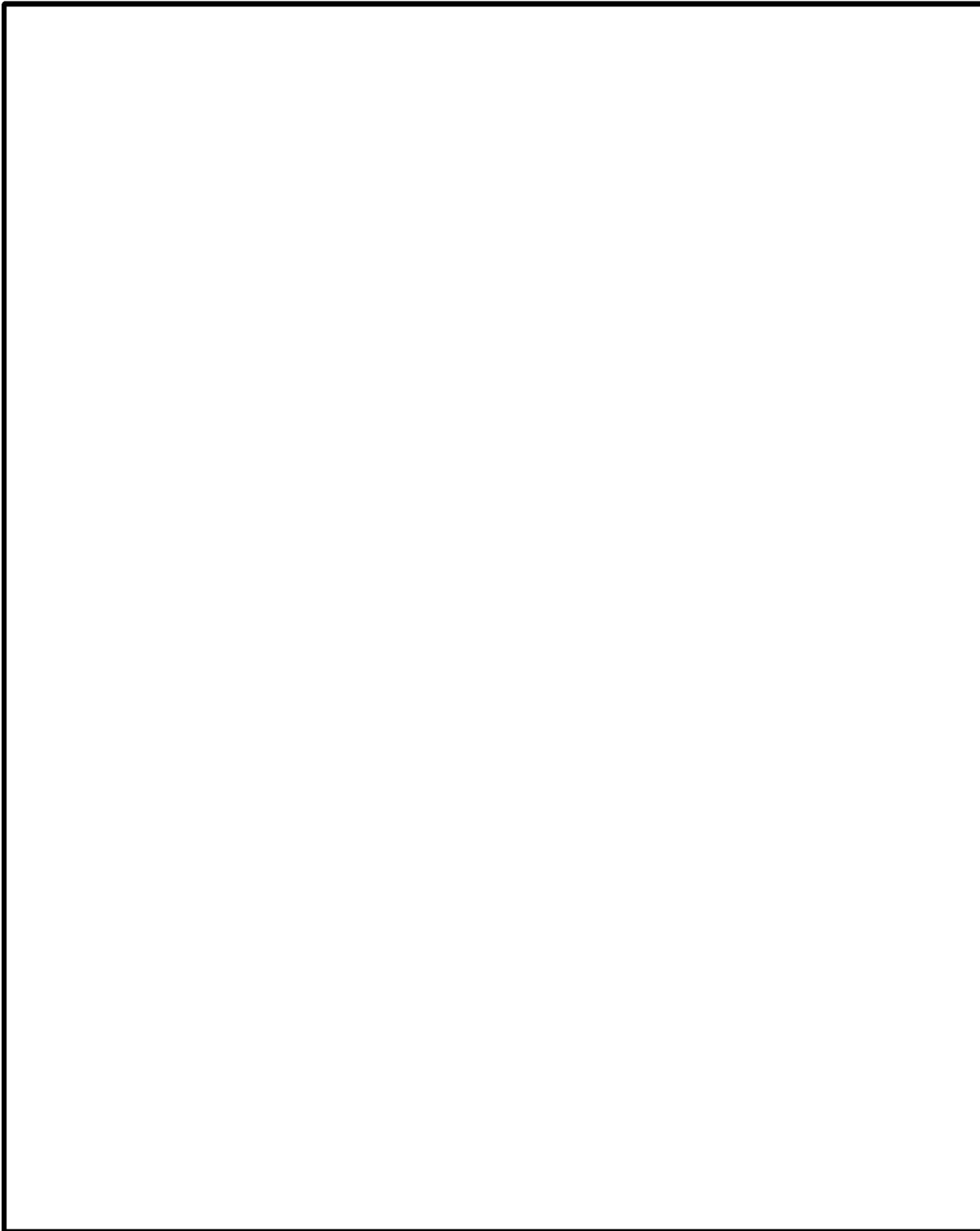
Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



Appendix, Continued

APPENDIX H
Accessing National Crime Information Center Interstate
Identification Index (NCIC III) Data
(June 17, 2005)

IBIS NN-16 User Agreement

United States Citizenship and Immigration Services
IBIS SOP March 1, 2006
~~For Official Use Only~~

Appendix
Page 170

Appendix, Continued

(b)(5)



(b)(5)

Appendix, Continued

**APPENDIX I
CLARIFICATION and MODIFICATION
of New Resolution Process for IBIS National
Security/Terrorism-Related Positive Results
(March 29, 2005)**

Appendix, Continued

U.S. Department of Homeland Security
Washington, DC 20251



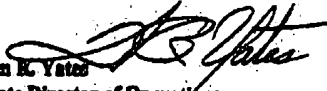
U.S. Citizenship
and Immigration
Services

HQ 702.1

Interoffice Memorandum

(b)(5)

To: Asylum Directors
Regional Directors
District Directors
Service Center Directors
National Benefits Center Director

From: 
William R. Yates
Associate Director of Operations


for Joseph Caddah
Associate Director, Office of Refugee, Asylum, and International Relations

Date: March 29, 2006

Subject: CLARIFICATION and MODIFICATION of New Resolution Process for IBIS National Security/Terrorism-Related Positive Results



(b)(5)

(b)(5)

(b)(5)

Appendix, Continued

APPENDIX J
National Security and Public Safety
Adjudications Unit--FOCUS
(March 29, 2005)

Appendix, Continued

U.S. Department of Homeland Security
20 Massachusetts Avenue
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

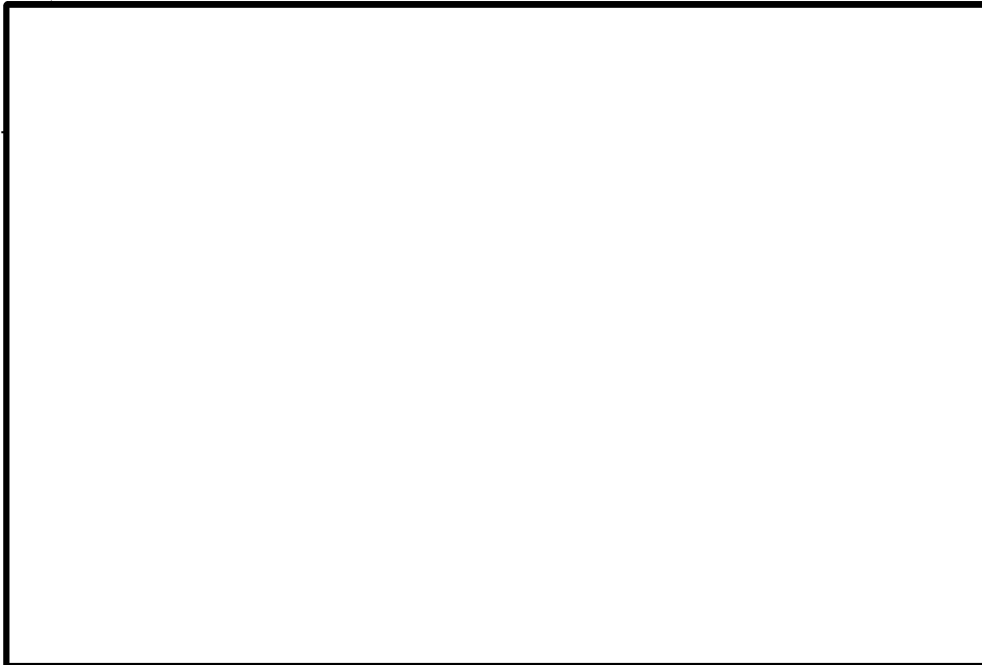
March 29, 2005

Interoffice Memorandum

To: REGIONAL DIRECTORS
DISTRICT DIRECTORS
NATIONAL BENEFITS DIRECTOR
SERVICE CENTER DIRECTORS
FRAUD DETECTION AND NATIONAL SECURITY DIRECTOR
OFFICE OF CHIEF COUNSEL
DIRECTOR OF TRAINING, FLETC

From: William R. Yates
Director,
Domestic Operations

Re: National Security and Public Safety Adjudications Unit—FOCUS



Appendix, Continued

(b)(5)

National Security and Public Safety Adjudications Unit—FOCUS
Page 2



Appendix, Continued

APPENDIX K
Discontinuation of IBIS Alias Name Checks for Petitions and
Applications When the Beneficiary and Dependents are not
Physically Present in the United States
(March 23, 2005)

Appendix, Continued

U.S. Department of Homeland Security
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

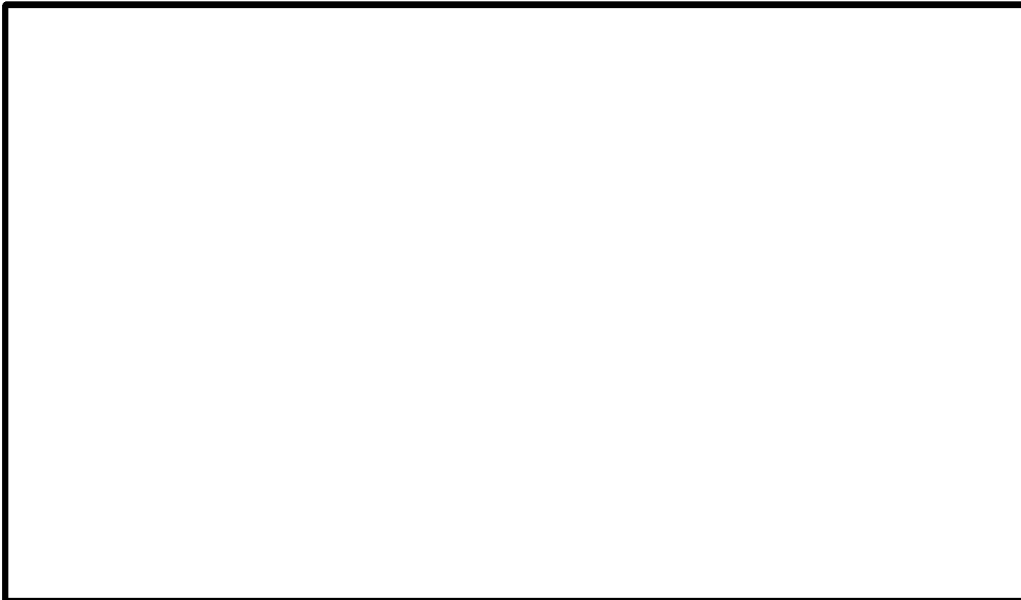
Interoffice Memorandum

To: REGIONAL DIRECTORS
SERVICE CENTER DIRECTORS
DISTRICT DIRECTORS
NATIONAL BENEFITS CENTER DIRECTOR

From: William R. Yates /S/
Associate Director of Operations
U.S. Citizenship and Immigration Services

Date: March 23, 2005

Re: Discontinuation of IBIS Alias Name Checks for Petitions and Applications When the Beneficiary and Dependents are not Physically Present in the United States



(b)(5)

(b)(5)

Appendix, Continued

APPENDIX L
Safeguarding Sensitive but Unclassified Information
(January 27, 2005)

Safeguarding Sensitive but Unclassified
(For Official Use Only) Information
(January 6, 2005)

Management Directive 11042.1, "Safeguarding Sensitive but
Unclassified (For Official Use Only) Information"
(January 11, 2005)

Appendix, Continued

U.S. Department of Homeland Security
20 Massachusetts Avenue, NW
Washington, DC 20529



U.S. Citizenship
and Immigration
Services

Interoffice Memorandum

To: Management Team

From: Michael Maxwell /S/
Director, Office of Security and Investigations

Date: January 27, 2005

Re: Safeguarding Sensitive but Unclassified Information

On January 6, 2005, the Department of Homeland Security revised portions of its policy on the handling of sensitive but unclassified (SBU) information. The changes are reflected in DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, the governing directive for all DHS employees and contractors on protecting SBU information from unauthorized disclosure. The purpose of this memorandum is to provide USCIS personnel with the updated version of the directive, along with a memo from Janet Hale, DHS Under Secretary for Management, explaining recent revisions (see attached).

As a result of the changes, federal employees of DHS will no longer be required to sign a non-disclosure agreement for access to SBU information. The directive affirms, however, that all DHS employees, detailees, contractors and consultants will receive formal training on the requirements for safeguarding For Official Use Only (FOUO) information and other SBU information.

All USCIS employees are expected to read and familiarize themselves with this directive, which establishes the procedures to be followed when USCIS personnel come into possession of SBU information.

The directive establishes that DHS uses the term "For Official Use Only" to identify a prominent subcategory of SBU information - "unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, 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." Part 6 provides some of the most common categories of information that should be considered FOUO (Section C), but allows supervisory personnel the authority to designate other types of information FOUO as well (Section D).

Access to FOUO information should be withheld from all but those who have been determined to have a valid "need-to-know" in performance of an authorized government duty. To achieve this end,

www.uscis.gov

Appendix, Continued

Page 2

employees are obligated to adhere to the handling requirements set forth in the directive. Standards for marking, storage, dissemination, transmission and destruction are provided.

The directive also identifies other categories of SBU information, all covered by their own statutes. The most common example encountered at USCIS is information found in "records maintained on individuals," also known as Privacy Act information because it is covered by 5 U.S.C. 552A, *The Privacy Act of 1974*. Privacy Act information should be handled in accordance with FOUO standards. For other special categories, such as Tax Return information, Grand Jury information and Critical Infrastructure Information, the applicable statute should be consulted to determine handling requirements. At a minimum, all sensitive information must be protected in accordance with FOUO standards.

All employees are reminded that procedures for handling SBU information do not apply to classified national security information (NSI). Access to classified NSI (security clearance) can only be granted by the authority of the USCIS Office of Security and Investigations, Personnel Security Unit.

The attached directive can also be found under the Security link on DHS Online. Any questions pertaining to this policy should be directed to your local Security Officer, or to John M. Shephard, Administrative Security Unit, Headquarters Office of Security and Investigations, at (202) 272-1217.

Appendix, Continued

Department of Homeland Security
Management Directive System
MD Number: 11042.1

SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION

1.6.2006

1. Purpose

This directive establishes Department of Homeland Security (DHS) policy regarding the identification and safeguarding of sensitive but unclassified information originated within DHS. It also applies to other sensitive but unclassified information received by DHS from other government and non-governmental activities.

2. Scope

This directive is applicable to all DHS Headquarters, components, organizational elements, detailees, contractors, consultants, and others to whom access to information covered by this directive is granted.

3. Authorities

Homeland Security Act of 2002.

4. Definitions

Access: The ability or opportunity to gain knowledge of information.

For Official Use Only (FOUO): The term used within DHS to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, 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. Information impacting the National Security of the United States and classified Confidential, Secret, or Top Secret under Executive Order 12958; "Classified National Security Information," as amended, or its predecessor or successor orders, is not to be considered FOUO. FOUO is not to be considered classified information.

Need-to-know: The determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to

MD 11042.1

Appendix, Continued

perform or assist in a lawful and authorized governmental function, i.e., access is required for the performance of official duties.

Organizational Element: As used in this directive, organizational element is as defined in DHS MD Number 0010.1, Management Directive System and DHS Announcements.

Protected Critical Infrastructure Information (PCII): Critical infrastructure information (CII) is defined in 6 U.S.C. 131(3) (Section 212(3) of the Homeland Security Act). Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Protected Critical Infrastructure Information is a subset of CII that is voluntarily submitted to the Federal Government and for which protection is requested under the PCII program by the requestor.

Sensitive Security Information (SSI): Sensitive security information (SSI) is defined in 49 C.F.R. Part 1520. SSI is a specific category of information that requires protection against disclosure. 49 U.S.C. 40119 limits the disclosure of information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy; reveal a trade secret or privileged or confidential commercial or financial information; or be detrimental to the safety of passengers in transportation.

5. Responsibilities

A. The DHS Office of Security will:

1. Be responsible for practical application of all aspects of the program to protect FOUO.
2. Promulgate Department-wide policy guidance.
3. Develop and implement an education and awareness program for the safeguarding of FOUO and other sensitive but unclassified information.

B. Heads of DHS Organizational Elements will:

1. Ensure compliance with the standards for safeguarding FOUO and other sensitive but unclassified information as cited in this directive.
2. Designate an official to serve as a Security Officer or Security Liaison.

C. The organizational element's Security Officer/Security Liaison will:

Appendix, Continued

Be responsible for implementation and oversight of the FOUO information protection program and will serve as liaison between the DHS Office of Security and other organizational security officers.

D. DHS employees, detailees, contractors, consultants and others to whom access is granted will:

1. Be aware of and comply with the safeguarding requirements for FOUO information as outlined in this directive.
2. Participate in formal classroom or computer based training sessions presented to communicate the requirements for safeguarding FOUO and other sensitive but unclassified information.
3. Be aware that divulging information without proper authority could result in administrative or disciplinary action.

E. Contractors and Consultants shall:

Execute a DHS Form 11000-6, Sensitive But Unclassified Information Non-Disclosure Agreement (NDA), as a condition of access to such information. Other individuals not assigned to or contractually obligated to DHS, but to whom access to information will be granted, may be requested to execute an NDA as determined by the applicable program manager. Execution of the NDA shall be effective upon publication of this directive and not applied retroactively.

F. Supervisors and managers will:

1. Ensure that an adequate level of education and awareness is established and maintained that serves to emphasize safeguarding and prevent unauthorized disclosure of FOUO information.
2. Take appropriate corrective actions, to include administrative or disciplinary action as appropriate, when violations occur.

6. Policy and Procedures

A. General

1. The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive

Appendix, Continued

order or an act of Congress to be kept secret in the interest of national defense or foreign policy." However, with the exception of certain types of information protected by statute, specific, standard criteria and terminology defining the types of information warranting designation as "sensitive information" does not exist within the Federal government. Such designations are left to the discretion of each individual agency.

2. Within the "sensitive but unclassified" arena, in addition to the various categories of information specifically described and protected by statute or regulation, e.g., Tax Return Information, Privacy Act Information, Sensitive Security Information (SSI), Critical Infrastructure Information (CII), Grand Jury Information, etc. There are numerous additional caveats used by various agencies to identify unclassified information as sensitive, e.g., For Official Use Only, Law Enforcement Sensitive, Official Use Only, Limited Official Use, etc. Regardless of the caveat used to identify it, however, the reason for the designation does not change. Information is designated as sensitive to control and restrict access to certain information, the release of which could cause harm to a person's privacy or welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding of our national interests.

3. Information shall not be designated as FOUO in order to conceal government negligence, ineptitude, illegalities, or other disreputable circumstances embarrassing to a government agency.

4. Information designated as FOUO is not automatically exempt from disclosure under the provisions of the Freedom of Information Act, 5 U.S.C. 552, (FOIA). Information requested by the public under a FOIA request must still be reviewed on a case-by-case basis.

B. For Official Use Only

Within DHS, the caveat "FOR OFFICIAL USE ONLY" will be used to identify sensitive but unclassified information within the DHS community that is not otherwise specifically described and governed by statute or regulation. The use of these and other approved caveats will be governed by the statutes and regulations issued for the applicable category of information.

C. Information Designated as FOUO

1. The following types of information will be treated as FOUO information. Where information cited below also meets the standards for designation pursuant to other existing statutes or regulations, the applicable statutory or regulatory guidance will take precedence. For example, should information meet the standards for designation as Sensitive Security Information (SSI), then SSI guidance for marking, handling, and safeguarding will take precedence.

Appendix, Continued

- (a) Information of the type that may be exempt from disclosure per 5 U.S.C. 552, Freedom of Information Act, and its amendments. Designation of information as FOUO does not imply that the information is already exempt from disclosure under FOIA. Requests under FOIA for information designated as FOUO, will be reviewed and processed in the same manner as any other FOIA request.
- (b) Information exempt from disclosure per 5 U.S.C. 552a, Privacy Act.
- (c) Information within the international and domestic banking and financial communities protected by statute, treaty, or other agreements.
- (d) Other international and domestic information protected by statute, treaty, regulation or other agreements.
- (e) Information that could be sold for profit.
- (f) Information that could result in physical risk to personnel.
- (g) DHS information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 12958, as amended, will be classified as appropriate.
- (h) Systems security data revealing the security posture of the system. For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.
- (i) Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended.
- (j) Information that could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security.
- (k) Developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with

Appendix, Continued

sufficient information to clone, counterfeit, or circumvent a process or system.

2. Other government agencies and international organizations may use different terminology to identify sensitive information, such as "Limited Official Use (LOU)," and "Official Use Only (OUO)." In most instances the safeguarding requirements for this type of information are equivalent to FOUO. However, other agencies and international organizations may have additional requirements concerning the safeguarding of sensitive information. Follow the safeguarding guidance provided by the other agency or organization. Should there be no such guidance, the information will be safeguarded in accordance with the requirements for FOUO as provided in this manual. Should the additional guidance be less restrictive than in this directive, the information will be safeguarded in accordance with this directive.

D. Designation Authority

Any DHS employee, detailee, or contractor can designate information falling within one or more of the categories cited in section 8, paragraph C, as FOUO. Officials occupying supervisory or managerial positions are authorized to designate other information, not listed above and originating under their jurisdiction, as FOUO.

E. Duration of Designation

Information designated as FOUO will retain its designation until determined otherwise by the originator or a supervisory or management official having program management responsibility over the originator and/or the information.

F. Marking

1. Information designated as FOUO will be sufficiently marked so that persons having access to it are aware of its sensitivity and protection requirements. The lack of FOUO markings on materials does not relieve the holder from safeguarding responsibilities. Where the FOUO marking is not present on materials known by the holder to be FOUO, the holder of the material will protect it as FOUO. Other sensitive information protected by statute or regulation, e.g., PCI and SSI, etc., will be marked in accordance with the applicable guidance for that type of information. Information marked in accordance with the guidance provided for the type of information need not be additionally marked FOUO.

(a) Prominently mark the bottom of the front cover, first page, title page, back cover and each individual page containing FOUO information with the caveat "FOR OFFICIAL USE ONLY."

Appendix, Continued

(b) Materials containing specific types of FOUO may be further marked with the applicable caveat, e.g., "LAW ENFORCEMENT SENSITIVE," in order to alert the reader of the type of information conveyed. Where the sensitivity of the information warrants additional access and dissemination restrictions, the originator may cite additional access and dissemination restrictions. For example:

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

(c) Materials being transmitted to recipients outside of DHS, for example, other federal agencies, state or local officials, etc. who may not be aware of what the FOUO caveat represents, shall include the following additional notice:

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

(d) Computer storage media, i.e., disks, tapes, removable drives, etc., containing FOUO information will be marked "FOR OFFICIAL USE ONLY."

(e) Portions of a classified document, i.e., subjects, titles, paragraphs, and subparagraphs that contain only FOUO information will be marked with the abbreviation (FOUO).

(f) Individual portion markings on a document that contains no other designation are not required.

(g) Designator or originator information and markings, downgrading instructions, and data/event markings are not required.

G. General Handling Procedures

Although FOUO is the DHS standard caveat for identifying sensitive unclassified information, some types of FOUO information may be more sensitive than others

Appendix, Continued

and thus warrant additional safeguarding measures beyond the minimum requirements established in this manual. For example, certain types of information may be considered extremely sensitive based on the repercussions that could result should the information be released or compromised. Such repercussions could be the loss of life or compromise of an informant or operation. Additional control requirements may be added as necessary to afford appropriate protection to the information. DHS employees, contractors, and detailees must use sound judgment coupled with an evaluation of the risks, vulnerabilities, and the potential damage to personnel or property as the basis for determining the need for safeguards in excess of the minimum requirements and protect the information accordingly.

1. When removed from an authorized storage location (see section 8.1) and persons without a need-to-know are present, or where casual observation would reveal FOUO information to unauthorized persons, a "FOR OFFICIAL USE ONLY" cover sheet (Enclosure 1) will be used to prevent unauthorized or inadvertent disclosure.
2. When forwarding FOUO information, a FOUO cover sheet should be placed on top of the transmittal letter, memorandum or document.
3. When receiving FOUO equivalent information from another government agency, handle in accordance with the guidance provided by the other government agency. Where no guidance is provided, handle in accordance with the requirements of this directive.

H. Dissemination and Access

1. FOUO information will not be disseminated in any manner - orally, visually, or electronically - to unauthorized personnel.
2. 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.
3. The holder of the information will comply with any access and dissemination restrictions.
4. A security clearance is not required for access to FOUO information.
5. When discussing or transferring FOUO information to another individual(s), ensure that the individual with whom the discussion is to be held or the information is to be transferred has a valid need-to-know, and that precautions are taken to prevent unauthorized individuals from overhearing the conversation, observing the materials, or otherwise obtaining the information.

Appendix, Continued

6. FOUO information may be shared with other agencies, federal, state, tribal, or local government and law enforcement officials, provided a specific need-to-know has been established and the information is shared in furtherance of a coordinated and official governmental activity. Where FOUO information is requested by an official of another agency and there is no coordinated or other official governmental activity, a written request will be made from the requesting agency to the applicable DHS program office providing the name(s) of personnel for whom access is requested, the specific information to which access is requested, and basis for need-to-know. The DHS program office shall then determine if it is appropriate to release the information to the other agency official. (see section 6.F for marking requirements)
7. Other sensitive information protected by statute or regulation, i.e., Privacy Act, CII, SSI, Grand Jury, etc., will be controlled and disseminated in accordance with the applicable guidance for that type of information.
8. If the information requested or to be discussed belongs to another agency or organization, comply with that agency's policy concerning third party discussion and dissemination.
9. When discussing FOUO information over a telephone, the use of a STU III (Secure Telephone Unit), or Secure Telephone Equipment (STE), is encouraged, but not required.

I. Storage

1. When unattended, FOUO materials will, at a minimum, be stored in a locked file cabinet, locked desk drawer, a locked overhead storage compartment such as a systems furniture credenza, or similar locked compartment. Materials can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know, such as a locked room, or an area where access is controlled by a guard, cipher lock, or card reader.
2. FOUO information will not be stored in the same container used for the storage of classified information unless there is a correlation between the information. When FOUO materials are stored in the same container used for the storage of classified materials, they will be segregated from the classified materials to the extent possible, i.e. separate folders, separate drawers, etc.
3. IT systems that store FOUO information will be certified and accredited for operation in accordance with federal and DHS standards. Consult the DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A, for more detailed information.

Appendix, Continued

4. Laptop computers and other media containing FOUO information will be stored and protected to prevent loss, theft, unauthorized access and unauthorized disclosure. Storage and control will be in accordance with DHS Information Technology Security Program Handbook for Sensitive Systems, Publication 4300A.

J. Transmission

1. Transmission of hard copy FOUO within the U.S. and its Territories:
 - (a) Material will be placed in a single opaque envelope or container and sufficiently sealed to prevent inadvertent opening and to show evidence of tampering. The envelope or container will bear the complete name and address of the sender and addressee, to include program office and the name of the intended recipient (if known).
 - (b) FOUO materials may be mailed by U.S. Postal Service First Class Mail or an accountable commercial delivery service such as Federal Express or United Parcel Service.
 - (c) FOUO materials may be entered into an inter-office mail system provided it is afforded sufficient protection to prevent unauthorized access, e.g., sealed envelope.
2. Transmission to Overseas Offices: When an overseas office is serviced by a military postal facility, i.e., APO/FPO, FOUO may be transmitted directly to the office. Where the overseas office is not serviced by a military postal facility, the materials will be sent through the Department of State, Diplomatic Courier.
3. Electronic Transmission.
 - (a) Transmittal via Fax. Unless otherwise restricted by the originator, FOUO information may be sent via nonsecure fax. However, the use of a secure fax machine is highly encouraged. Where a nonsecure fax is used, the sender will coordinate with the recipient to ensure that the materials faxed will not be left unattended or subjected to possible unauthorized disclosure on the receiving end. The holder of the material will comply with any access, dissemination, and transmittal restrictions cited on the material or verbally communicated by the originator.
 - (b) Transmittal via E-Mail
 - (i) FOUO information transmitted via email should be protected by encryption or transmitted within secure communications systems. When this is impractical or unavailable, FOUO may be transmitted over regular email channels. For added security, when

Appendix, Continued

transmitting FOUO over a regular email channel, the information can be included as a password protected attachment with the password provided under separate cover. Recipients of FOUO information will comply with any email restrictions imposed by the originator.

(ii) Per DHS MD 4300, DHS Sensitive Systems Handbook, due to inherent vulnerabilities, FOUO information shall not be sent to personal email accounts.

(c) DHS Internet/Intranet

(i) FOUO information will not be posted on a DHS or any other internet (public) website.

(ii) FOUO information may be posted on the DHS intranet or other government controlled or sponsored protected encrypted data networks, such as the Homeland Security Information Network (HSIN). However, the official authorized to post the information should be aware that access to the information is open to all personnel who have been granted access to that particular intranet site. The official must determine the nature of the information is such that need-to-know applies to all personnel; the benefits of posting the information outweigh the risk of potential compromise; the information posted is prominently marked as FOR OFFICIAL USE ONLY; and information posted does not violate any provisions of the Privacy Act.

K. Destruction

1. FOUO material will be destroyed when no longer needed. Destruction may be accomplished by:

(a) "Hard Copy" materials will be destroyed by shredding, burning, pulping, pulverizing, such as to assure destruction beyond recognition and reconstruction. After destruction, materials may be disposed of with normal waste.

(b) Electronic storage media shall be sanitized appropriately by overwriting or degaussing. Contact local IT security personnel for additional guidance.

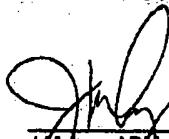
(c) Paper products containing FOUO information will not be disposed of in regular trash or recycling receptacles unless the materials have first been destroyed as specified above.

Appendix, Continued

L. Incident Reporting

1. The loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will be reported. Incidents involving FOUO in DHS IT systems will be reported to the organizational element Computer Security Incident Response Center in accordance with IT incident reporting requirements.
2. Suspicious or inappropriate requests for information by any means, e.g., email or verbal, shall be report to the DHS Office of Security.
3. Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will report it immediately, but not later than the next duty day, to the originator and the local Security Official.
4. Additional notifications to appropriate DHS management personnel will be made without delay when the disclosure or compromise could result in physical harm to an individual(s) or the compromise of a planned or on-going operation.
5. At the request of the originator, an inquiry will be conducted by the local security official or other designee to determine the cause and affect of the incident and the appropriateness of administrative or disciplinary action against the offender.

Dated: 1/6/05



J.M. Loy, ADM
Deputy Secretary of Homeland Security

Department of Homeland Security

FOR OFFICIAL USE ONLY

THE ATTACHED MATERIALS CONTAIN DEPARTMENT OF HOMELAND SECURITY INFORMATION THAT IS "FOR OFFICIAL USE ONLY," OR OTHER TYPES OF SENSITIVE BUT UNCLASSIFIED INFORMATION REQUIRING PROTECTION AGAINST UNAUTHORIZED DISCLOSURE. THE ATTACHED MATERIALS WILL BE HANDLED AND SAFEGUARDED IN ACCORDANCE WITH DHS MANAGEMENT DIRECTIVES GOVERNING PROTECTION AND DISSEMINATION OF SUCH INFORMATION.

AT A MINIMUM, THE ATTACHED MATERIALS WILL BE DISSEMINATED ONLY ON A "NEED-TO-KNOW" BASIS AND WHEN UNATTENDED, WILL BE STORED IN A LOCKED CONTAINER OR AREA OFFERING SUFFICIENT PROTECTION AGAINST THEFT, COMPROMISE, INADVERTENT ACCESS AND UNAUTHORIZED DISCLOSURE.

Appendix, Continued

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



**Homeland
Security**

January 11, 2005

TO: Under Secretaries
General Counsel
Chief of Staff
Executive Secretary
Commandant, U.S. Coast Guard
Director, U.S. Citizenship and Immigration Services
Director, U.S. Secret Service
Director, Office of State and Local Government
Coordination and Preparedness
Director, Federal Law Enforcement Training Center
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Commissioner, U.S. Customs and Border Protection
Assistant Secretary, U.S. Immigration and Customs
Enforcement
Assistant Secretary, Transportation Security Administration

FROM: Janet Hale, *M. Hale*
Under Secretary for Management

SUBJECT: Management Directive 11042.1, "Safeguarding Sensitive but
Unclassified (For Official Use Only) Information"

DHS is uniquely situated due to its mission to protect the nation's homeland and infrastructure. As a result, DHS employees are entrusted with vast amounts of sensitive but unclassified (SBU) information every day, and regularly and rightfully share it with other Federal agencies and our partners in state and local governments, tribal officials, and the private-sector. Examples of these types of information include:

- Vulnerability assessments of the nation's critical infrastructure, including Protected Critical Infrastructure Information (PCII), e.g., bridges and tunnels, pipelines for hazardous/flammable liquids, air-traffic equipment, and government buildings;
- Information technology systems servicing these critical infrastructure facilities;

www.dhs.gov

Appendix, Continued

- Strategic and tactical law enforcement plans, capabilities, operations, and investigative techniques, methods, and sources;
- Research and development of sensitive technology, including proprietary information, as well as information about devices to detect chemical, biological or other destructive weaponry; and
- Information that could endanger the physical security and safety of DHS employees.

Protecting this SBU information is therefore an essential element of ensuring the nation's homeland security as is sharing it with those that need it. To safeguard this information without impeding its legitimate flow, DHS established Management Directive (MD) 11042 "Safeguarding Sensitive but Unclassified (For Official Use Only) Information" in May 2004. This policy was created in order to define for our employees what constitutes SBU information and provide standards to safeguard it. Included in this initial policy was a requirement to execute a Non-Disclosure Agreement (NDA) for access to SBU information. This provision was designed as an interim measure to efficiently and effectively educate employees and communicate the standards promulgated by the MD.

Effective January 6, 2005, MD 11042 has been superseded by revised version MD 11042.1 that expands upon and formalizes its educational purpose without the need for our employees or Federal detailees to complete an NDA. Pursuant to the revised policy, the DHS Office of Security will develop and implement an education and awareness program for the safeguarding of SBU information. Once this program is developed and appropriate notifications are provided, all employees will participate in classroom or computer-based training sessions designed to educate employees on what constitutes SBU information and the standards for handling and disseminating it. Completion of this training will ensure that each employee has the knowledge they need to recognize and handle SBU information responsibly.

Those NDA's previously signed by DHS employees pursuant to MD 11042 will no longer be valid. The Office of Security in a subsequent communication will provide instructions for the proper collection of these documents. DHS will take reasonable steps to retrieve these documents and destroy them in accordance with DHS records management policy. All employees, however, are reminded that they are obligated to follow the statutory and regulatory requirements governing the handling and dissemination of all categories of SBU information.

MD 11042.1 is available online at www.dhsonline.dhs.gov.

Appendix, Continued

APPENDIX M
New Resolution Process for IBIS National
Security/Terrorism-Related Positive Results
(November 29, 2004)

IBIS National Security Case Resolution Request

IBIS-National Security Record

IBIS-National Security Notification

Appendix, Continued

U.S. Department of Homeland Security
Washington, DC 20258



U.S. Citizenship
and Immigration
Services

HQ 70/2.1

(b)(5)

Interoffice Memorandum

To: Asylum Directors
Regional Directors
District Directors
Service Center Directors
National Benefits Center Director

From: William R. Yates /S/
Associate Director of Operations

Joseph Cuddihy
Associate Director, Office of Refugee, Asylum, and International Relations

Date: November 29, 2004

Subject: New Resolution Process for IBIS National Security/Terrorism-Related Positive Results



(b)(5)

(b)(5)

(b)(7)(c)

(b)(5)

(b)(7)(e)

(b)(5)

(b)(7)(e)

(b)(5)

(b)(7)(e)

(b)(5)

(b)(7)(e)

Appendix, Continued

APPENDIX N
Required Security Checks
(August 4, 2004)

Appendix, Continued

(b)(5)

U.S. Department of Homeland Security
Street Address
City, State Zip



U.S. Citizenship
and Immigration
Services

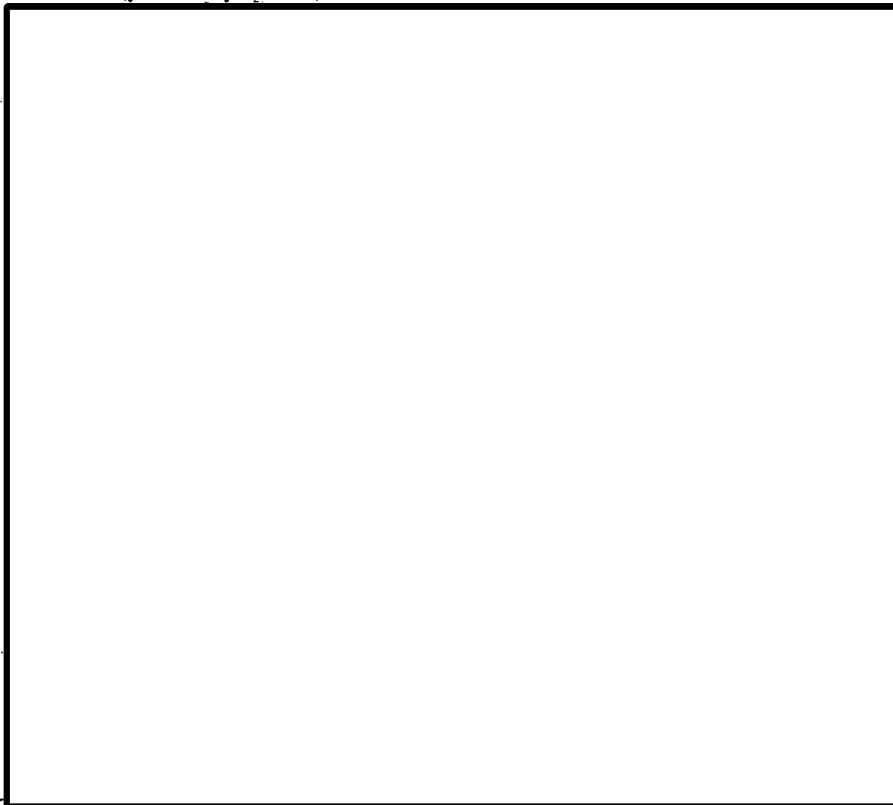
August 4, 2004

Interoffice Memorandum

To: REGIONAL DIRECTORS
DISTRICT DIRECTORS
SERVICE CENTER DIRECTORS
NATIONAL BENEFITS CENTER DIRECTOR

From: William R. Yates *W. R. Yates*
Associate Director of Operations

Re: Required Security Checks



(b)(5)

Appendix, Continued

APPENDIX O
New National Security-Related IBIS Procedures
(May 21, 2004)

Appendix, Continued

--FOR INTERNAL USE ONLY--



U.S. Department of Homeland Security
U. S. Citizenship and Immigration Services

May 21, 2004
HQ FDNS 70/2.1

(b)(5)

425 I Street, NW
Washington, DC 20536

MEMORANDUM FOR REGIONAL DIRECTORS
DISTRICT DIRECTORS
SERVICE CENTER DIRECTORS
NATIONAL BENEFITS CENTER DIRECTOR
ADMINISTRATIVE APPEALS OFFICE DIRECTOR
OFFICE OF INTERNATIONAL AFFAIRS DIRECTOR
ASYLUM DIRECTORS

FROM: William R. Yates /S/
Associate Director of Operations
Citizenship & Immigration Services

SUBJECT: New National Security-Related IBIS Procedures



1
--FOR INTERNAL USE ONLY--

(b)(5)

(b)(5)

Appendix, Continued

APPENDIX P
IBIS Technical Support Guidelines at POEs
(March 2, 2001)

Appendix, Continued

Appendix, Continued

(b)(5)

Appendix, Continued

APPENDIX Q

**Memorandum of Understanding Between the U.S. Customs
Service and the Immigration and Naturalization Service for
Use of the Treasury Enforcement Communications System
(July 9, 1993)**

Appendix, Continued

**Memorandum of Understanding
Between the U.S. Customs Service
and the Immigration and Naturalization Service
for Use of the
Treasury Enforcement Communications System (TECS)**

Dated: **JUL 9 1983**

The U.S. Customs Service (hereinafter Customs Service), as system manager, and the Immigration and Naturalization Service (hereinafter INS) agree to the following Memorandum of Understanding (MOU) provisions for use of the Treasury Enforcement Communications System (hereinafter TECS) and for protection of the sensitive law enforcement information contained therein.

I. Introduction

There is a recognized need to promote the sharing of sensitive law enforcement information between the Federal law enforcement agencies. TECS was designed to support this need by providing multiagency access to a common database of enforcement data supplied by the participating agencies. The Customs Service is both a user of TECS and the system manager. In operating a multiagency enforcement system, it is imperative that the participating agencies observe common procedures to provide adequate security, data integrity, and performance. This MOU is needed to document those procedures.

The Interagency Border Inspection System (IBIS), a multiagency mechanism for providing support to the nation's border security mission, is a further requirement for this MOU. As defined in the IBIS Charter and accompanying procedures, TECS is the designated clearinghouse for the border security information supplied by the IBIS agencies. An MOU between the Customs Service and IBIS requires the Customs Service, as the system manager of TECS, to take the necessary actions to collect, maintain, and protect this information, and to make this information available to the IBIS agencies. In response to this mandate, and as prescribed by the IBIS data sharing procedures, the Customs Service is entering into individual MOU's with the IBIS agencies to document the agreements necessary to effectively share and protect the IBIS information maintained in TECS.

II. Statement of Purpose

This MOU is intended to document the agreement between the Customs Service and INS for the use of TECS, the protection of TECS data, and the adherence to common procedures for the effective sharing of sensitive law enforcement and related information.

Appendix, Continued

- 2 -

III. Agreement

A. Standard Terms for all Agencies Using TECS:

1. TECS is the repository for data from many separate agency sources. This data includes sensitive law enforcement information from Federal law enforcement agencies. Each agency supplying data is considered to be the owner of that data and is responsible for its content and validity. In accepting this responsibility, INS agrees to comply with the TECS Data Standards, Customs Service Directive Number 4320-03 issued July 20, 1990, and, for the transmission of data to TECS, the IBIS Data Exchange Procedures, dated October 3, 1991, and any subsequent editions of those standards.
2. A "TECS user agency" is defined as an agency that has been granted access to TECS. TECS user agency "personnel" are defined as duly authorized employees of, or assigned to, a TECS user agency. "TECS users" are defined as TECS user agency personnel that have been granted individual access to TECS.
3. The Customs Service is responsible for ensuring the integrity of the agency records after they are supplied to TECS and for maintaining safeguards to prevent any unauthorized disclosure of the data. Disclosure of the data will be consistent with the Privacy Act, 5 U.S.C. 552a and other applicable law.
4. INS agrees to comply with the appropriate administrative security provisions related to the use and dissemination of the information in TECS and to consider all information in TECS as "Unclassified, For Official Use Only."
5. The information in TECS is covered by the provisions of the "third agency rule." Pursuant to this principle, INS agrees not to disclose Level 2, 3, or 4 data (i.e., records restricted to agency, group or individual access) to third parties without the prior knowledge and consent of the owning agency. TECS Level 1 records (i.e., those records that are available to all TECS users) may be disclosed to third parties, if otherwise authorized by law, without prior knowledge or consent of the owning agency, only under the following conditions:

the third party must be an employee or detailee of one of the TECS user agencies (this information cannot be further disclosed to parties who are not TECS user agency personnel without approval from the owner of that information);

Appendix, Continued

- 3 -

- the material being disclosed must include labeling indicating that the information is "For Official Use Only";
 - in the case of information on persons, an automated CF-191 Record of Disclosure must be completed to document the disclosure; and,
 - the records are not Immigration and Naturalization (INS) NAILS records which, because they originate from multiple sources, cannot be disclosed without the prior consent of INS.
6. INS agrees to designate a National System Control Officer (SCO) who will be responsible for implementing INS policy for TECS use and coordinating the designation and assignment of TECS access for all applicable employees in INS. Further, the National SCO will serve as the single point of contact within INS for general TECS access and use issues.
 7. Unless exempted by the Commissioner, U.S. Customs Service, all TECS users must have a completed background investigation of one of the following types. Access to TECS functions and data will be limited, depending on the type of background investigation that has been completed, as described below:
 - Type 1: National Crime Information Center (NCIC), TECS, and Credit Checks. Users with this type of background investigation will be limited to basic TECS functions including sign-on, main menu, E-Mail, "Daily News," and entry/query of subject records. These users may only access records owned by the user's agency.
 - Type 2: National Agency Check with Inquiries (NACI) conducted in accordance with the criteria in the Federal Personnel Manual (FPM) Section 763-13. Users with this type of background investigation may have access to any of the functions authorized for the user's agency with the exception of: supervisory approval functions, internal affairs functions, and SCO functions. These users may also access level 1 data from other agencies, but are denied access to higher level data from other agencies.
 - Type 3: Full-field background investigation which has been conducted in accordance with the criteria in the Federal Personnel Manual (FPM) Section 736-13. Users with this type of background investigation may be given access to any of the functions and data authorized for use by INS (as defined in section III. B.).

Appendix, Continued

- 4 -

INS is responsible for ensuring that no INS employee will be granted access to TECS without one of these types of completed background investigations. Twice yearly, the Customs Service will supply the INS National SCO with a computer listing of all INS TECS users and their type of background investigation. The National SCO will be required to sign this listing verifying that completed background investigations, of the specified type, are on file with INS, and return the signed listing to the Customs Service within 30 calendar days. The Customs Service will periodically conduct audits to verify compliance with this requirement.

8. INS agrees to distribute to its TECS users the TECS USER SECURITY HANDBOOK and take steps to ensure that these users abide by the provisions of this document. As part of this responsibility, INS agrees to conduct annual audits of compliance with this handbook, and provide the results of these audits to the Director, Office of Enforcement Systems. The Customs Service will also verify compliance with this requirement, providing INS with reasonable notice of the time and procedures to be followed for this verification.
9. As a member of the IBIS Steering Committee, INS agrees to provide a senior management representative to attend the Steering Committee's meetings. INS will also provide a working level representative for the IBIS Users Group meetings.
10. The automated functions within TECS for adding, updating, reporting, retrieving, or otherwise processing information, are the responsibility of the Customs Service. Any additions, enhancements, or modifications to these automated functions desired by INS will be designed, developed, and implemented by the Customs Service according to requirements and specifications supplied by INS, and in accordance with Customs Service ADP development standards.
11. TECS provides users with access to the NCIC and the National Law Enforcement Telecommunications System (NLETS) through interfaces governed by agreements between the Customs Service and the managers of these systems. INS agrees to abide by these agreements (copies attached) in its use of these interfaces.
12. INS has the option of designating the data it enters into TECS as access Level 1, 2, 3, or 4, and to specify which TECS users may access this data. INS understands and agrees that any data it provides to TECS and designates as Level 1 will be accessible to all TECS users. Further, INS understands and agrees that this Level 1 data may be disseminated to other TECS user agencies, without prior notification to INS, as stipulated in paragraph III.A.5. of this MOU.

Appendix, Continued

- 5 -

B. Terms Specific to INS:

1. INS will have access to TECS data, functions, and other support as follows, subject to the background investigation limitations described in section III. A. 7.

Data Access: INS will have access to the following categories of records in TECS:

- TECS Level 1 records.
- TECS Level 2, 3, and 4 records owned by INS and entered into TECS at the option of INS consistent with paragraph III.B.2. of this MOU.
- TECS Level 3 and 4 records owned by other user agencies, with the owning agencies' authorization. This authorization will be documented by a memorandum from the owning agency to the Director, Office of Enforcement Systems, U.S. Customs Service, explicitly stating the records and access to be granted.
- Primary Query History (PQH) records. These are records of the primary queries made at airports and land borders which can be used to identify individuals or vehicles entering the country.
- I-94 Entry/Exit records. These records are automated versions of the I-94 Entry/Exit form collected by INS from non-immigrant aliens, converted to automated format, and transferred to TECS for inclusion in the TECS database.
- National Crime Information Center (NCIC) records. NCIC records including Federal warrants, stolen vehicles and plates, vehicles used in felonies, other stolen items, and criminal histories, are available through the on-line interface between TECS and NCIC.
- National Law Enforcement Telecommunications System (NLETS) records. Records from the 50 states on criminal histories and motor vehicle registration data are available through the on-line interface between TECS and NLETS.
- Images associated with accessible records.

Access to Functions: INS TECS users will have access to the following sets of functions. The specific subset of these functions authorized for each TECS user will be determined by the INS National SCO. Also, the records displayed or printed under these functions are limited to those authorized under the previous section on data access.

Appendix, Continued

- 6 -

User Profile Record (UPR) Functions: These functions allow TECS users to create, modify, retrieve, and display records describing users on the system. Only designated System Control Officers are authorized to create or modify records on TECS users other than themselves.

Subject Query and Update: These functions allow TECS users to create, modify, and/or delete records on person, business, vehicle, vessel, and aircraft subjects, and to retrieve and display subject records based on the entry of query parameters. The modify and delete functions will only be available for records owned by INS.

"SQ94" I-94 Query: The "SQ94" query allows TECS users to query, retrieve, and display I-94 Entry/Exit records.

"Intell Alert" Query and Update: INS TECS users will have access to functions allowing them to create, modify, delete, and disseminate records providing intelligence related to inspection activities. These are called "Intell Alerts." INS TECS users will also be able to query, retrieve, and display these records.

Record Linking: This function retrieves and displays records that are related to records found during a subject or source document query.

Management Information Reports: These functions allow TECS users to request formatted reports for display or printing. INS TECS users will have access to those reports which pertain to INS operations.

NCIC/NLETS: These functions allow queries to the FBI's NCIC and the criminal history and motor vehicle registration files of 48 states through the NLETS.

Printing: This function allows TECS users to print records or groups of records retrieved through query functions or reports obtained through the management information function.

Primary Query History: This function provides on-line query and display, or off-line reports, of historical information on primary queries performed at airports and land borders.

System Support: This function includes "help," an on-line user guide, electronic mail, access to edit tables, and a variety of other general functions. INS TECS users will have access to all system support functions except those limited to systems management staff and Internal Affairs staff.

Appendix, Continued

- 7 -

Other Support: The Customs Service and INS enjoy a special, close working relationship because of their common mission requirements at the borders. This close relationship is extended to the data processing area where the two agencies work together on developing a maintaining joint, integrated systems supporting the border inspection process. The Customs Service agrees to support this relationship as follows.

Space for IBIS Staff: The Customs Service will provide necessary and reasonable office space, furniture, and supplies at the Customs Service data center in Springfield, Virginia, for INS personnel assigned to the IBIS staff.

Programming Support: The Customs Service will develop, enhance, and maintain TECS mainframe software to support INS inspection activities at IBIS field locations. The Customs Service will also develop, enhance, and maintain specialized software for the INS Local Area Network (LAN) equipment at IBIS locations.

Communications Link: The Customs Service will support a mainframe-to-mainframe communications link between the Customs Service data center and the Department of Justice data center in Rockville, Maryland. The Customs Service will provide the necessary communications and systems support to allow INS users on the INSINC network to sign-on to TECS through this communications link and to allow the transmission of bulk data from INS databases to TECS.

IBIS Field Equipment: The Customs Service and INS share responsibility for the installation of field equipment to support IBIS. This field equipment includes terminals, personal computers, LANs, controllers, cabling, and network connection devices. Areas of responsibility include planning, funding, procurement, site preparation (including cabling), installation, and maintenance. In general, for equipment installed at locations designated in the IBIS Field Installation Master Schedule: the Customs Service will be responsible for connection to the Consolidated Data Network (CDN) and access to TECS; the Customs Service will also be responsible for the local equipment (terminals, personal computers, LANs) intended for use by Customs Service employees; and, INS will be responsible for the local equipment intended for use by INS employees. The specific areas of responsibility for each agency (e.g., procurement, funding, etc.) will be decided on a case-by-case basis.

Appendix, Continued

- 8 -

2. INS agrees to share information at access Level 1 with the TECS community through the on-line entry of records, as appropriate, into the TECS data base. INS has also agreed to provide a large portion of its data to TECS users through a variety of means, as described below.

NAILS: INS agrees to transmit its National Automated Immigration Lookout System (NAILS) records to TECS on a daily basis via an on-line telecommunications link. These records will be stored as Level 1 TECS subject records, owned by INS, and will be made available to primary inspection locations for screening of passengers and conveyances.

NIIS: INS agrees to provide I-94 Entry/Exit records from its Non-Immigrant Information System (NIIS) to Customs for inclusion in TECS as Level 1 records for general secondary query access. These records will be provided by tape on a monthly basis.

ADIT: INS agrees to provide the Alien Documentation Identification Telecommunications (ADIT) Master File and Wanted File to Customs for inclusion in TECS as Level 1 records. Both files will be used to support the screening of arriving passengers at primary inspection locations. The Master File will be used to provide name and date-of-birth data, based on an alien registration number, for use in generating a primary query. The Wanted File will be checked when an alien registration number query is performed to identify possibly fraudulent use of lost/stolen alien registration documents.

3. All data provided to TECS by INS, whether entered on-line or transferred from INS data bases, will be stored as INS-owned records in the TECS data base. Only INS users will be allowed to modify or delete the records owned by INS.

IV. Term of Agreement

1. This MOU will be effective from the date of signature. Except as provided below, it may be terminated by either party upon 30 days advance written notice to the other. This agreement, or any addenda to this agreement, or the termination of this agreement, will not affect any other agreement or addenda entered into between the Customs Service and other parties, or entered into between agencies that have access to TECS unless provided by the specific terms of these agreements and addenda. If this agreement between the Customs Service and INS is terminated and INS is signatory to other agreements between the Customs Service and other entities, those agreements will remain unaffected by the termination of this agreement.

Appendix, Continued

APPENDIX R
INS Use of IBIS (TECS) Workstation with Internet Access
(October 2002)

Appendix, Continued

Immigration and Naturalization Service

and

United States Customs Service



INS use of IBIS (TECS) workstation with Internet Access

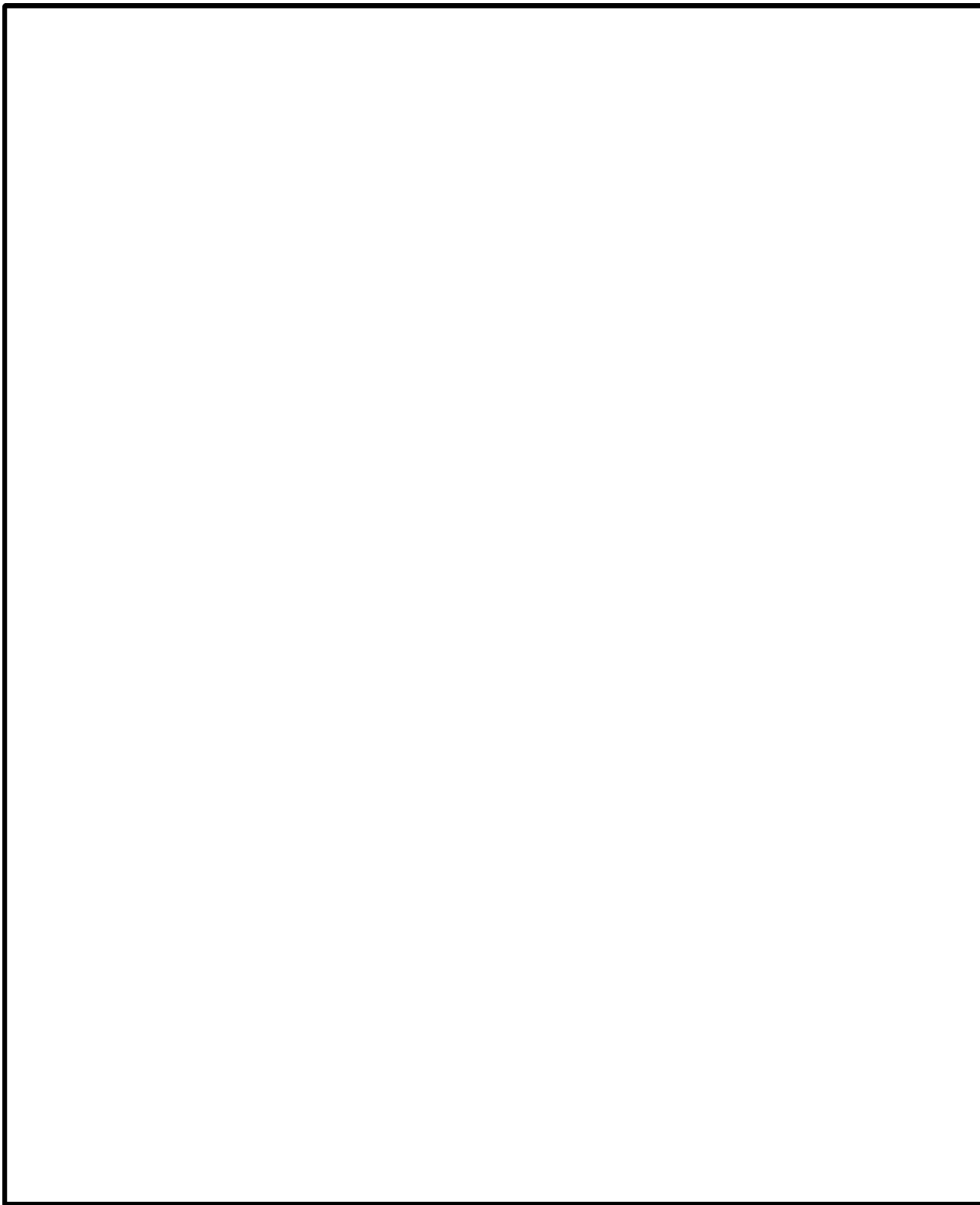
October 2002

**Department of Justice
U.S. Immigration and Naturalization Service**

**Department of the Treasury
United States Customs Service**

Appendix, Continued

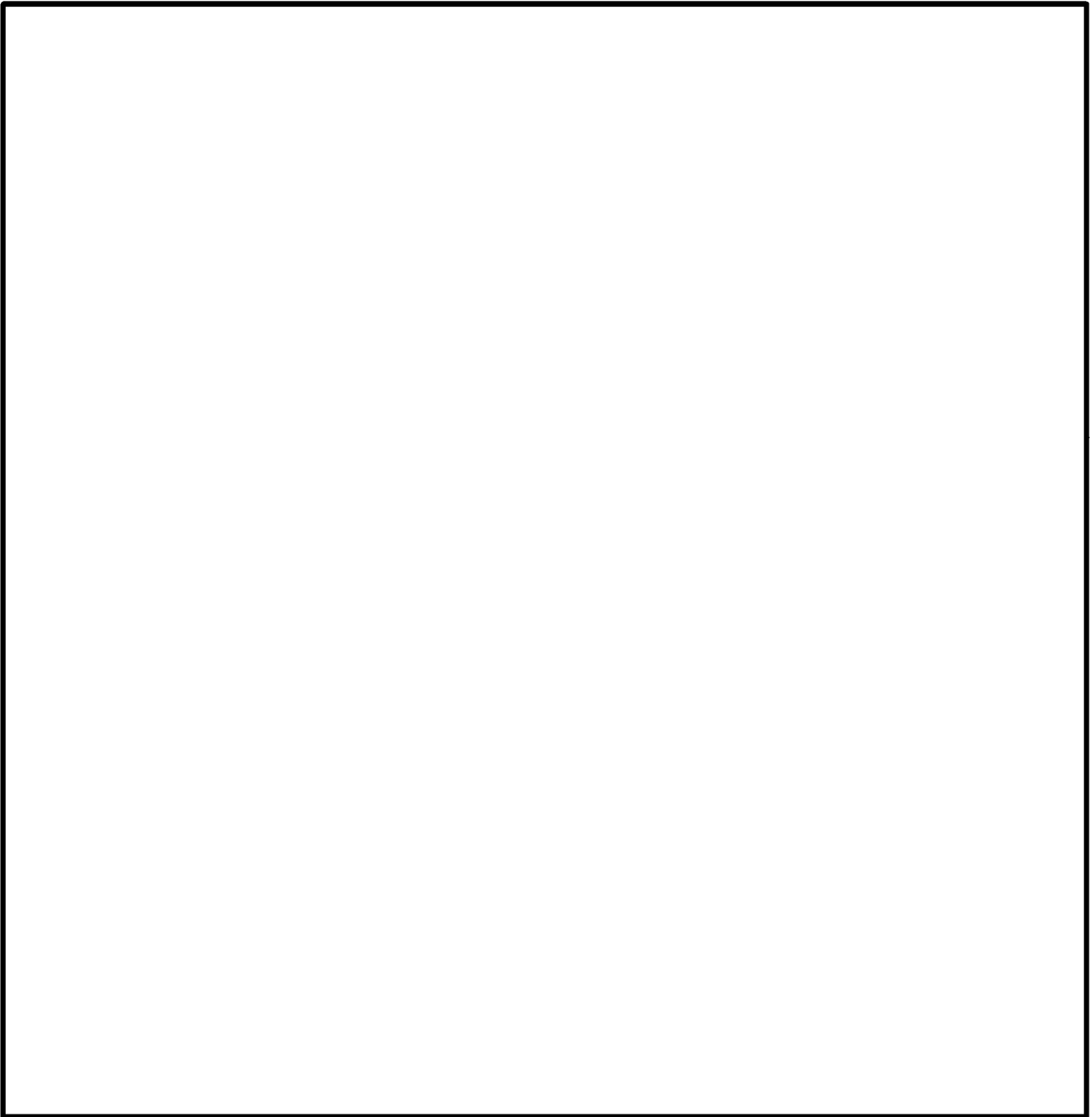
INS use of IBIS (TECS) Workstations with Internet Access



Appendix, Continued

(b)(5)

Appendix, Continued




(b)(5)

Appendix, Continued

SECTION 4 - SIGNATORY AUTHORITY. This ISA is valid for three (3) years after the latest date on either signature below if the technology documented herein does not change or if there are not other intervening requirements for update. At that time it must be reviewed, updated, and revalidated. Either party may terminate this agreement with thirty days-advanced notice or in the event of a security exception that would necessitate an immediate termination of this agreement.

Scott O. Hastings
Associate Commissioner
Office of Information Resources Management
U.S. Immigration and Naturalization Service

 (b)(7)(c)
Executive Director
Infrastructure Services Division
Office of Information and Technology
U.S. Customs Service

(Signature)

(Date)

(Signature)

(Date)

IBIS/Internet Business Impact **Statement**

The Immigration and Naturalization Service (INS) uses the Interagency Border Inspection System (IBIS) to check for lookouts and National Crime Information Center (NCIC) information pertaining to people applying for admission to the US, people applying for benefits from the INS, and to conduct research on investigative and intelligence cases. INS currently accesses IBIS from over 400 INS sites utilizing approximately 8,000 workstations. Many INS IBIS users also need to use the Internet as part of their job duties. This includes accessing other US agency websites for processing requests and performing online research. To comply with previous INS/USCS security policy, INS offices are currently prohibited from having internet connectivity on IBIS-connected workstations. Consequently, the INS has requested that Internet access from an IBIS workstation be granted for increased efficiency and cost reduction purposes and to be used as a standard tool for research.

Many INS IBIS users also need to use the Internet as part of their job duties. For instance Adjudicators must access Department of Labor and Department of State web sites in order to process benefit petitions in addition to running an IBIS query. Inspectors, Investigators and Intelligence officers often need to research businesses or verify information while working cases. All INS employees use the EmployeeExpress.Gov web site to monitor their leave and earning statements and Thrift Savings Plans as well as make changes to addresses and W4 information. DOJ and OMB web sites also contain important information that must be available to INS employees.

Currently in order to comply with the USCS policy, offices have had to be creative in their workstation configurations. Some offices set up banks of workstations that have access to either IBIS or the Internet and staff must rotate to these workstations to check either IBIS or the Internet. This interferes with the efficient flow of work and costs additional time to process cases. Some offices have set up two workstations on officers' desks and the officer's switch between workstations to do IBIS or Internet checks. In addition to the lost productivity, INS is incurring additional costs by having separate workstations available for IBIS and Internet use. In some cases older excess equipment has been set up, but in some cases new workstations have been purchased. With either the older equipment or new equipment additional staff support is required to set up and maintain these workstations.

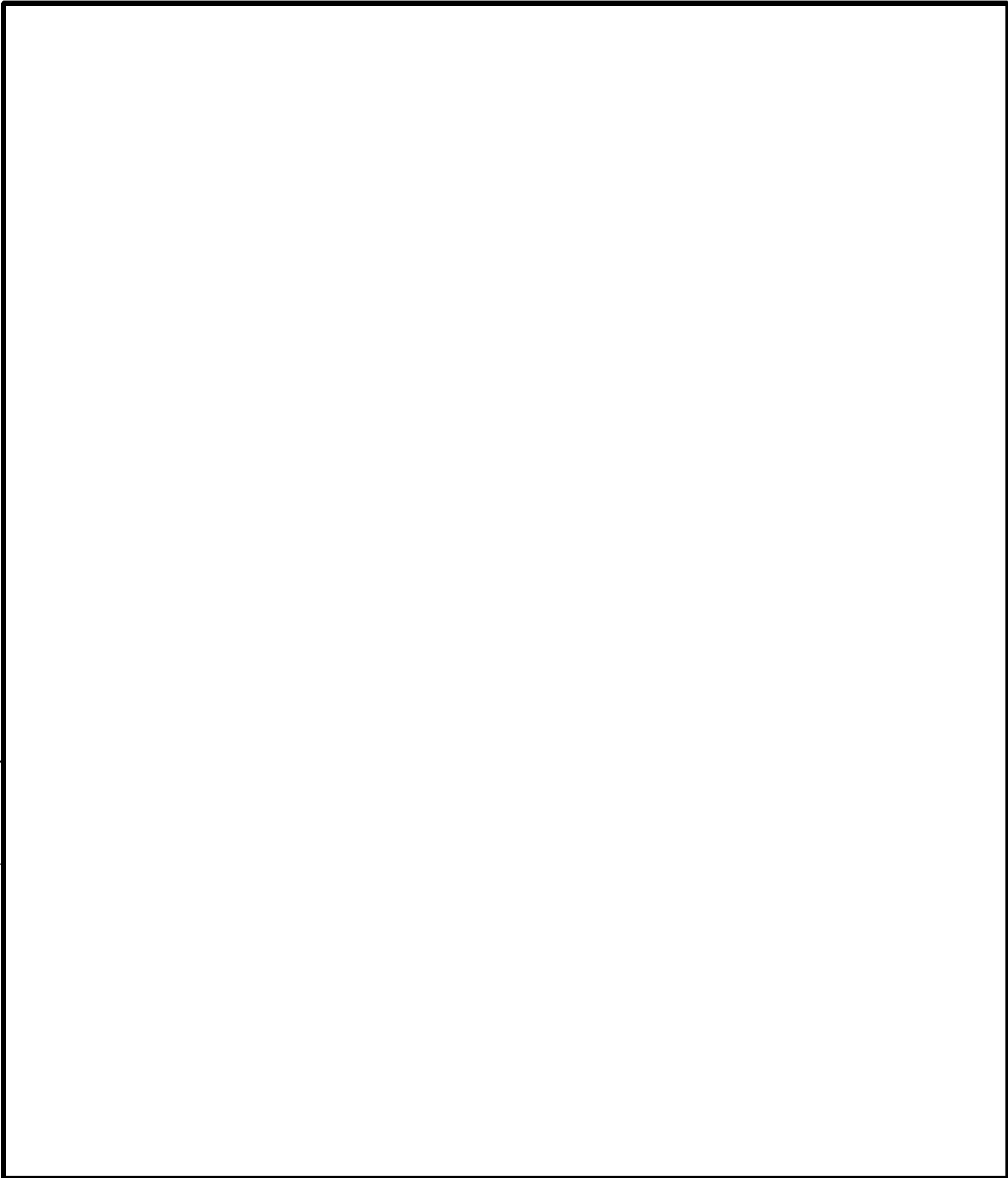
Appendix, Continued

APPENDIX S
Codes for TECS User Agencies and Sub Agencies
(February 16, 2006)

(b)(5) **Appendix, Continued**

(b)(7)(e) **Codes for TECS User Agencies and Sub Agencies**

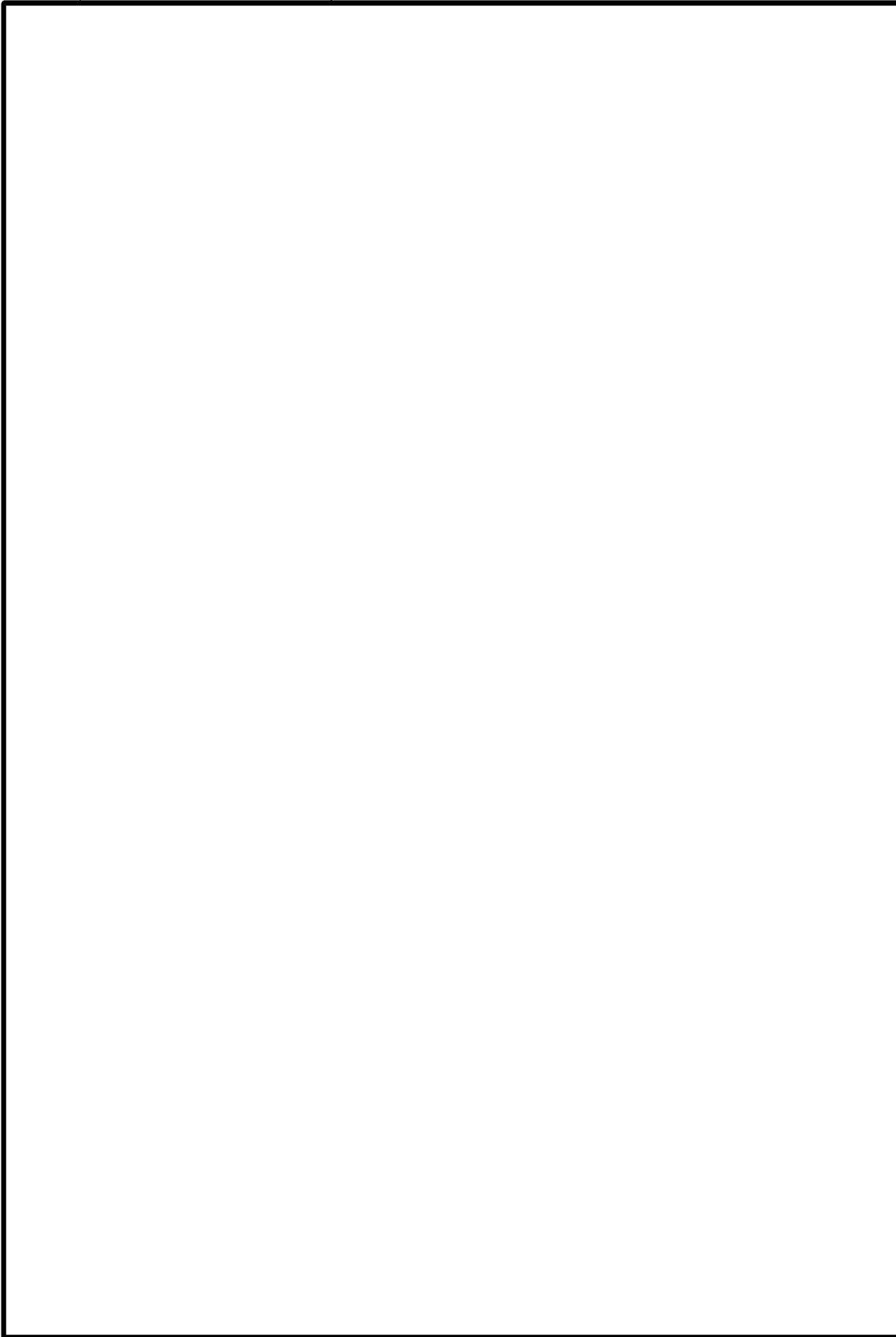
February 16, 2006



(b)(5)

(b)(7)(e)

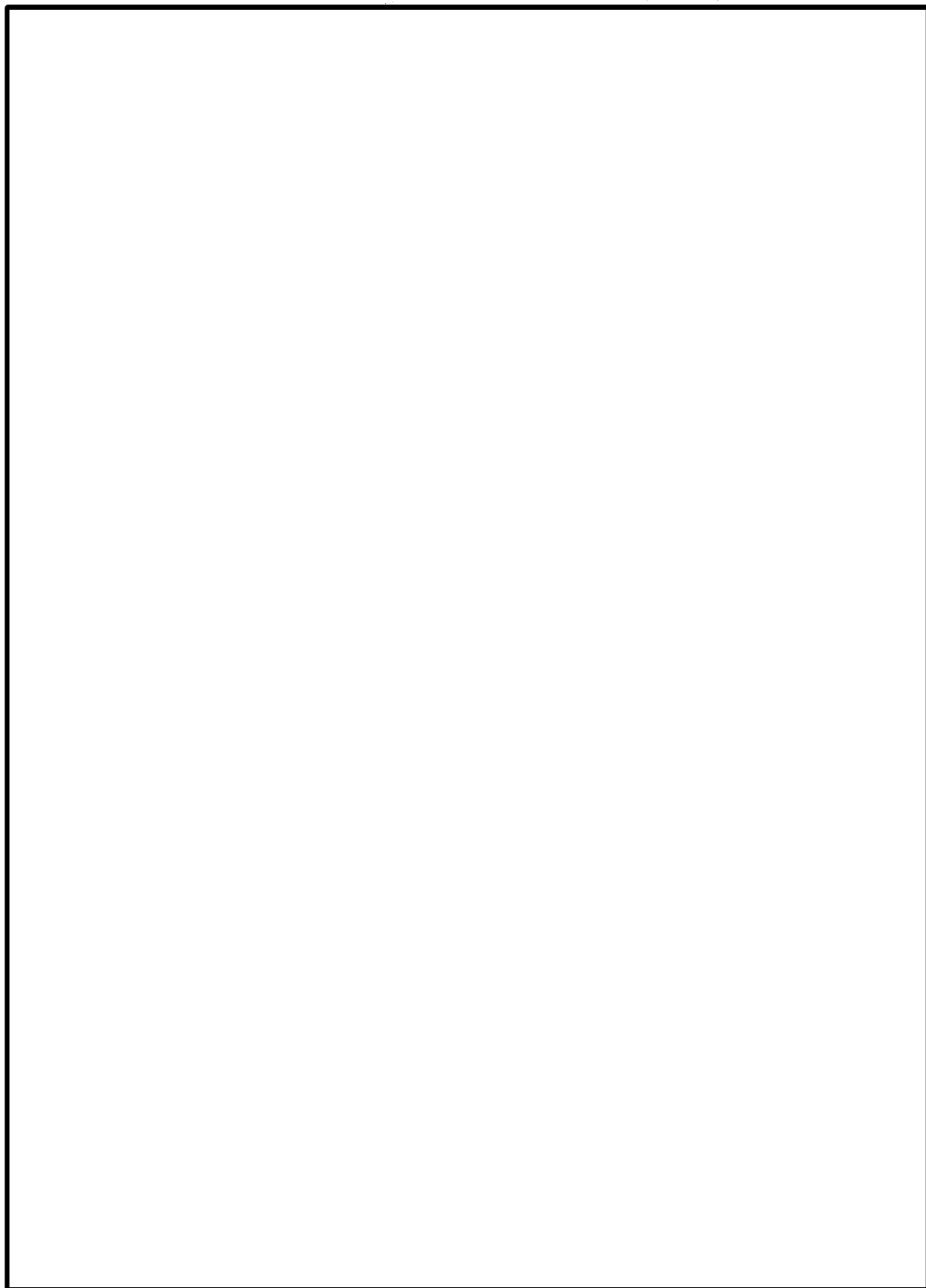
Appendix, Continued



(b)(7)(e)

(b)(5)

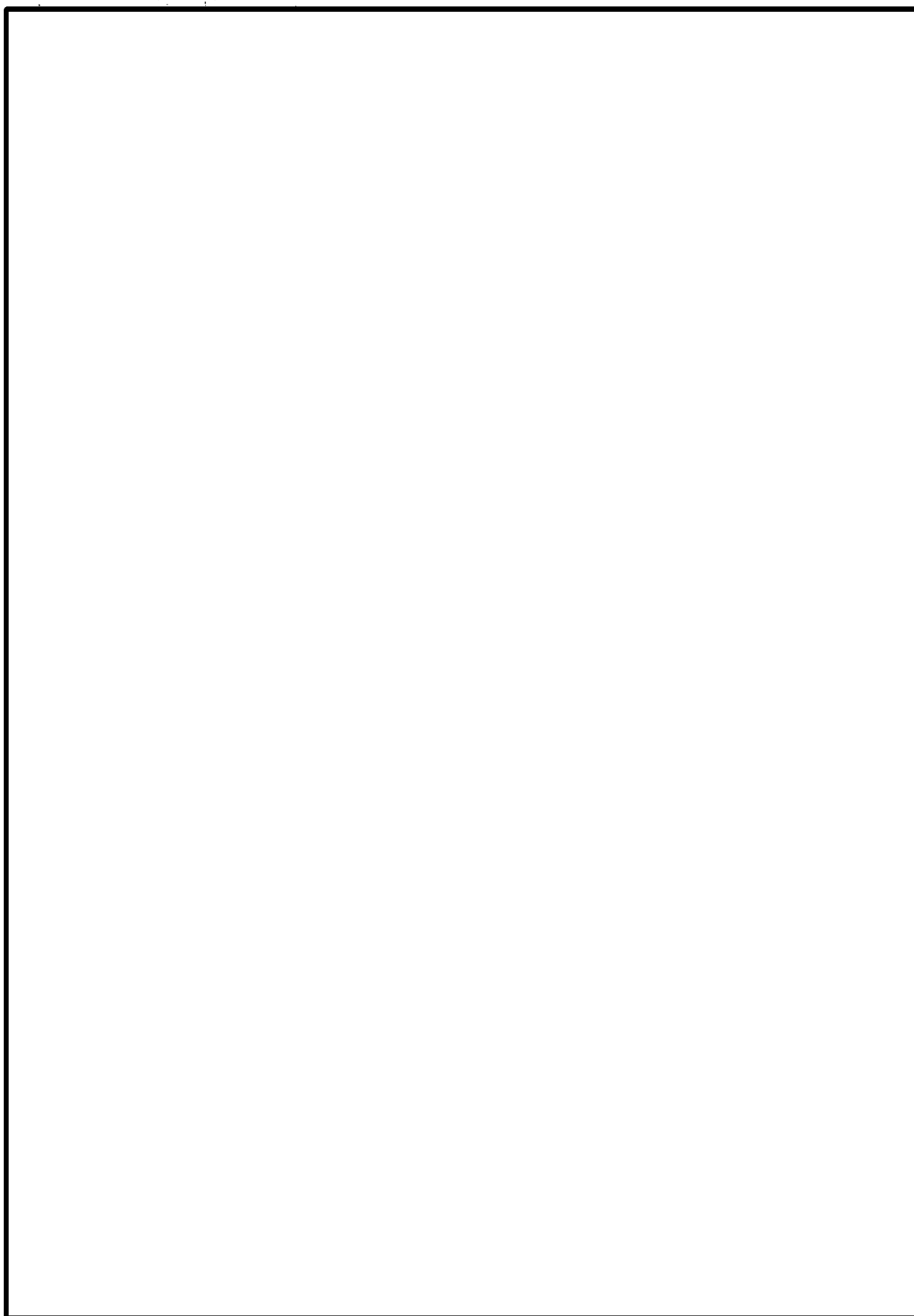
Appendix, Continued



(b)(5)

(b)(7)(e)

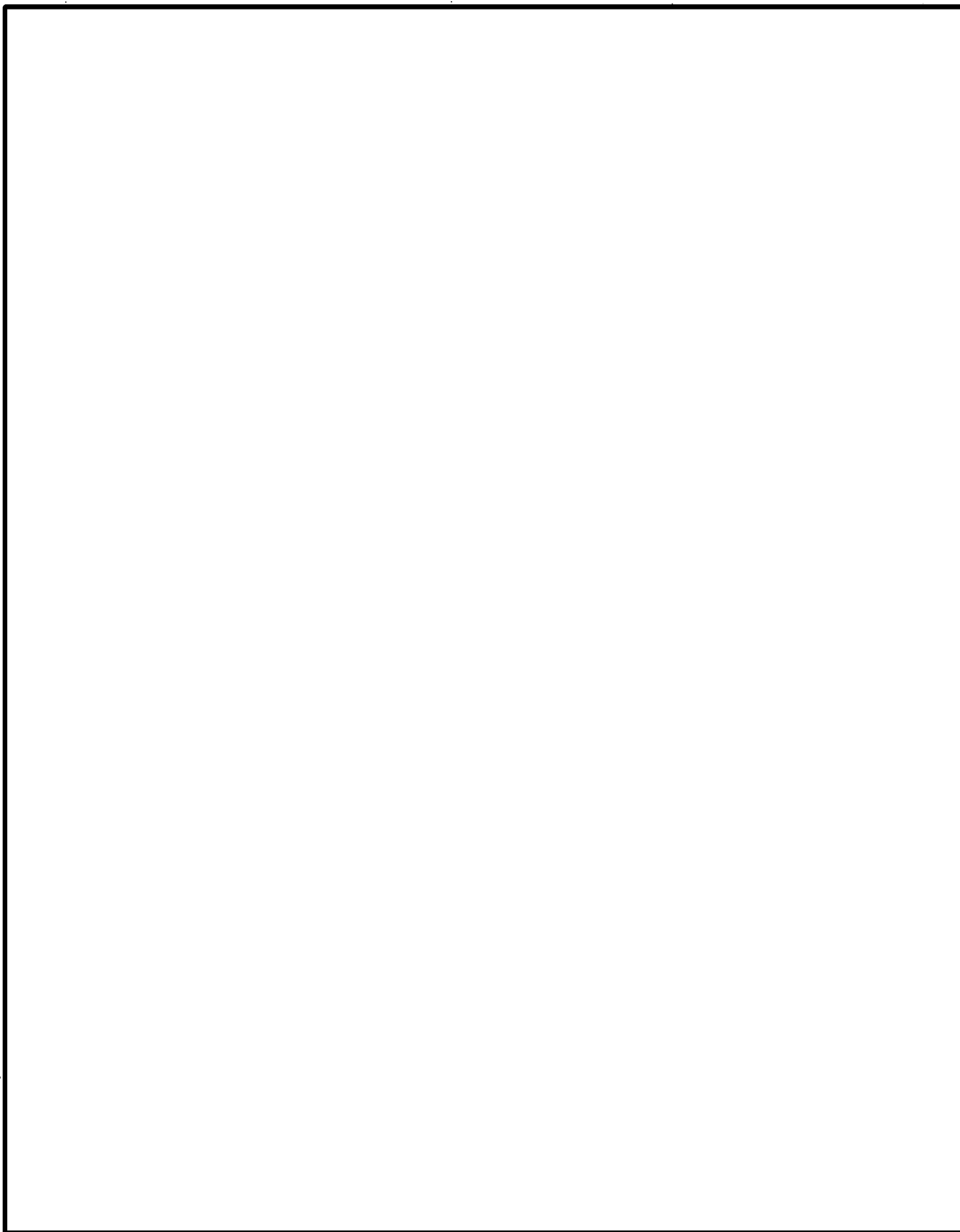
Appendix, Continued



(b)(5)

(b)(7)(e)

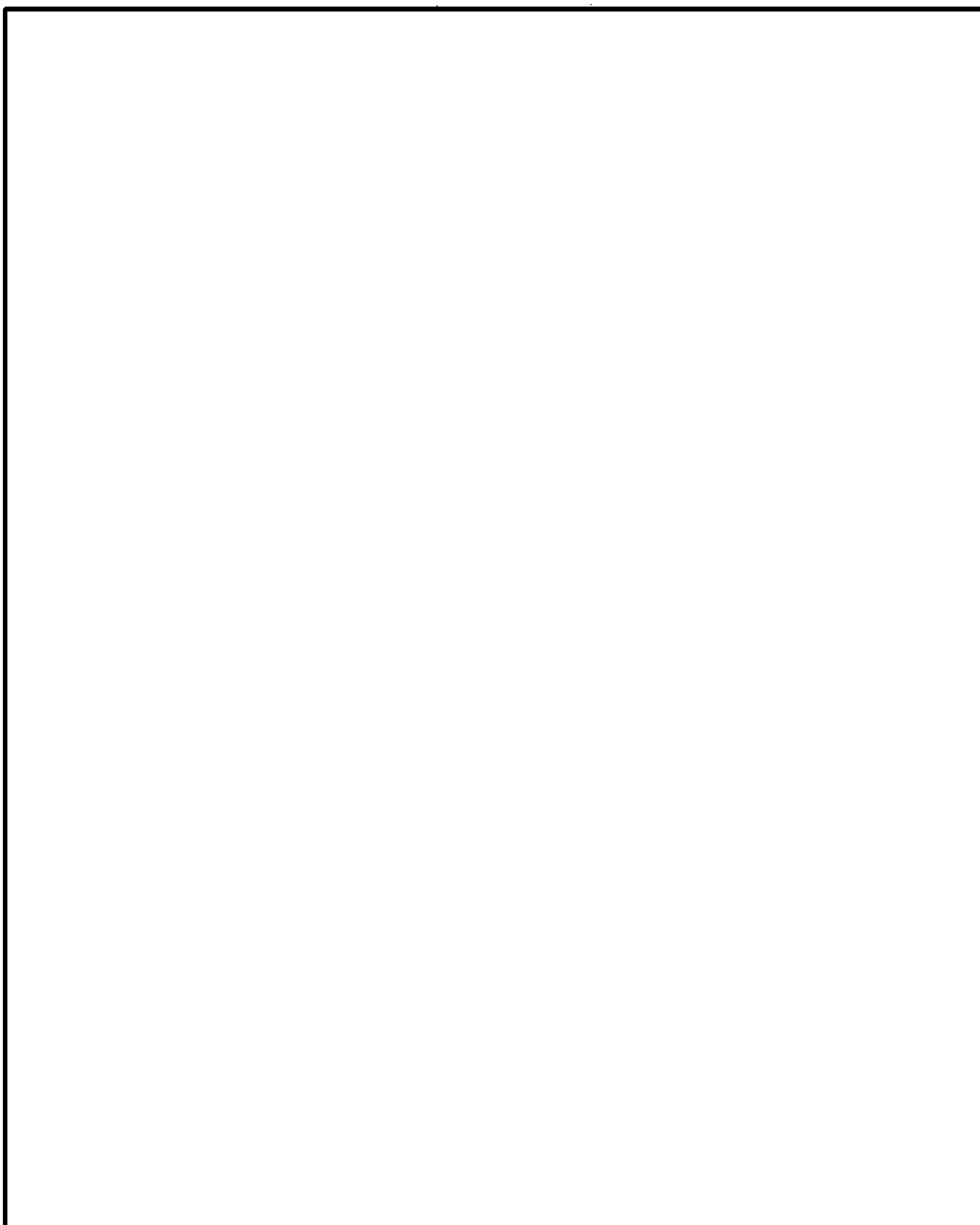
Appendix, Continued



(b)(7)(e)

(b)(5)

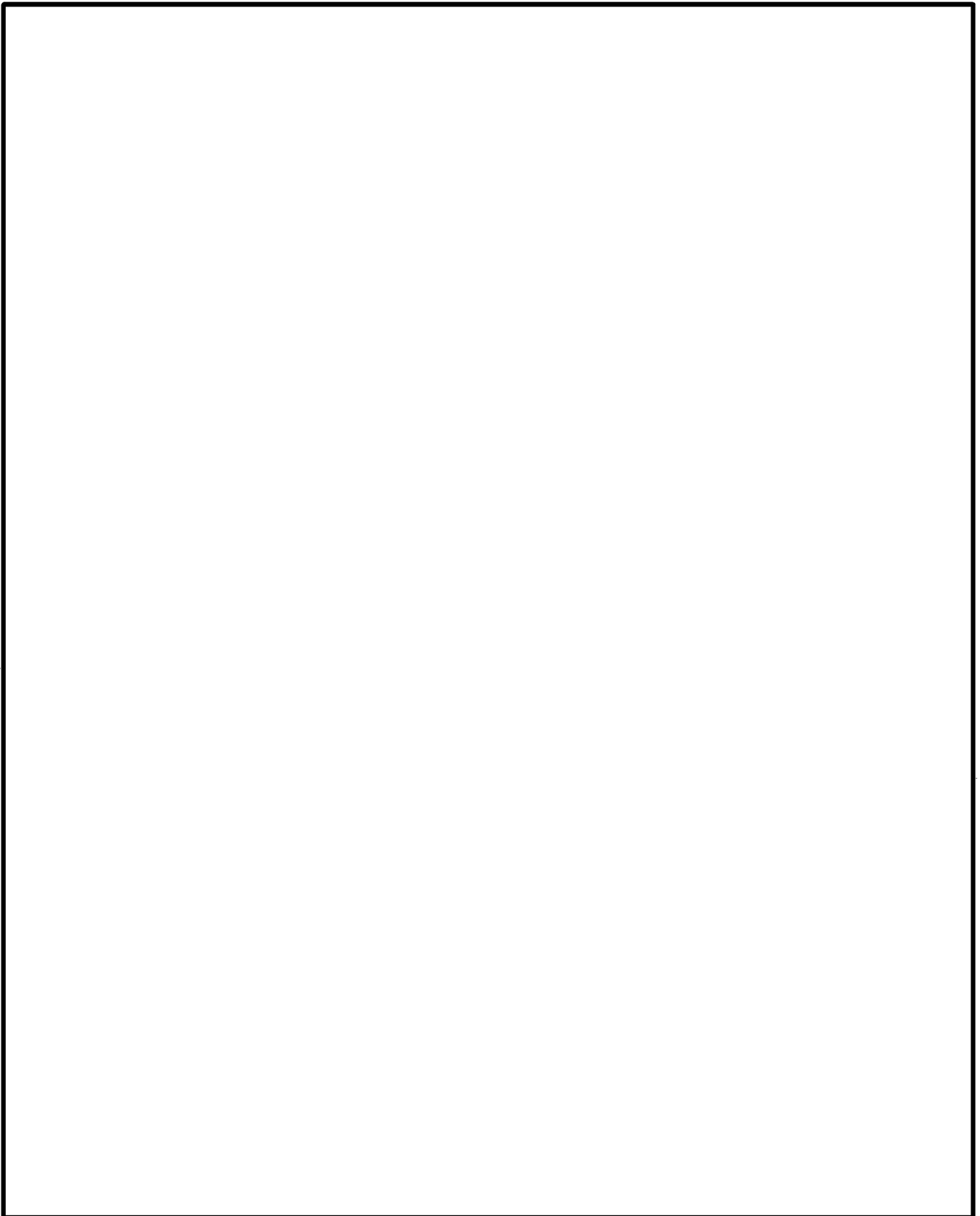
Appendix, Continued



(b)(5)

(b)(7)(e)

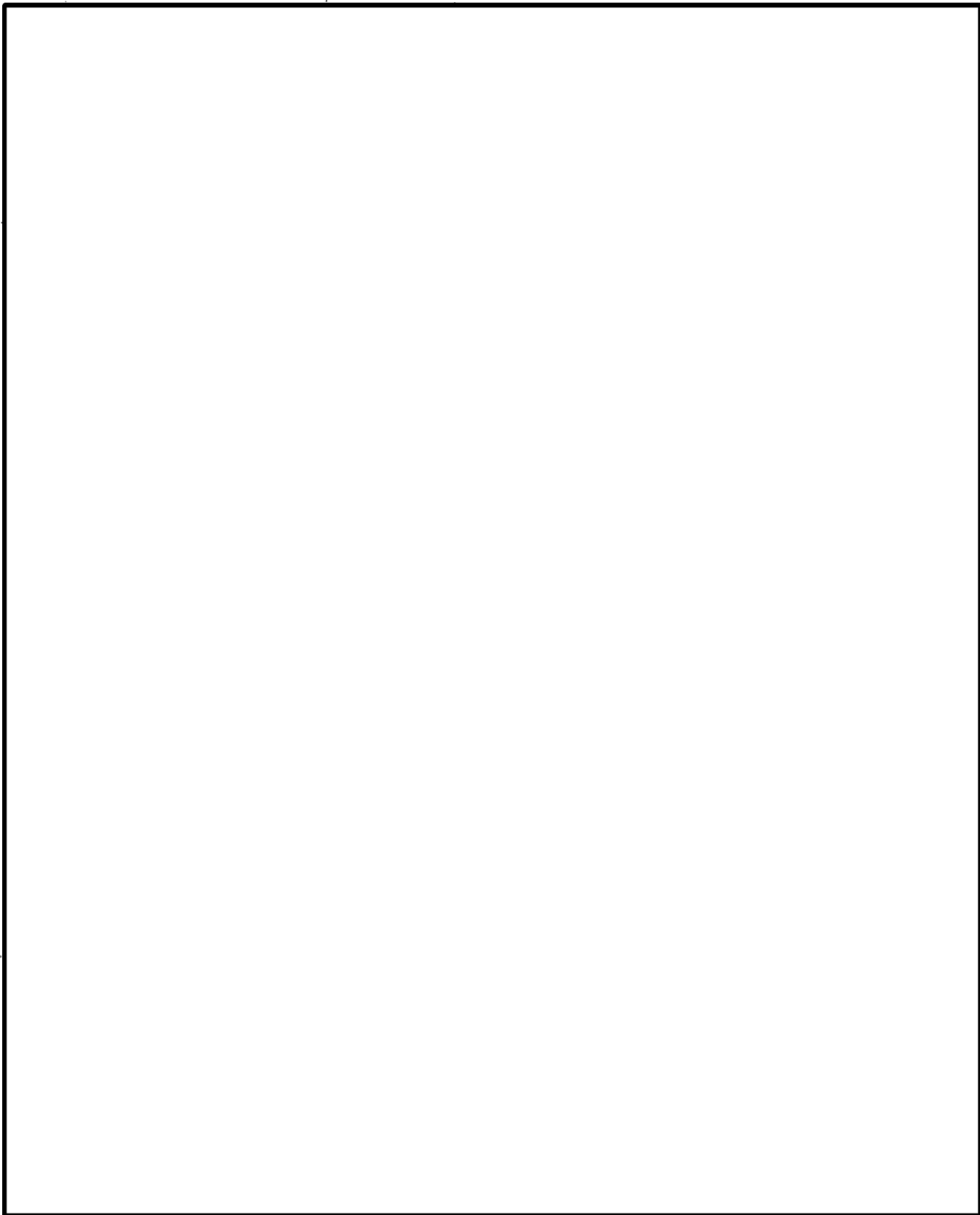
Appendix, Continued



(b)(7)(e)

(b)(5)

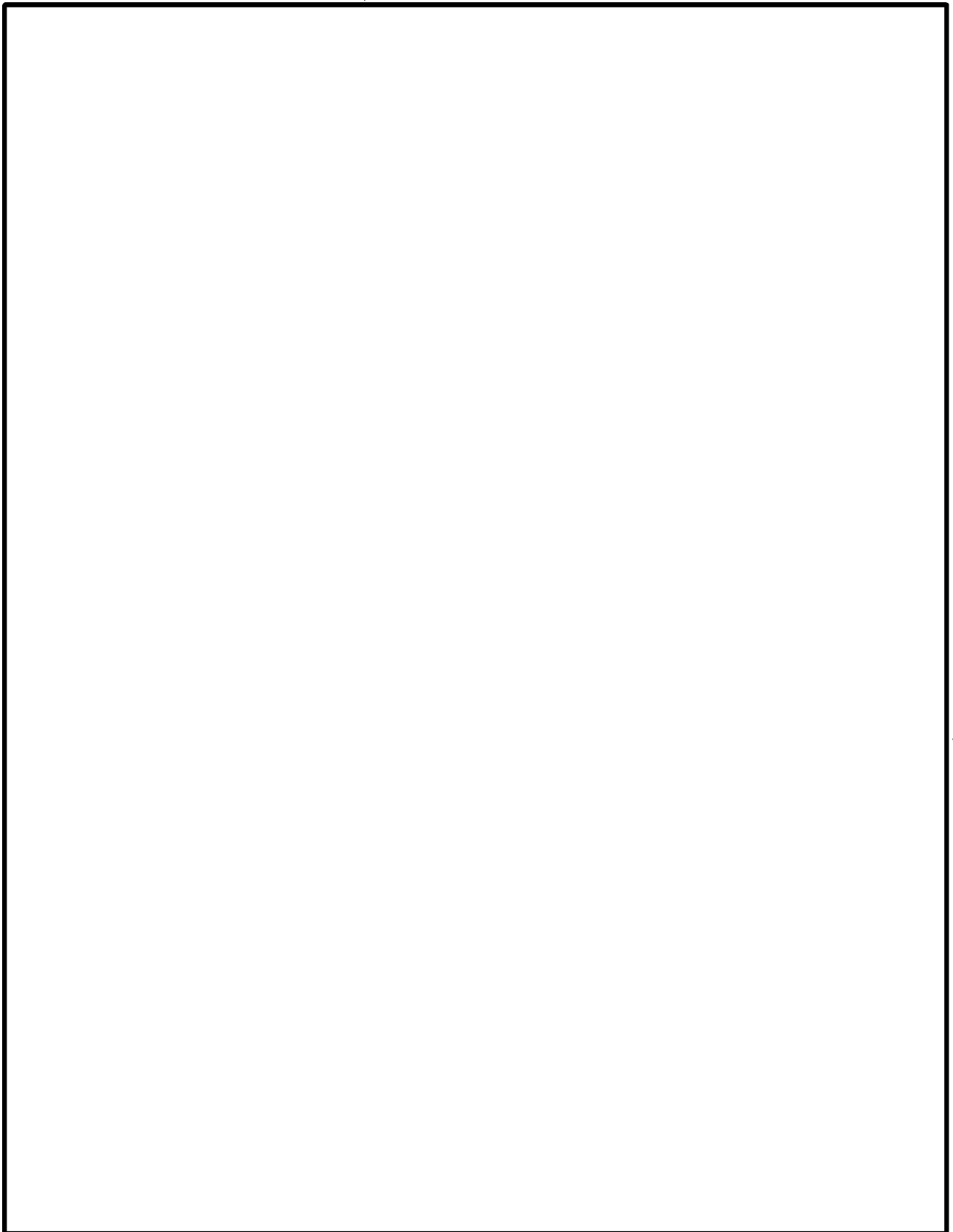
Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(7)(e)

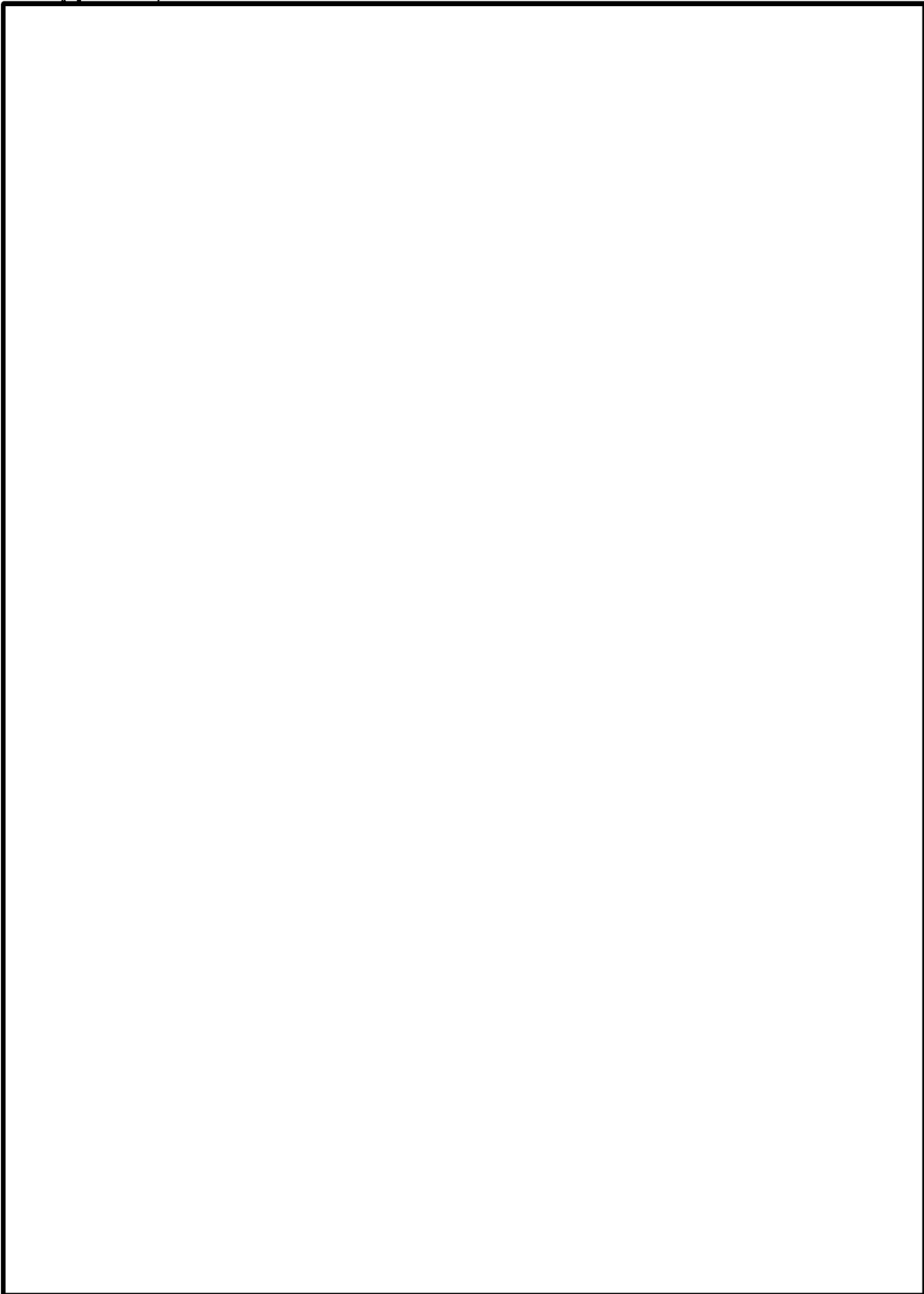
(b)(5)

Appendix, Continued

(b)(5)

(b)(7)(e)

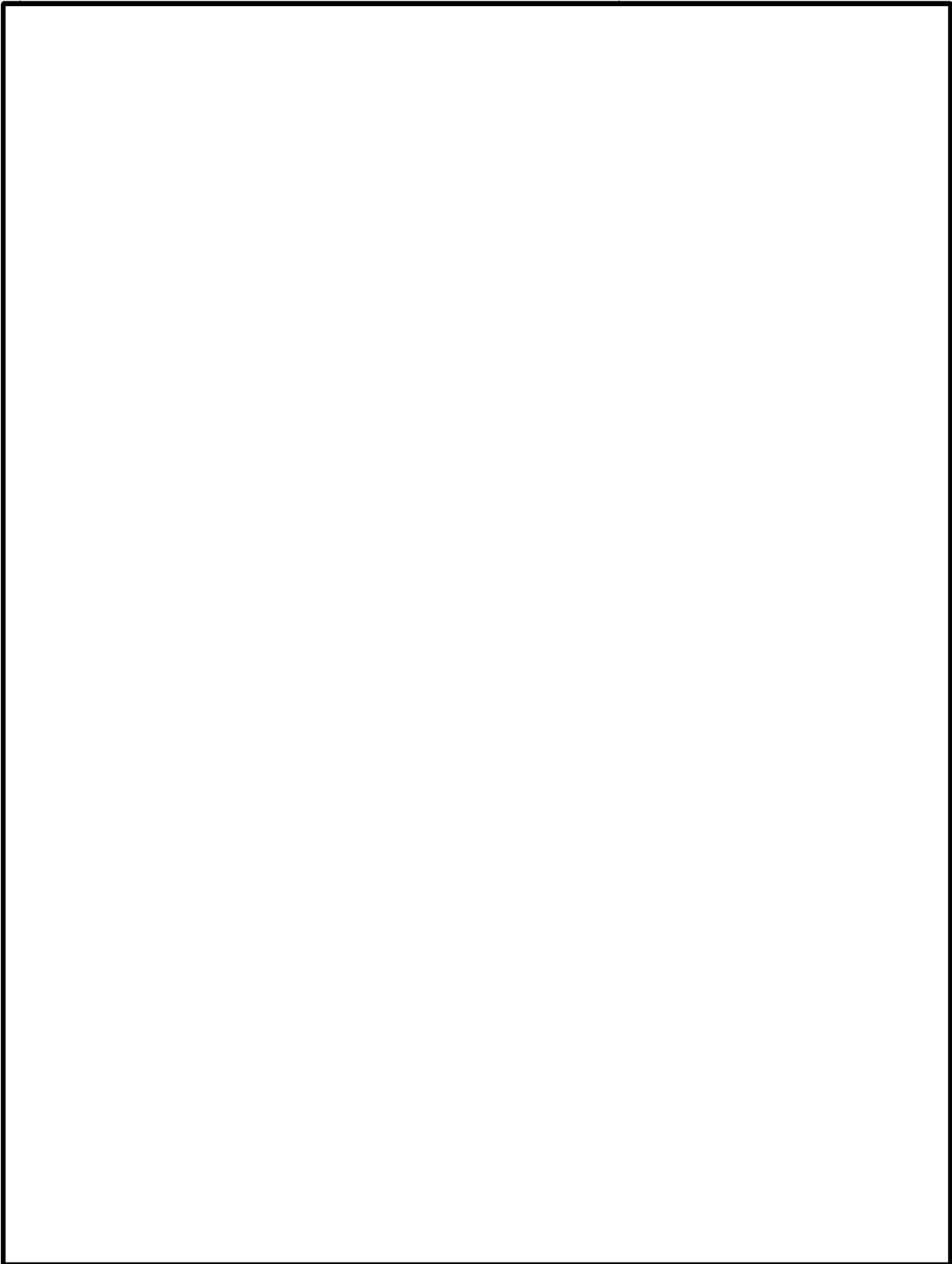
Appendix, Continued



(b)(7)(e)

(b)(5)

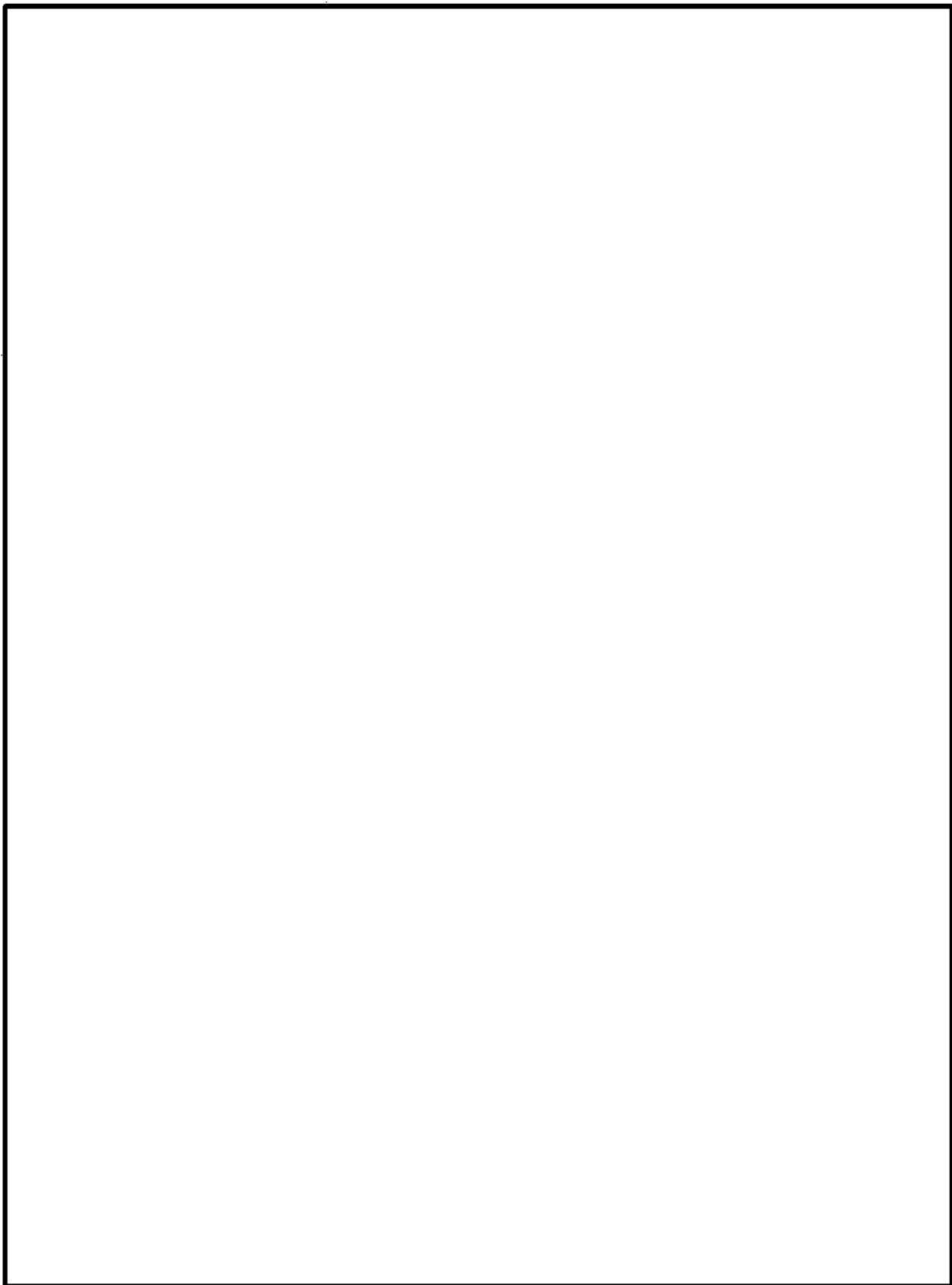
Appendix, Continued



(b)(5)

(b)(7)(e)

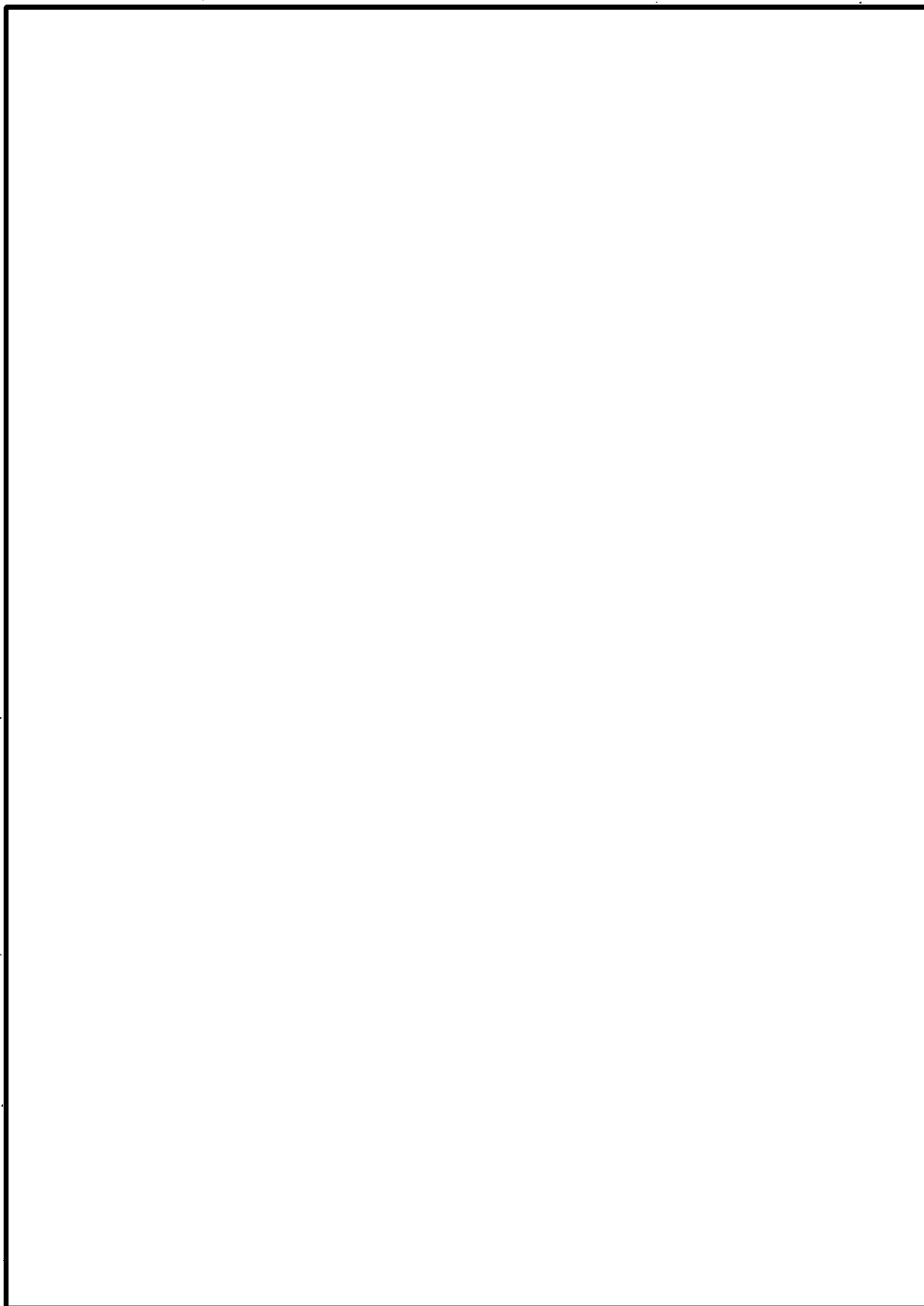
Appendix, Continued



(b)(7)(e)

(b)(5)

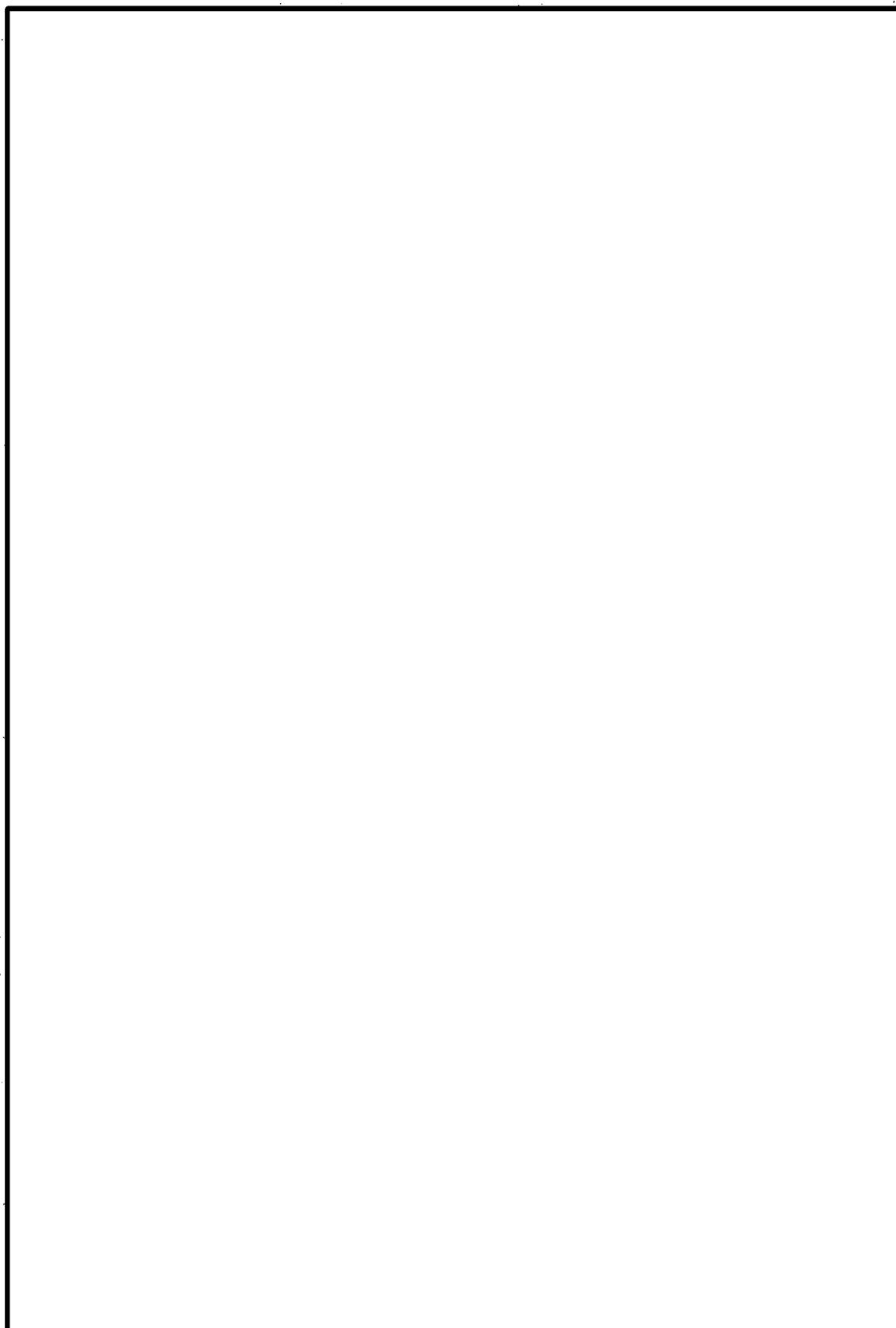
Appendix, Continued



(b)(5)

(b)(7)(e)

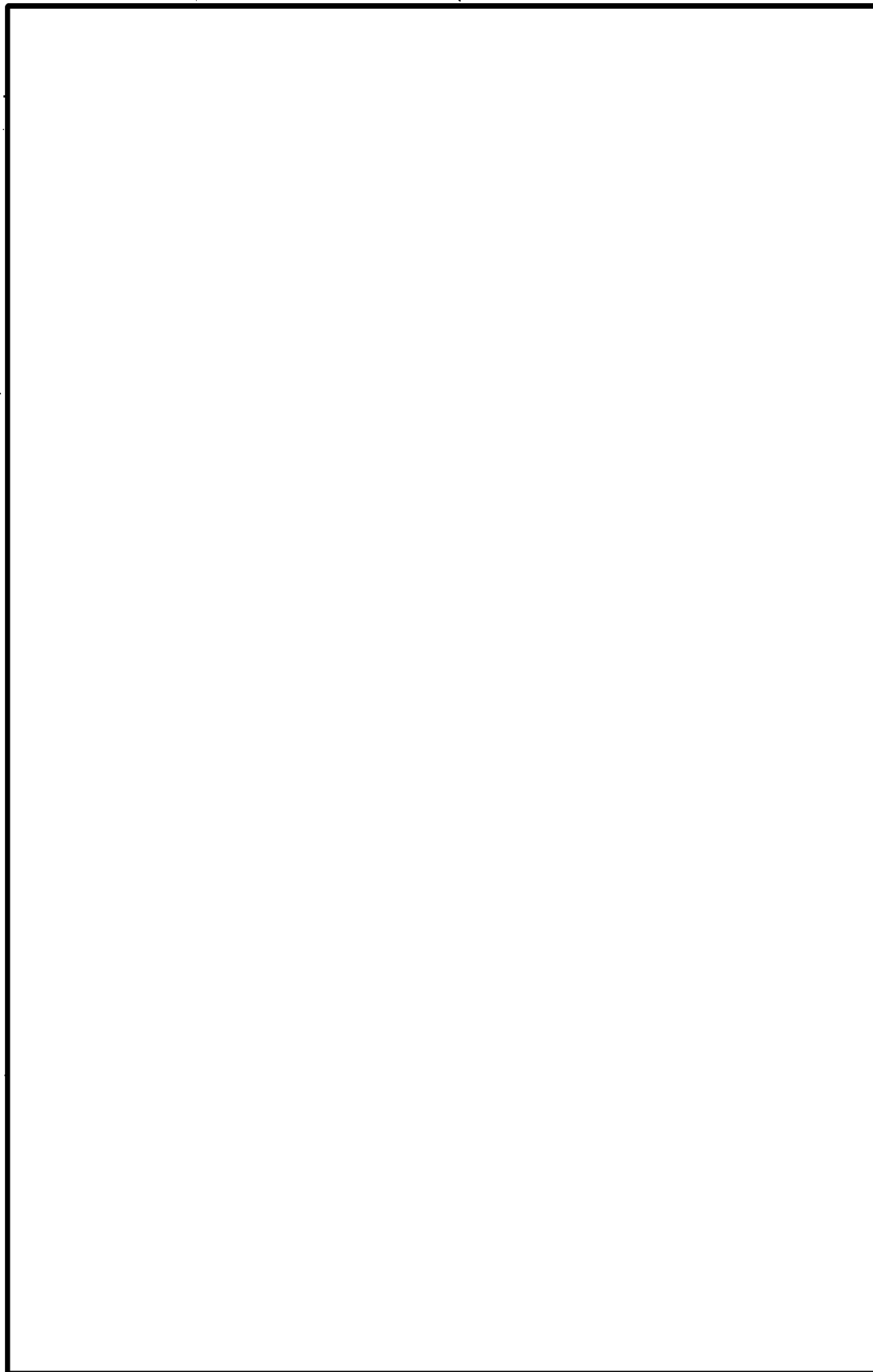
Appendix, Continued



(b)(5)

(b)(7)(e)

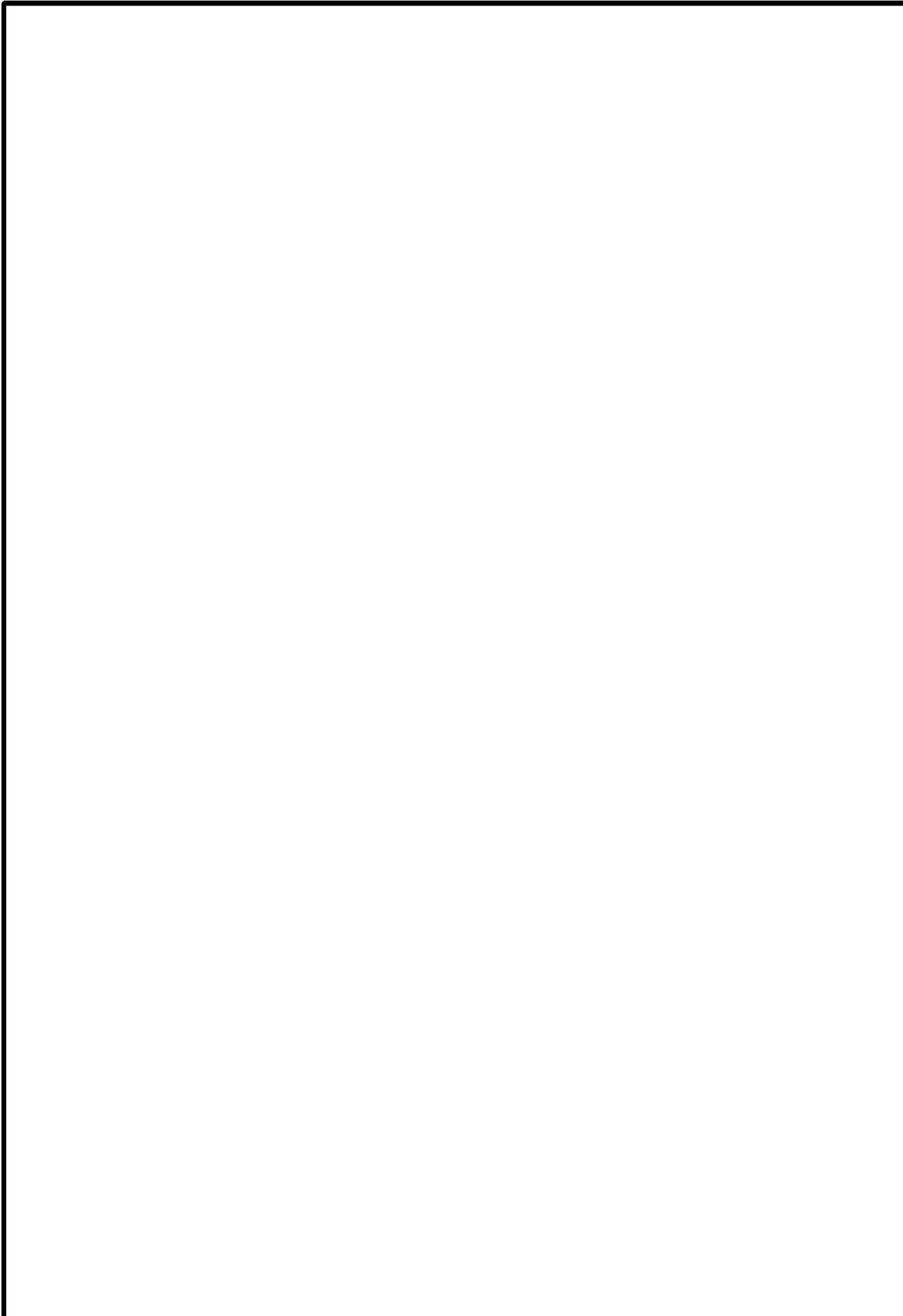
Appendix, Continued



(b)(7)(e)

(b)(5)

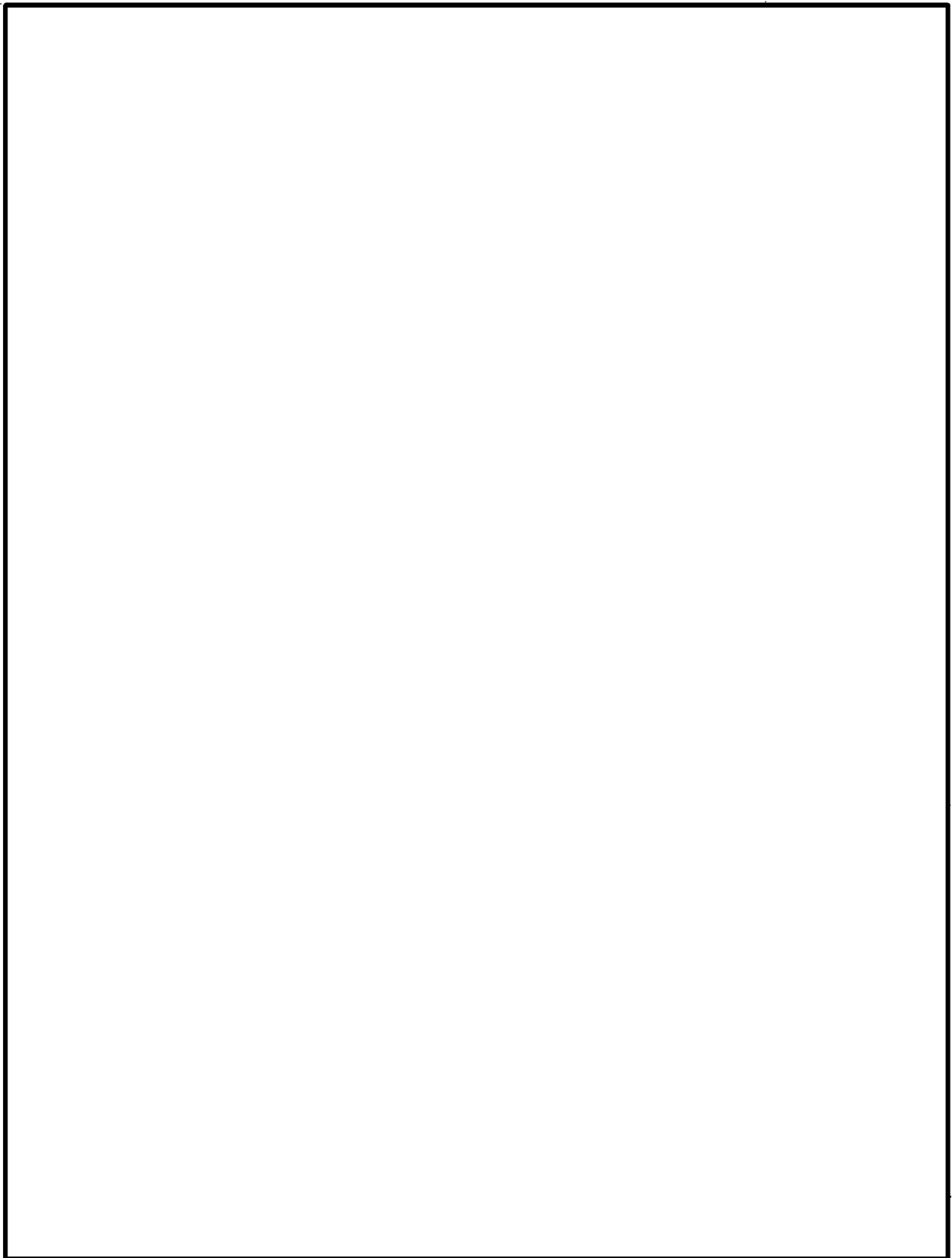
Appendix, Continued



(b)(5)

(b)(7)(e)

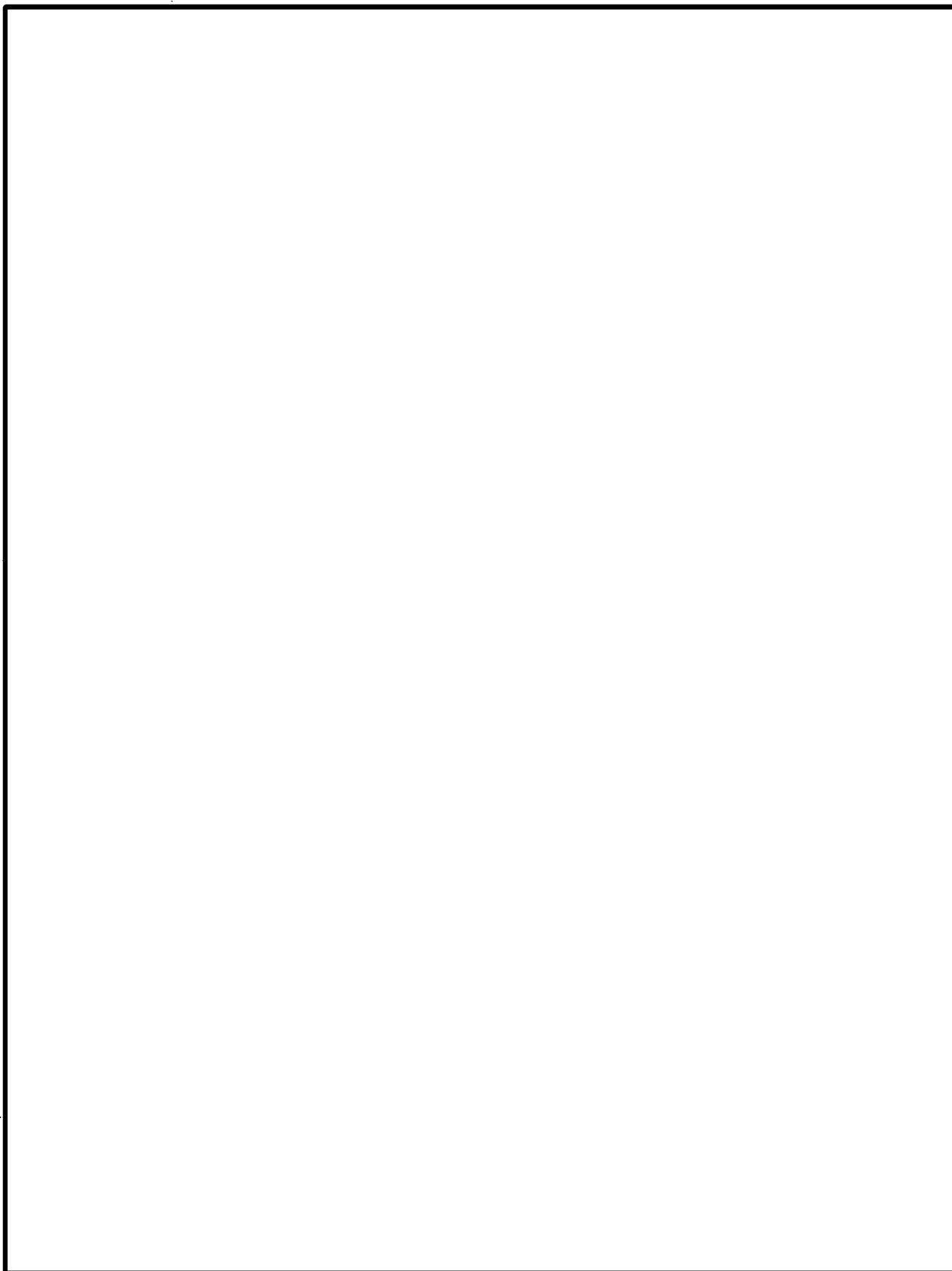
Appendix, Continued



(b)(7)(e)

(b)(5)

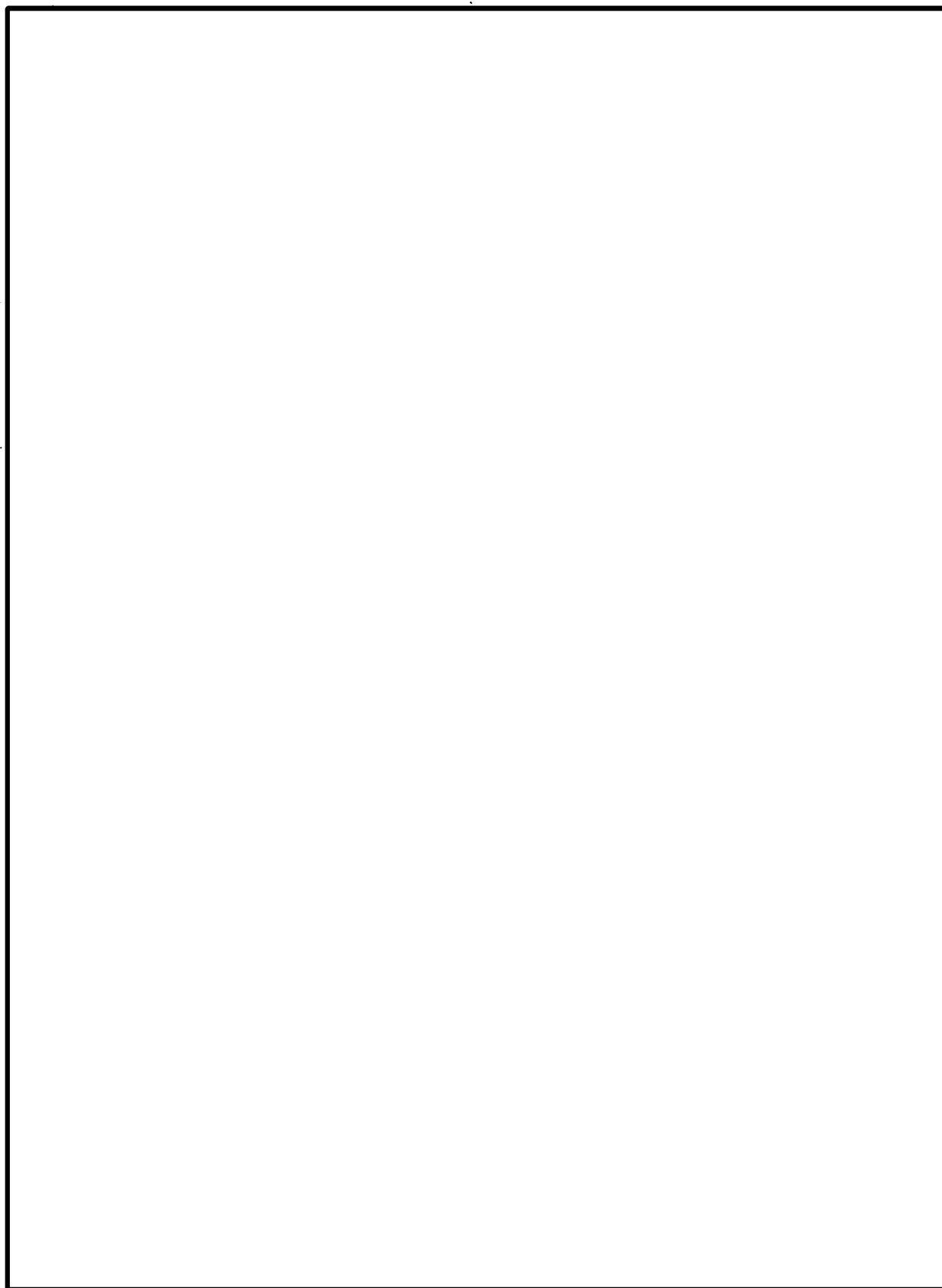
Appendix, Continued



(b)(5)

(b)(7)(e)

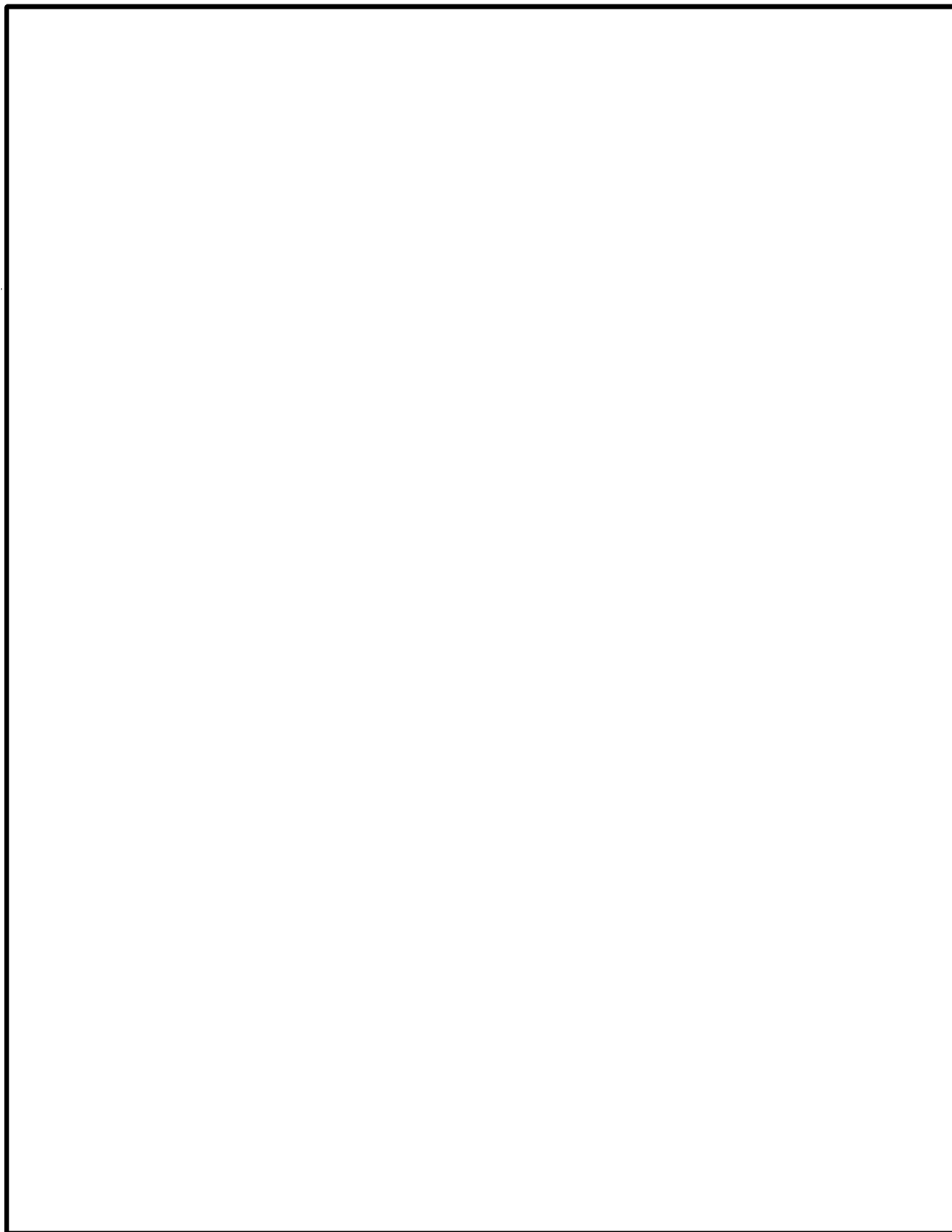
Appendix, Continued



(b)(7)(e)

(b)(5)

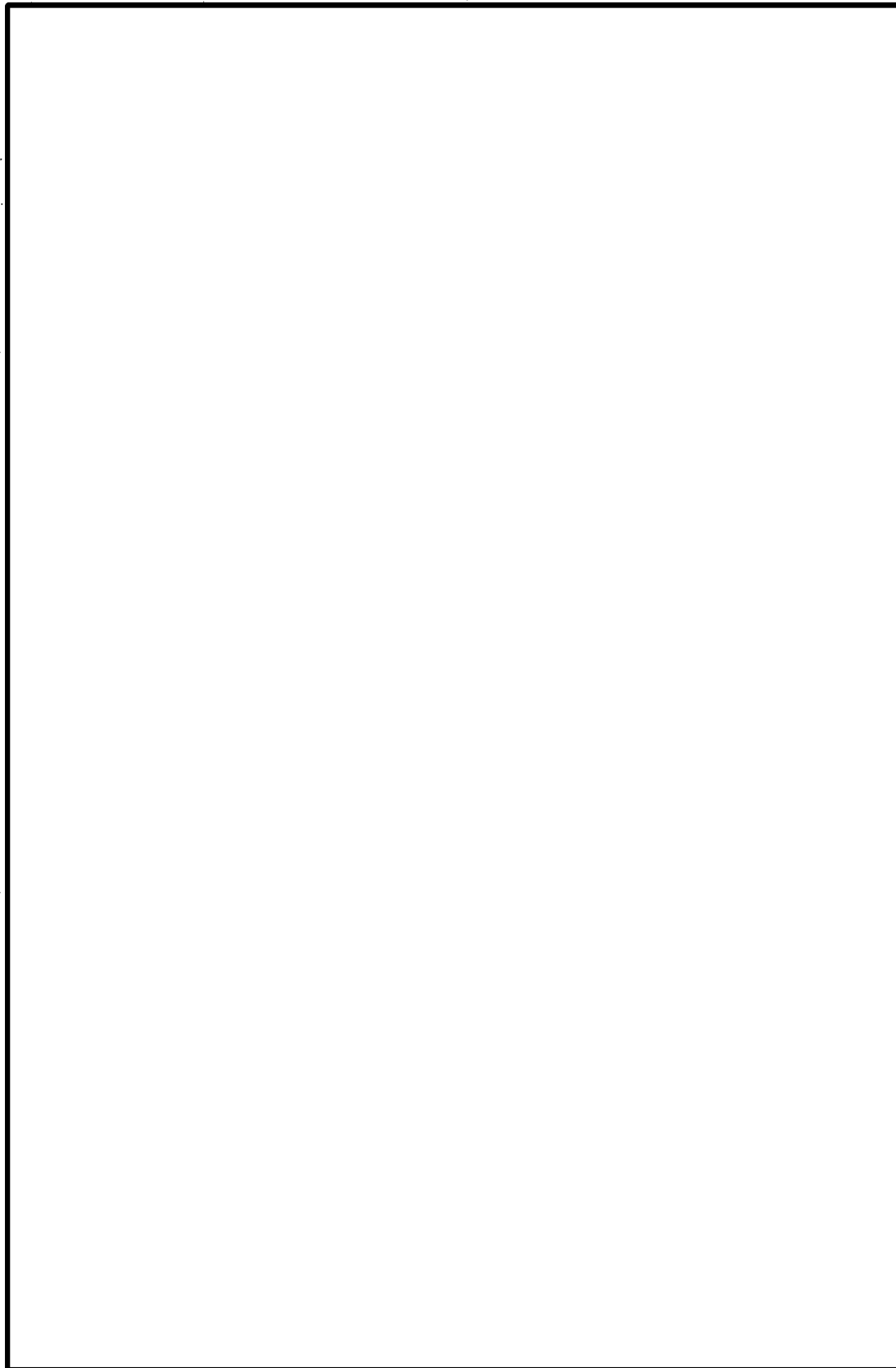
Appendix, Continued



(b)(5)

(b)(7)(e)

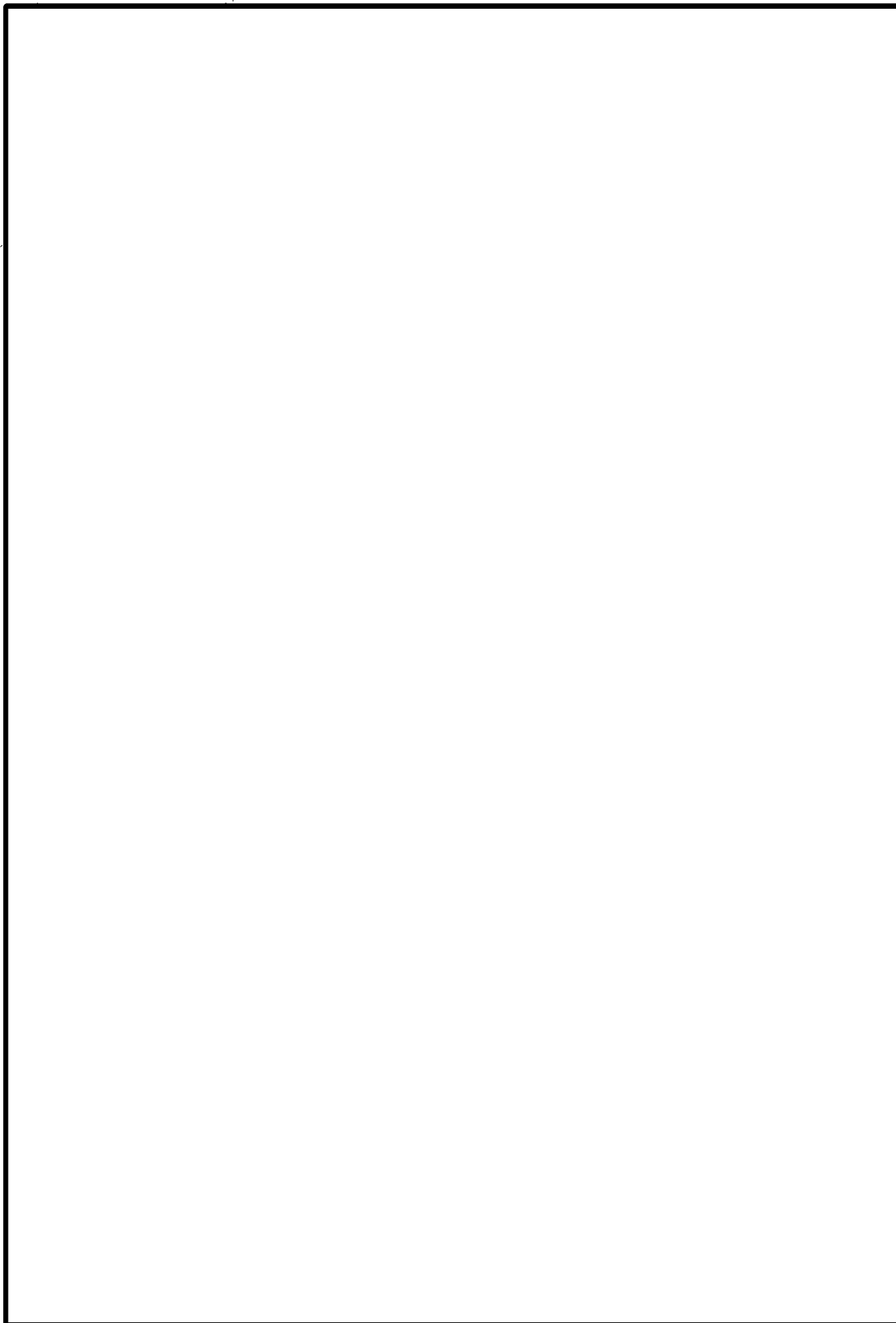
Appendix, Continued



(b)(7)(e)

(b)(5)

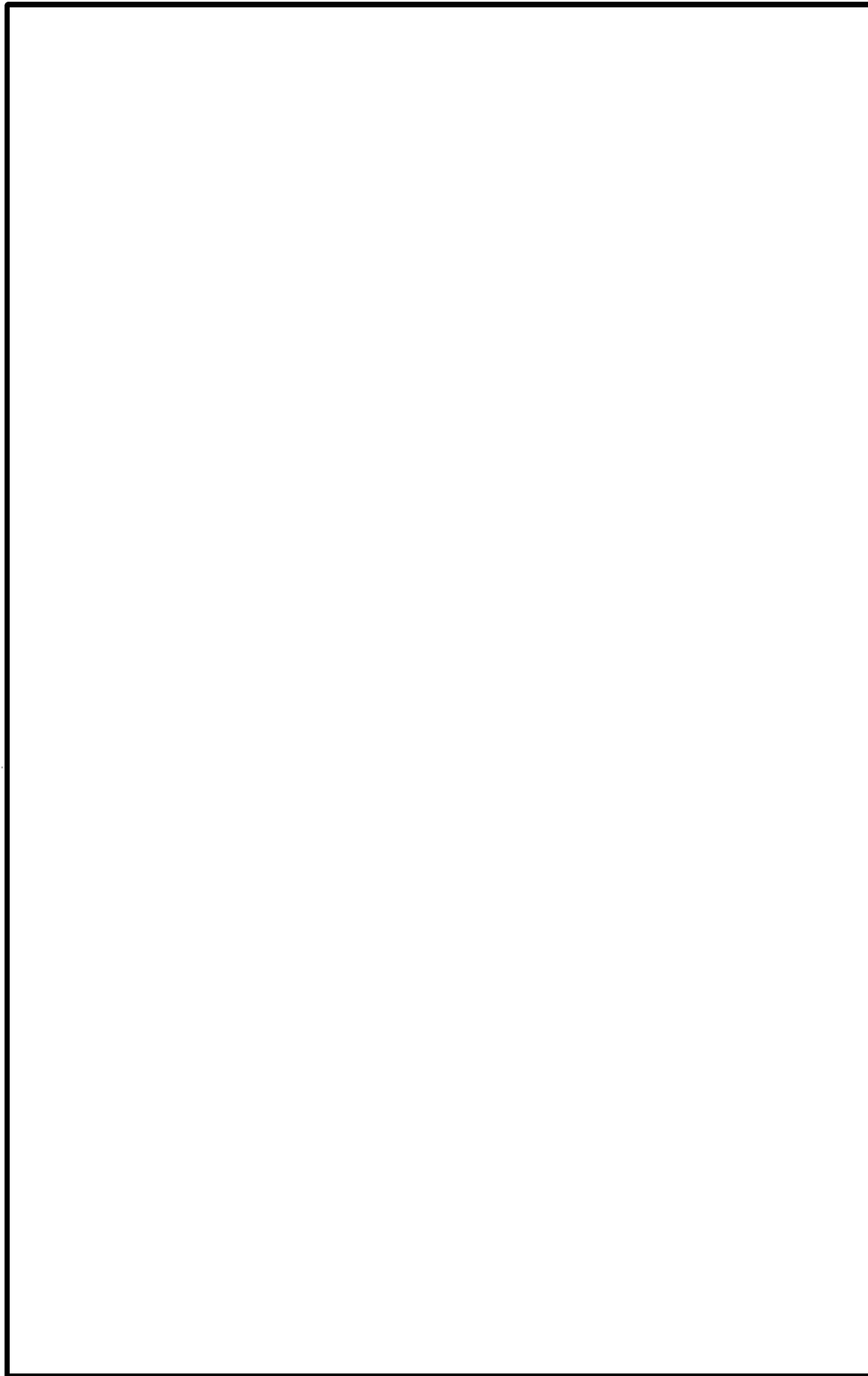
Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued



(b)(5)

(b)(7)(e)

Appendix, Continued

