NOT YET SCHEDULED FOR ORAL ARGUMENT

No. 23-5232

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

Doc Society and International Documentary Association,

Plaintiffs–Appellants,

v.

Antony J. Blinken, in his official capacity as Secretary of State, and Alejandro N. Mayorkas, in his official capacity as Secretary of Homeland Security,

Defendants–Appellees.

On appeal from the United States District Court for the District of Columbia — No. 1:19-cv-03632 (Kelly, T.)

JOINT APPENDIX — VOLUME II OF II (JA220–374)

Carrie DeCell
Jameel Jaffer
Katie Fallow
Anna Diakun
Knight First Amendment Institute at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
carrie.decell@knightcolumbia.org

Joshua Polster
Evan Gilbert
Simpson Thacher & Bartlett LLP
425 Lexington Avenue
New York, NY 10017
(212) 455-2000
joshua.polster@stblaw.com

Counsel for Plaintiffs–Appellants
(Additional counsel on next page)

Faiza Patel
Emile Ayoub
Brennan Center for Justice
at NYU School of Law
120 Broadway, Suite 1750
New York, NY 10271
(646) 292-8310
patelf@brennan.law.nyu.edu

Rachel Levinson-Waldman
Brennan Center for Justice
at NYU School of Law
1140 Connecticut Avenue, NW
11th Floor, Suite 1150
Washington, D.C. 20036
(202) 249-7190
levinsonr@brennan.law.nyu.edu

Counsel for Plaintiffs–Appellants

Table of Contents

VOLUME 1

Docket Entries JA001

Complaint (ECF No. 1), filed December 5, 2019 ..... JA010

Exhibit 1 to Defendants' Motion to Dismiss (ECF No. 31-2), filed April 15, 2020 ..... JA045

Exhibit 2 to Defendants' Motion to Dismiss (ECF No. 31-3), filed April 15, 2020 ..... JA057

Exhibit 3 to Defendants' Motion to Dismiss (ECF No. 31-4), filed April 15, 2020 ..... JA061

Exhibit 4 to Defendants' Motion to Dismiss (ECF No. 31-5), filed April 15, 2020 ..... JA065

Exhibit 5 to Defendants' Motion to Dismiss (ECF No. 31-6), filed April 15, 2020 ..... JA067

Exhibit 6 to Defendants' Motion to Dismiss (ECF No. 31-7), filed April 15, 2020 ..... JA070

Exhibit 7 to Defendants' Motion to Dismiss (ECF No. 31-8), filed April 15, 2020 ..... JA072

Exhibit 8 to Defendants' Motion to Dismiss (ECF No. 31-9), filed April 15, 2020 ..... JA096

Exhibit 9 to Defendants' Motion to Dismiss (ECF No. 31-10), filed April 15, 2020 ..... JA121

Exhibit 10 to Defendants' Motion to Dismiss (ECF No. 31-11), filed April 15, 2020 ..... JA124

Exhibit 11 to Defendants' Motion to Dismiss (ECF No. 31-12), filed April 15, 2020 ..... JA127

VOLUME II

Exhibit 12 to Defendants' Motion to Dismiss (ECF No. 31-13), filed April 15, 2020 ..... JA220

Exhibit 13 to Defendants' Motion to Dismiss (ECF No. 31-14), filed April 15, 2020 ..... JA294

Exhibit 14 to Defendants' Motion to Dismiss (ECF No. 31-15), filed April 15, 2020 ..... JA311

Order (ECF No. 66), filed August 11, 2023 ..... JA332

Memorandum Opinion (ECF No. 67), filed August 11, 2023 ..... JA333

Notice of Appeal (ECF No. 69), filed October 10, 2023 ..... JA373

EXHIBIT 12:

OMB Approval of Change to Nonimmigrant Visa Application

Sign In


U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER
Select Tooltip Language ENGLISH
Online Nonimmigrant Visa Application (DS-160)
Apply For a Nonimmigrant Visa
FAQs
Tooltip Language: English [View Tool Tip Help]
Most of this application has been translated. To see the translation point your mouse over any sentence on the page.
Welcome!
On this website, you can apply for a U.S. nonimmigrant visa. Filling out the application on our site is the first step in the process. After you submit your application, you can move on to the next steps, such as signing up for an interview.
Important: Before You Start
1. Learn about Types of Visas
2. List of Documents and Information you will need
3. Browser Requirements
4. How to complete the application
Other people can assist you with your visa application. Note that under U.S. law (22 C.F.R. 41.103) you must electronically sign and submit your own application unless you qualify for an exemption. Even if someone else helped you complete the application, you (the applicant) must click the "Sign Application" button, or your application may not be accepted.
Please be patient as you use this form. Download times may vary depending on your internet connection speed.
Get Started
Select a location where you will be applying for this visa
- SELECT ONE -
Enter the code as shown:
KW865
Select a location and make sure you have the documents and information you will need.
START AN APPLICATION
Select a location then select an application that you previously saved on your computer.
UPLOAD AN APPLICATION
You will be asked for your application ID and answer a security question.
RETRIEVE AN APPLICATION
Additional Information
» Read more about U.S. visas at travel.state.gov.
» Visit the website of the U.S. Embassy or Consulate.
This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information Disclaimers Paperwork Reduction Act

Application Information



Exit

U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Select Tooltip Language ENGLISH

Online Nonimmigrant Visa Application (DS-160)

Application Information

Please record your Application ID in a safe and secure place.

If there are technical issues with the system, or you want to complete your application some other time, you can save your work and later, start where you left off. In order to access your application later, however, you will need: (1) your Application ID, and (2) the answer to the security question that you will choose on this page.

Your Application ID is:
AA0001IRZK

Date
13-APR-2017

Print Application ID

To choose a security question, pick the one you like the best from the dropdown list, type your answer to that question in the box below, and click "Continue." Remember: In order to access your application later, you will need to know the answer ***exactly as you wrote it on this page.***

You can also use your Application ID and security question to retrieve your Confirmation Page after you have submitted your application, or to use your previously provided application information to complete a new application at a later date.

If you do not plan to complete your application within the next 30 days, download your application to your computer by clicking the "Save" button at the bottom of the last completed page. Follow the instructions. When you are ready to complete your application, select "Upload an Application". NOTE: Only download your application to a computer that cannot be accessed by anyone who does not have your permission to see or record your personal data. If you download your application a shared or public computer, such as a computer in a cyber café or library, your personal information may be able to be accessed by other users.

Note: Electronically submitting your DS-160 online application is the FIRST STEP in the visa application process. The next step is to review the internet page of the embassy or consulate where you plan to apply for your visa. Most visa applicants will need to schedule a visa interview, though some applicants may qualify for visa renewal. The embassy or consulate information may include specific local instructions about scheduling interviews, submitting your visa application, and other frequently asked questions.

Security Question
WHAT IS THE GIVEN NAME OF YOUR MOTHER'S MOTHER?

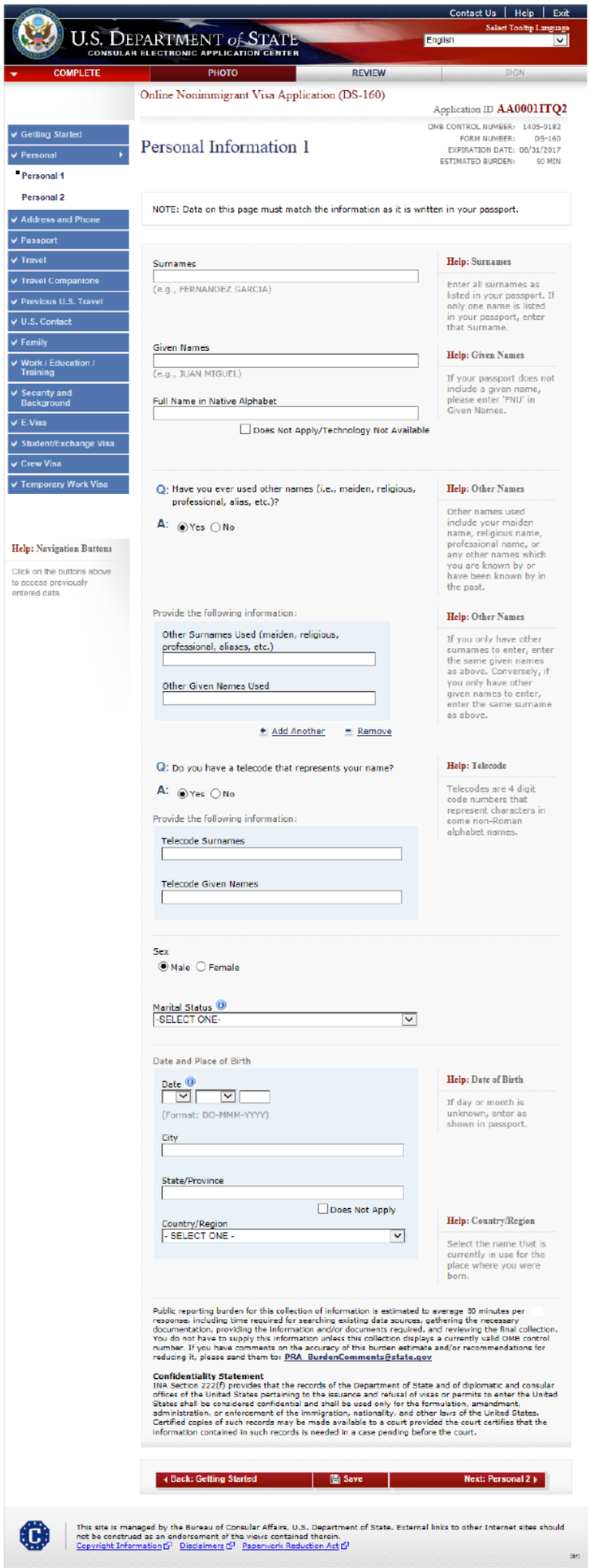
Answer

Continue Cancel

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information Disclaimers Paperwork Reduction Act

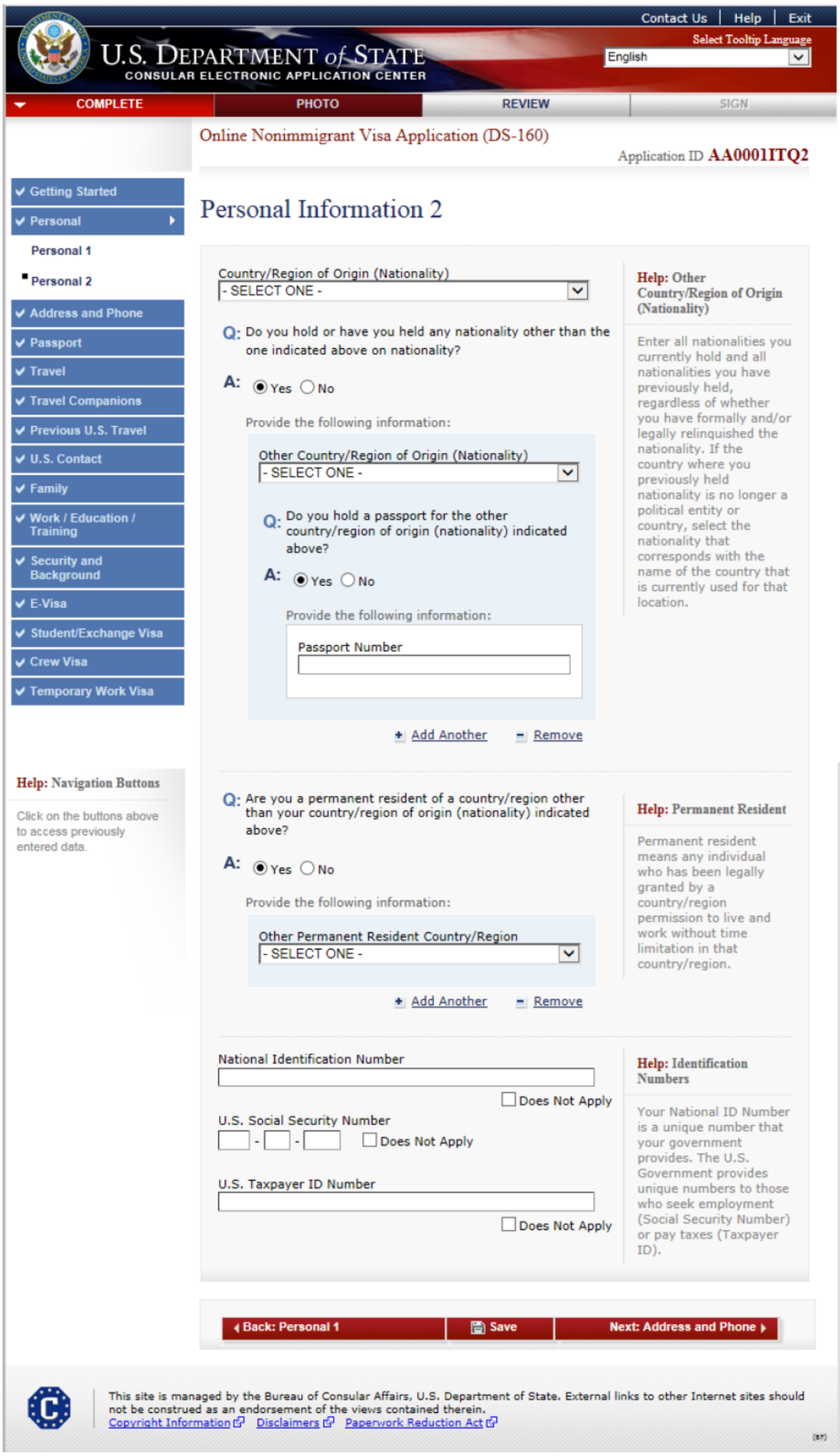
Personal Information 1

Displayed for all applicants.



Personal Information 2

Displayed for all applicants. Answered 'Yes' to all questions on the page. No additional fields are triggered if 'No' is answered to the question 'Do you hold a passport for the nationality above?'.

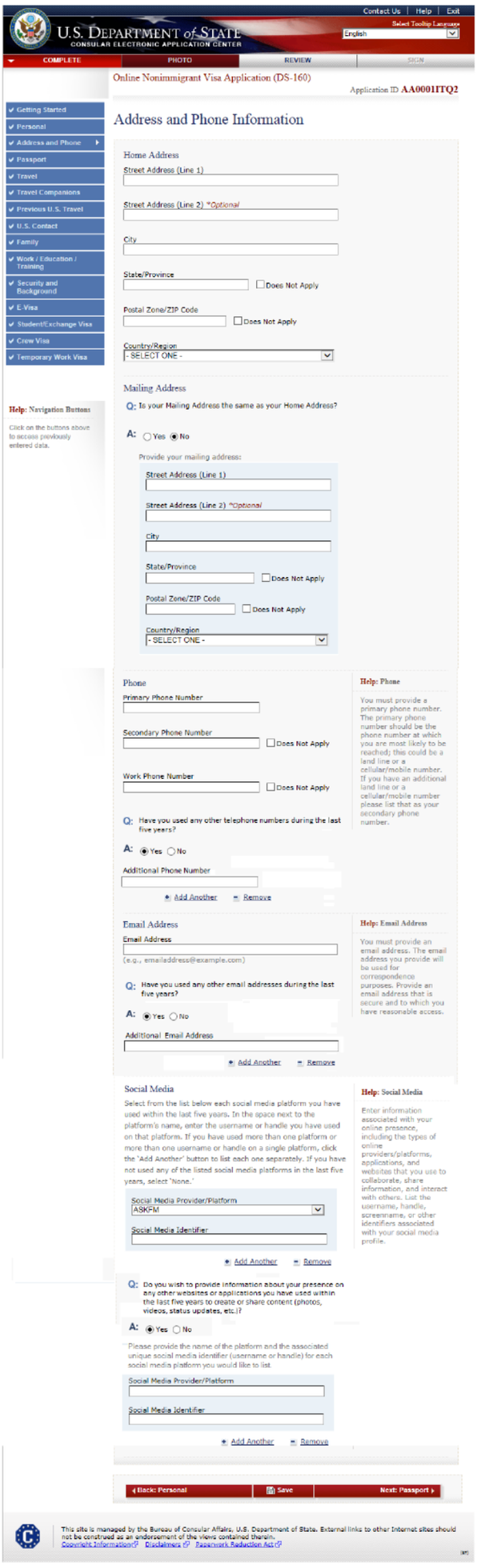


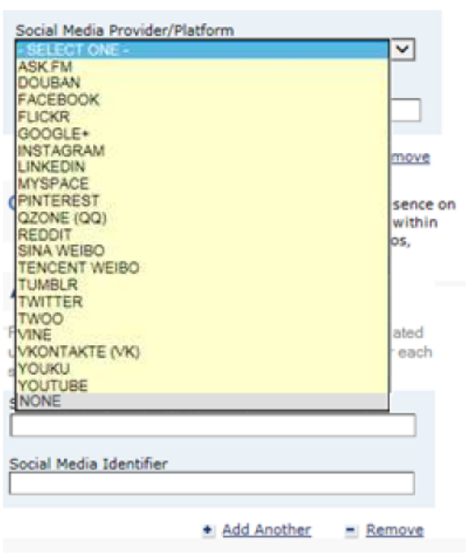
Address and Phone Information

Displayed for all applicants. All questions are answered 'Yes'.

Social Media and Additional 5 Years of Email and Telephone Questions

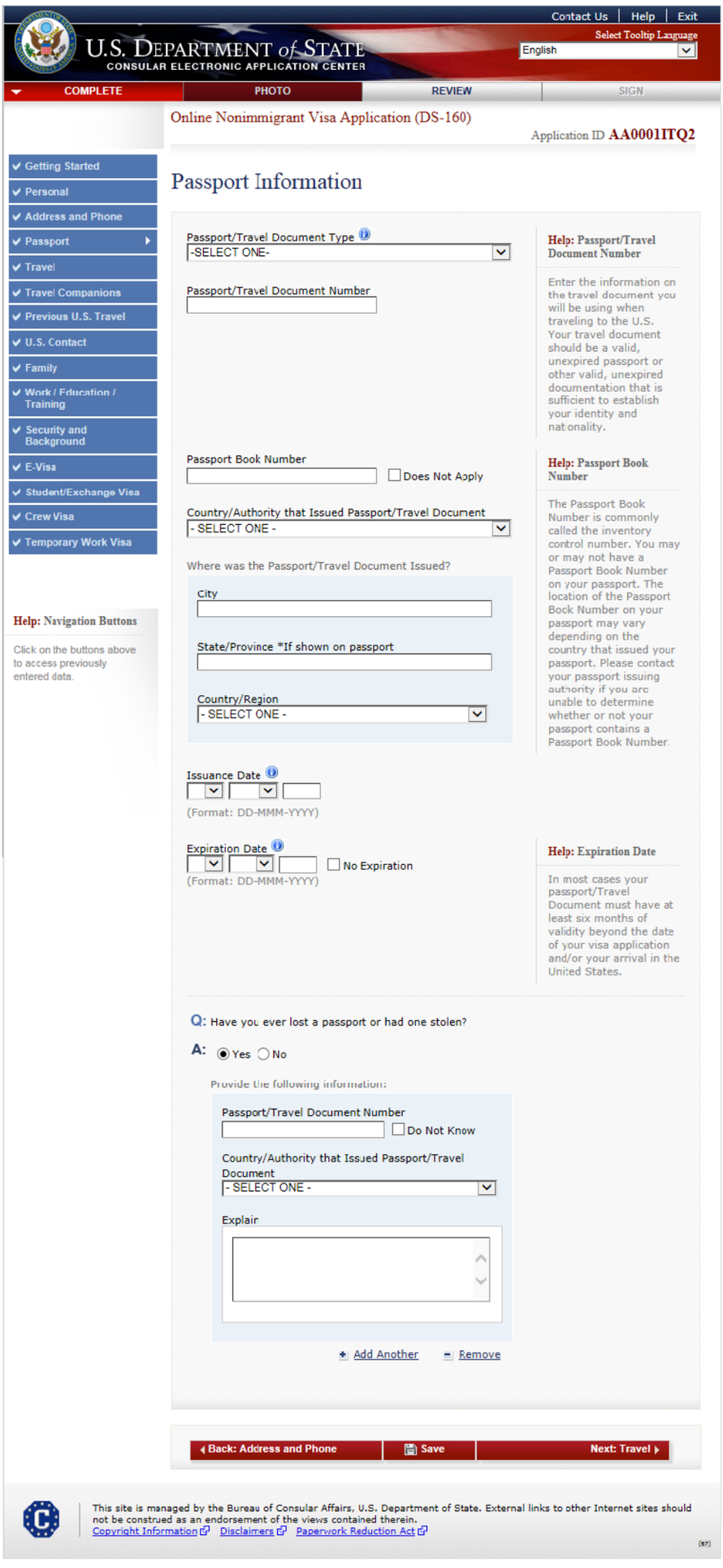
Displayed for all applicants except for most diplomatic and official type visa applicants.





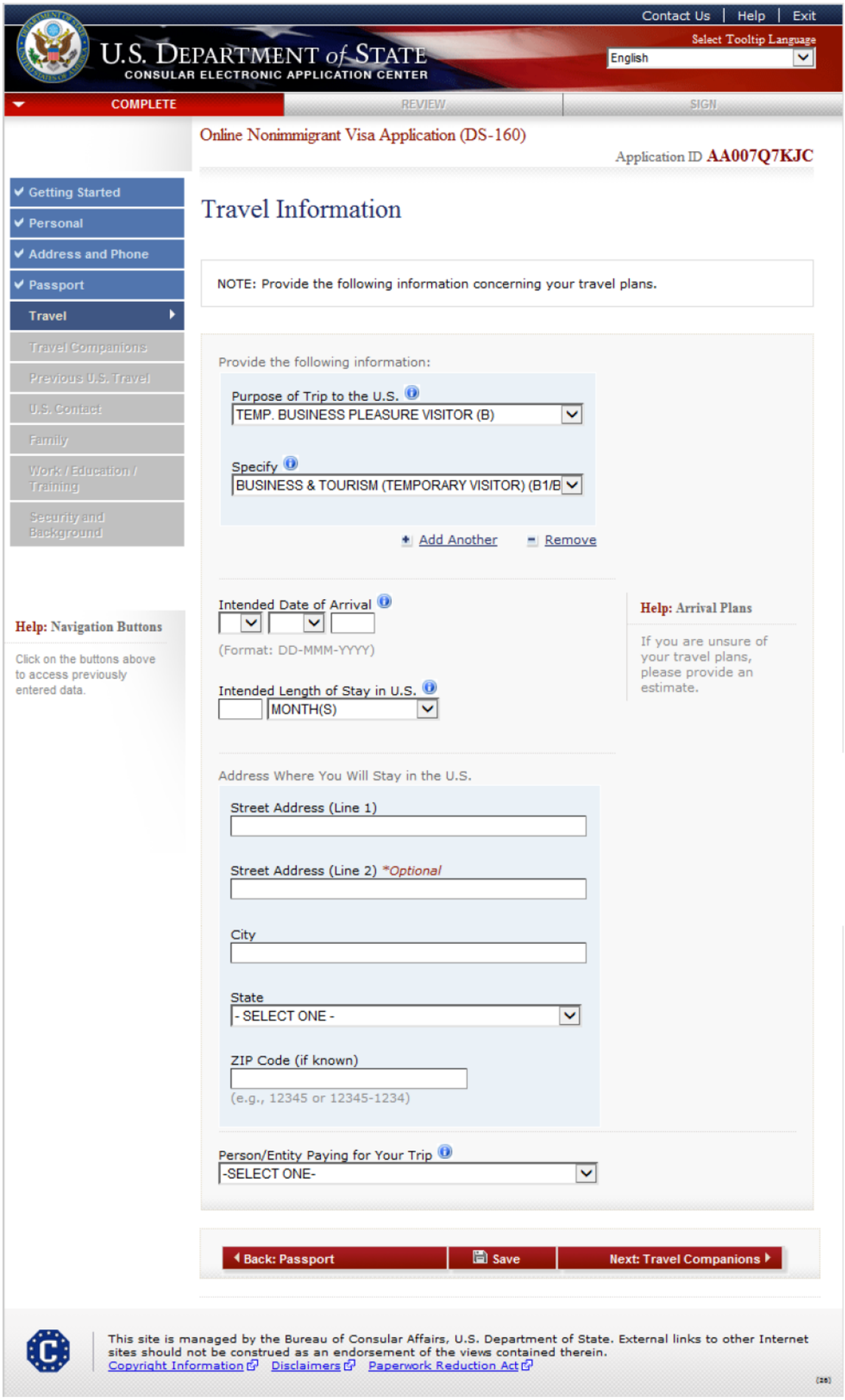
Passport Information

Displayed for all applicants. All questions are answered 'Yes'.



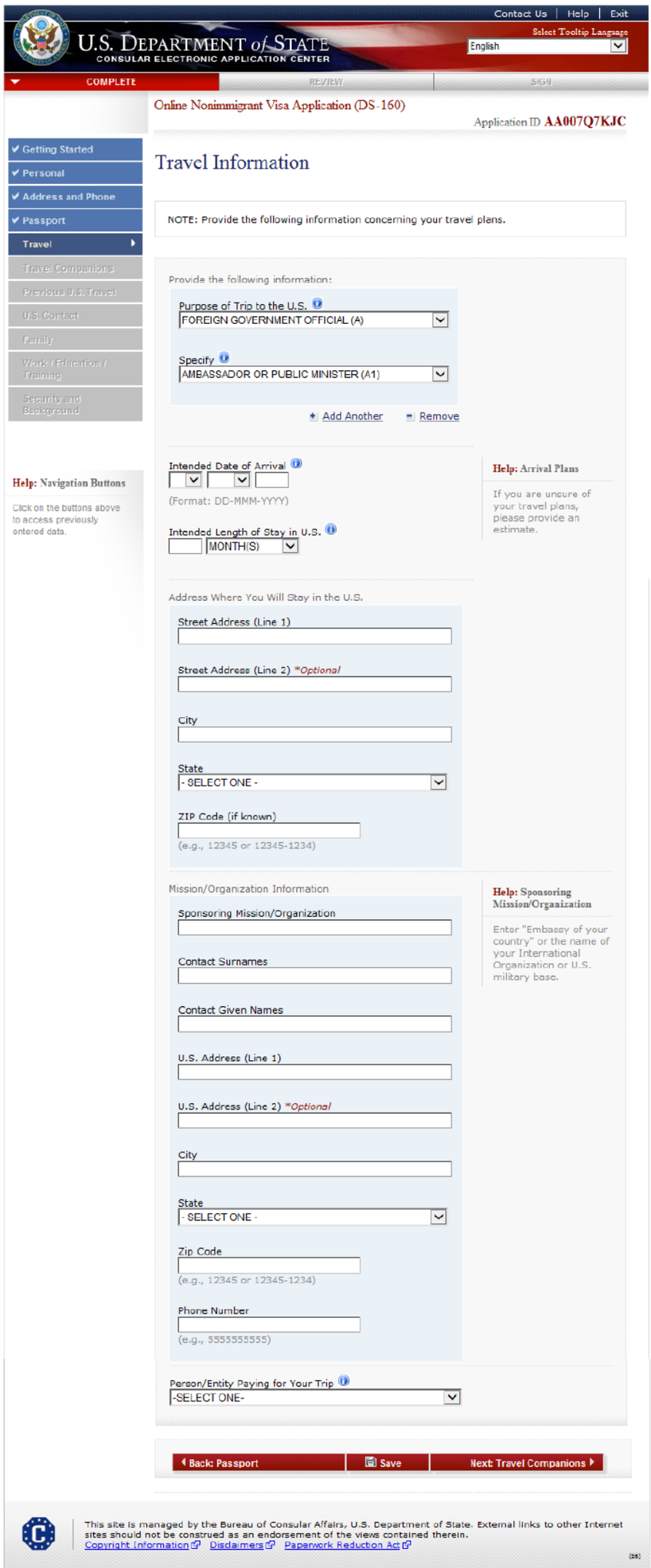
Travel Information

Displayed for principal applicants who select the following visa types: B, C, D, E, F, G, H1B1, I, J, M, N, NATO, Q, S, and Parcis.



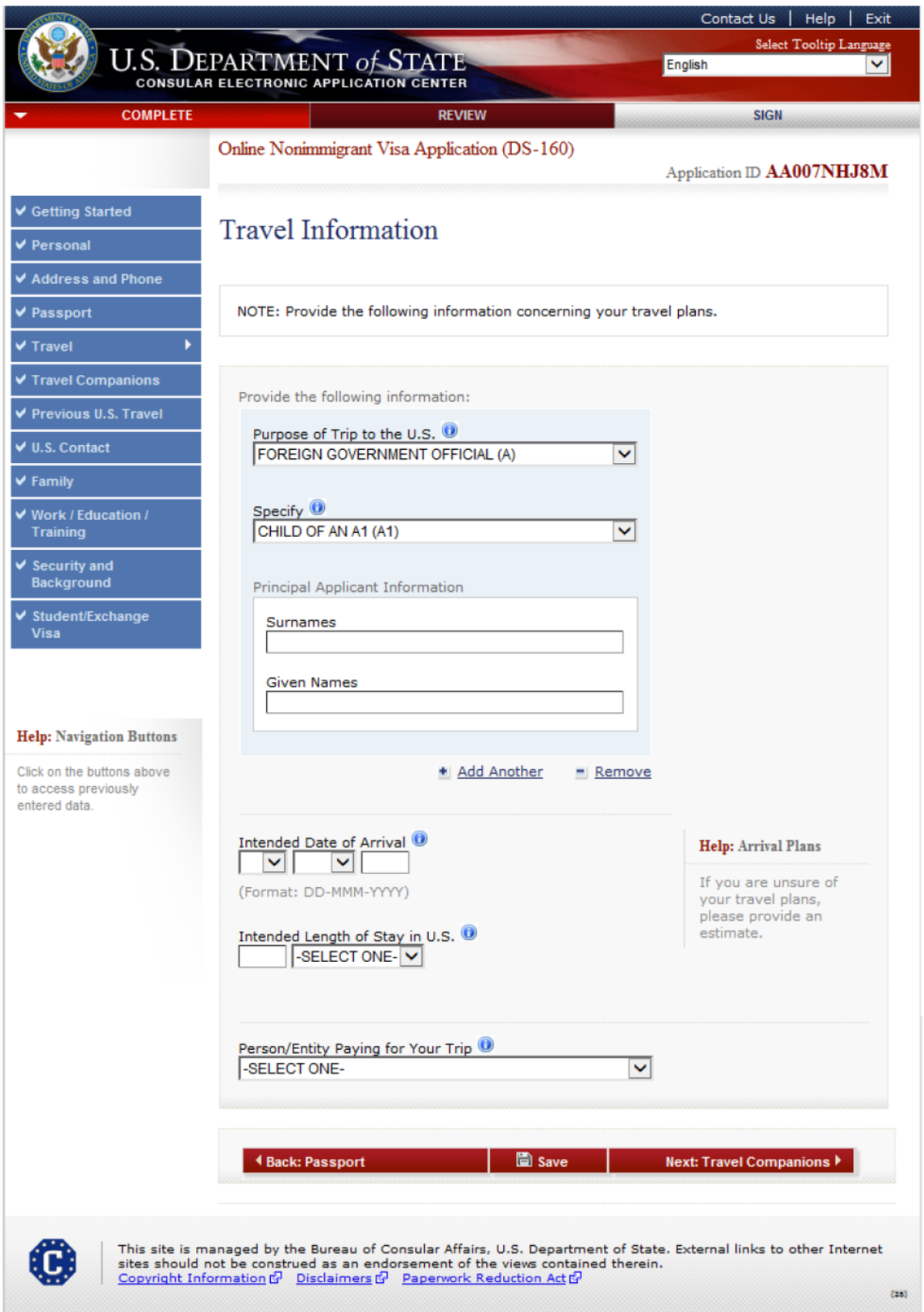
Travel Information

Displayed for principal applicants who select an A-Visa.



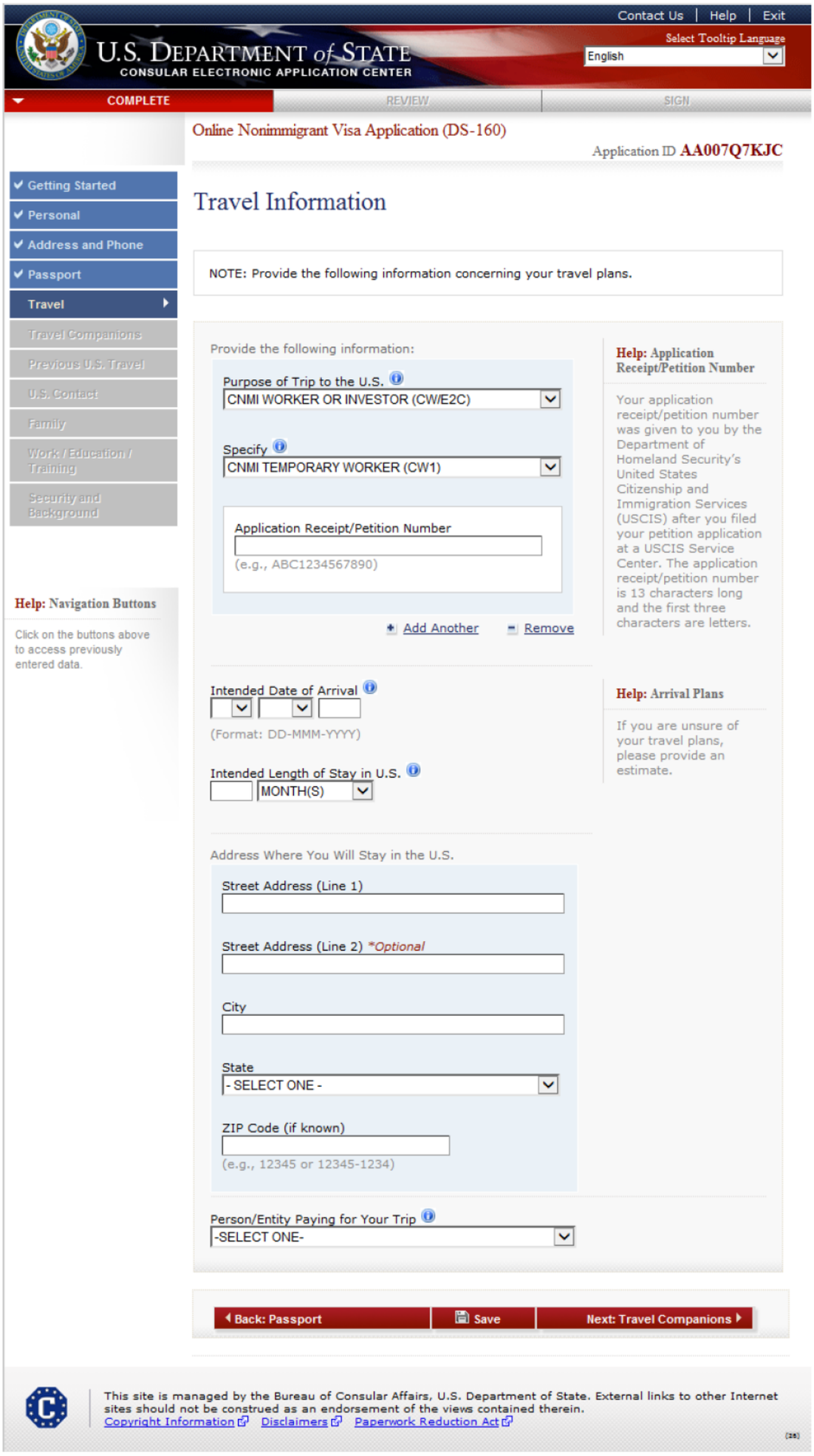
Travel Information

Displayed for non-principal applicants (ex. Child Of, Spouse Of, etc.) who select the following visa types: A, B, C, D, E, F, G, H1B1, I, J, M, N, NATO, Q, S, and PARCIS.



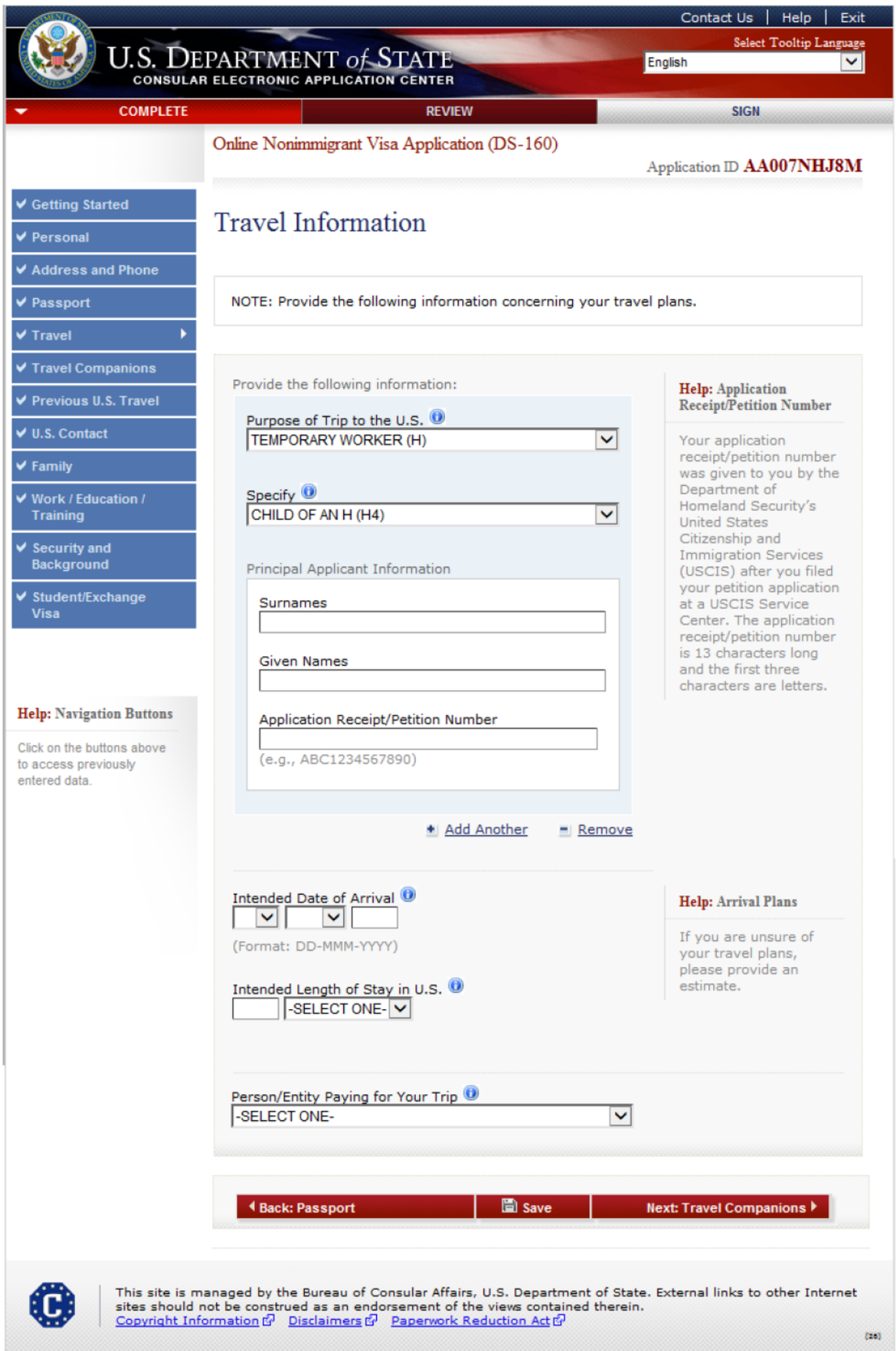
Travel Information

Displayed for principal applicants who select the following visa types: CW/E2C, H1B, H1C, H2A, H2B, H3, K1, K3, L, O, P, R, T, and U.



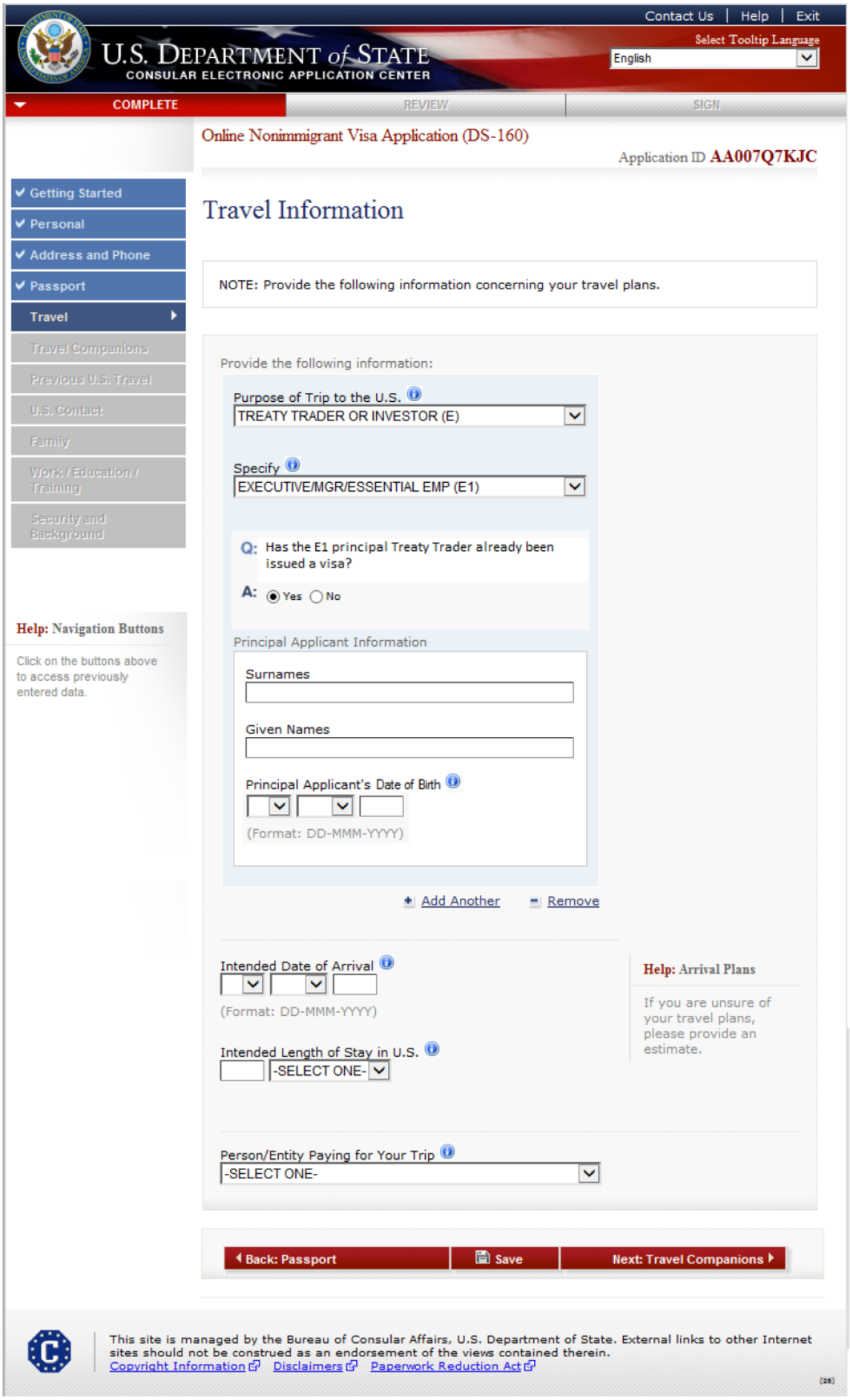
Travel Information

Displayed for non-principal applicants (ex. Child Of, Spouse Of, etc.) who select the following visa types: CW/E2C, H1B, H1C, H2A, H2B, H3, K1, K3, L, O, P, R, T, and U.



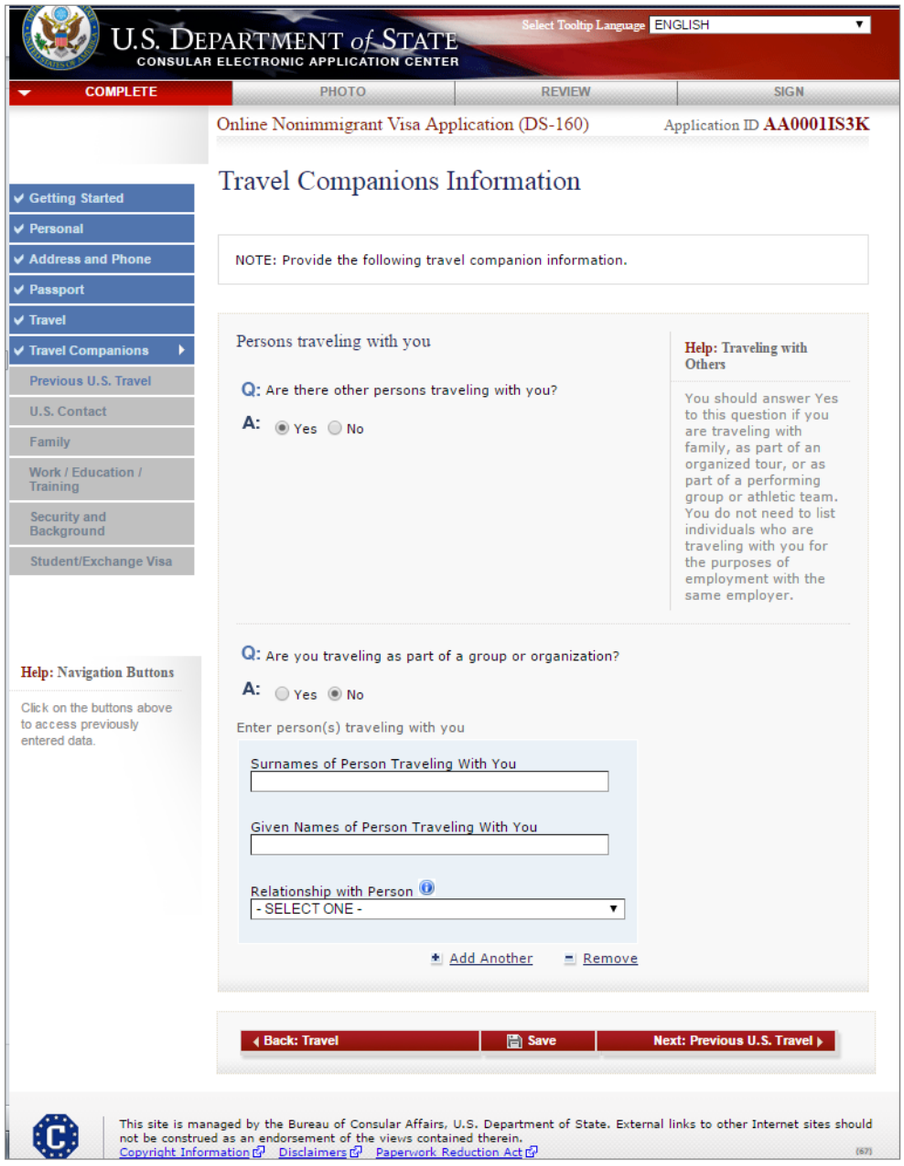
Travel Information

Displayed for principal applicants who select the E1-EX (Executive/Manager/Essential Employee) Visa and choose 'YES' for the following question.



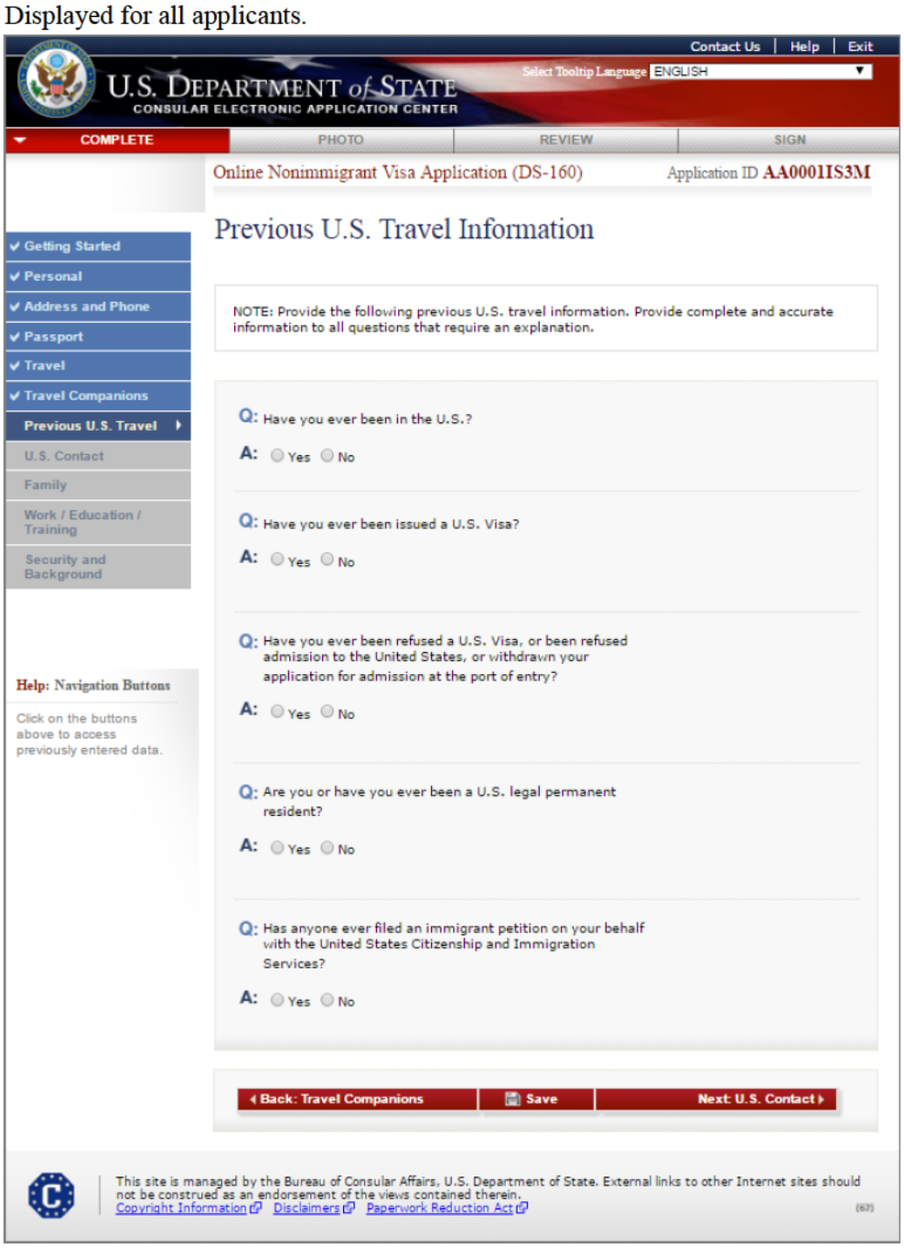
Travel Companions Information

Displayed for all applicants.



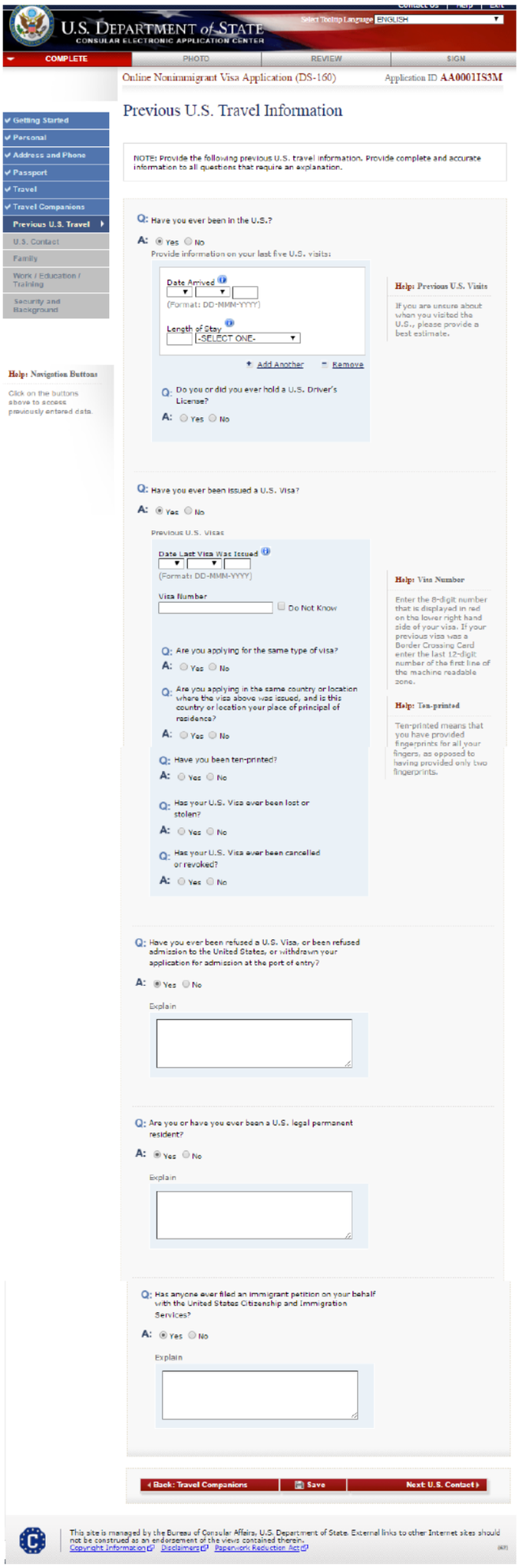
Previous U.S. Travel Information

Displayed for all applicants.



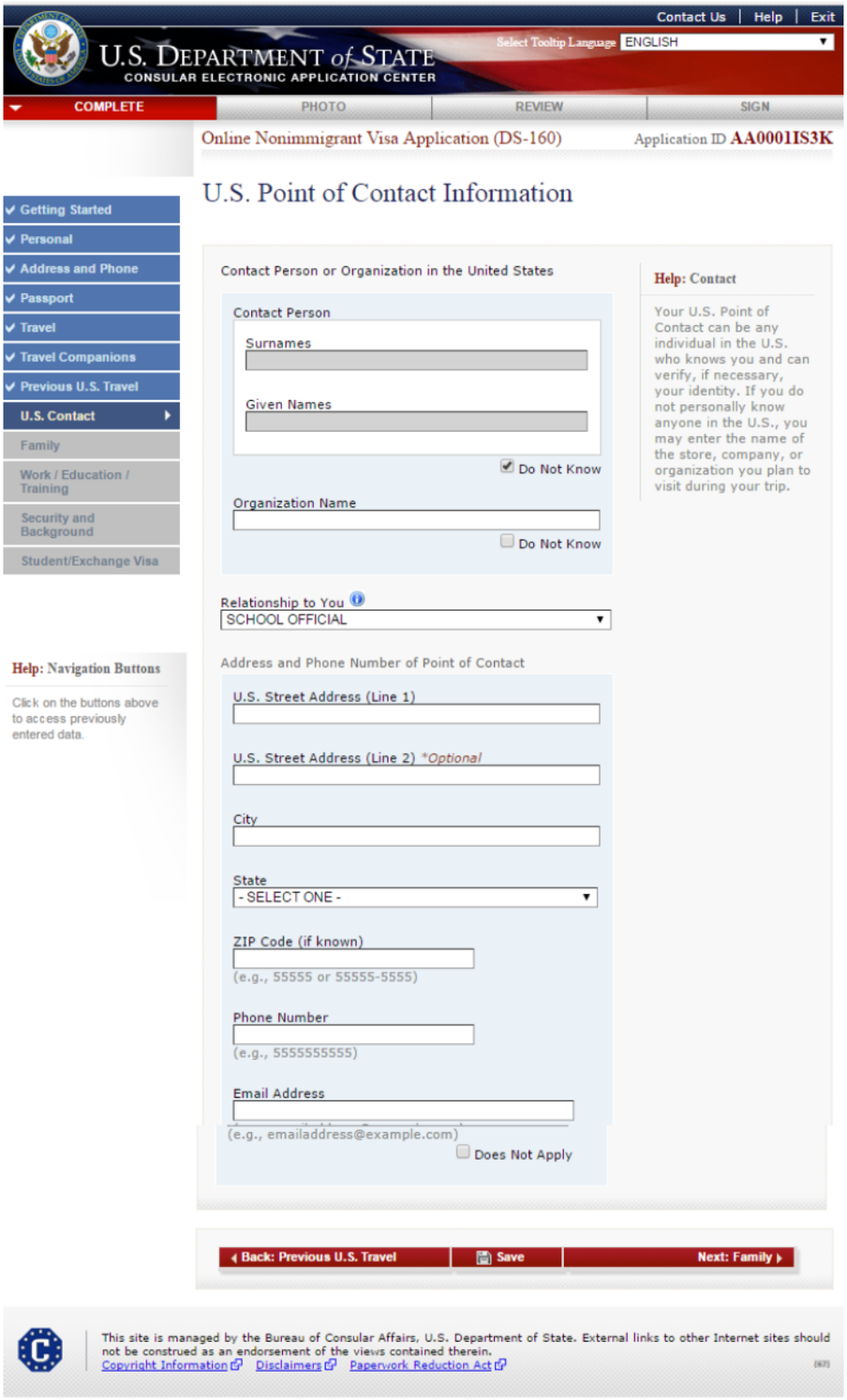
Previous U.S. Travel Information

When all questions are answered 'Yes'.



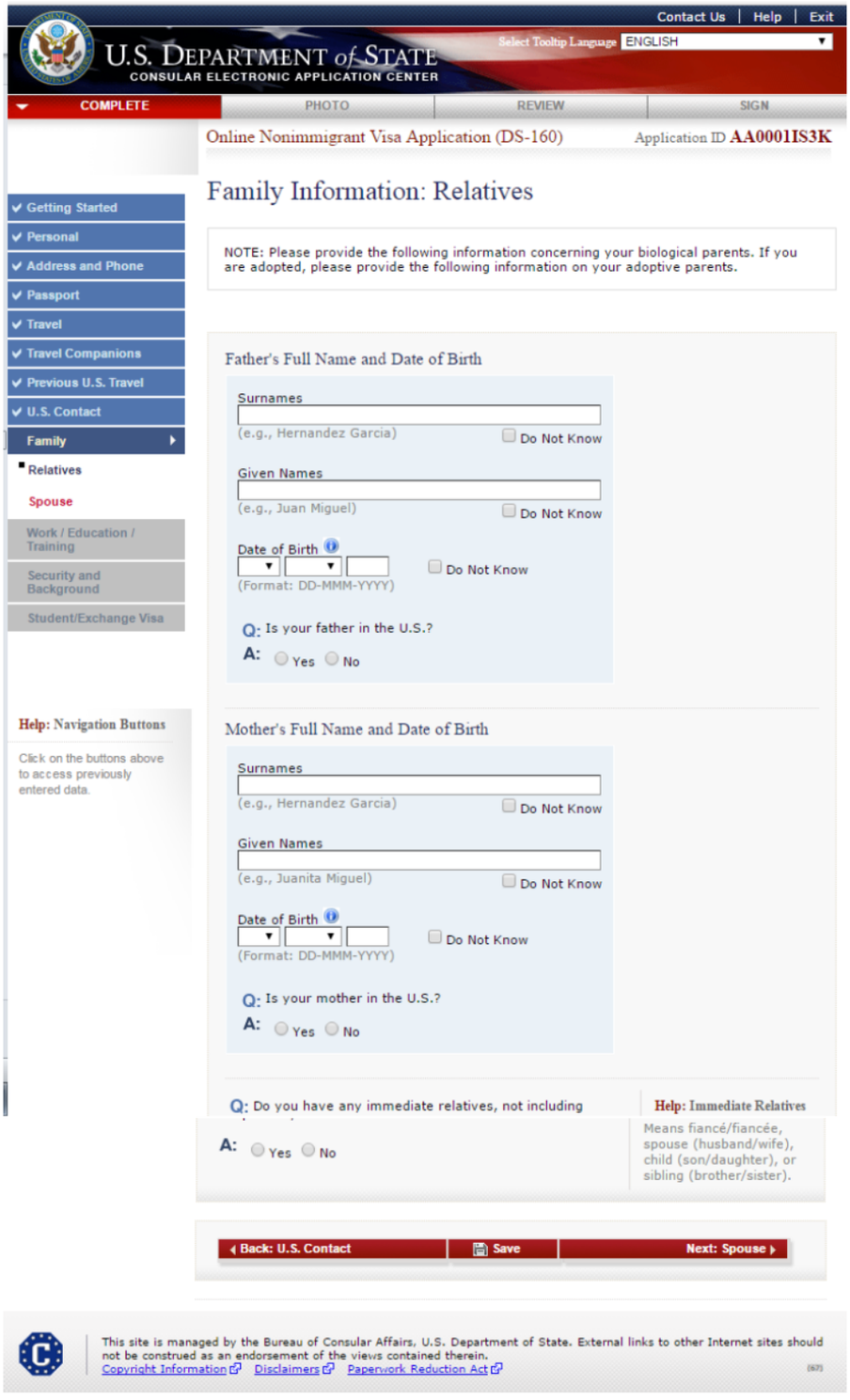
U.S. Point of Contact Information

Displayed for all applicants. All questions are answered 'Yes'.



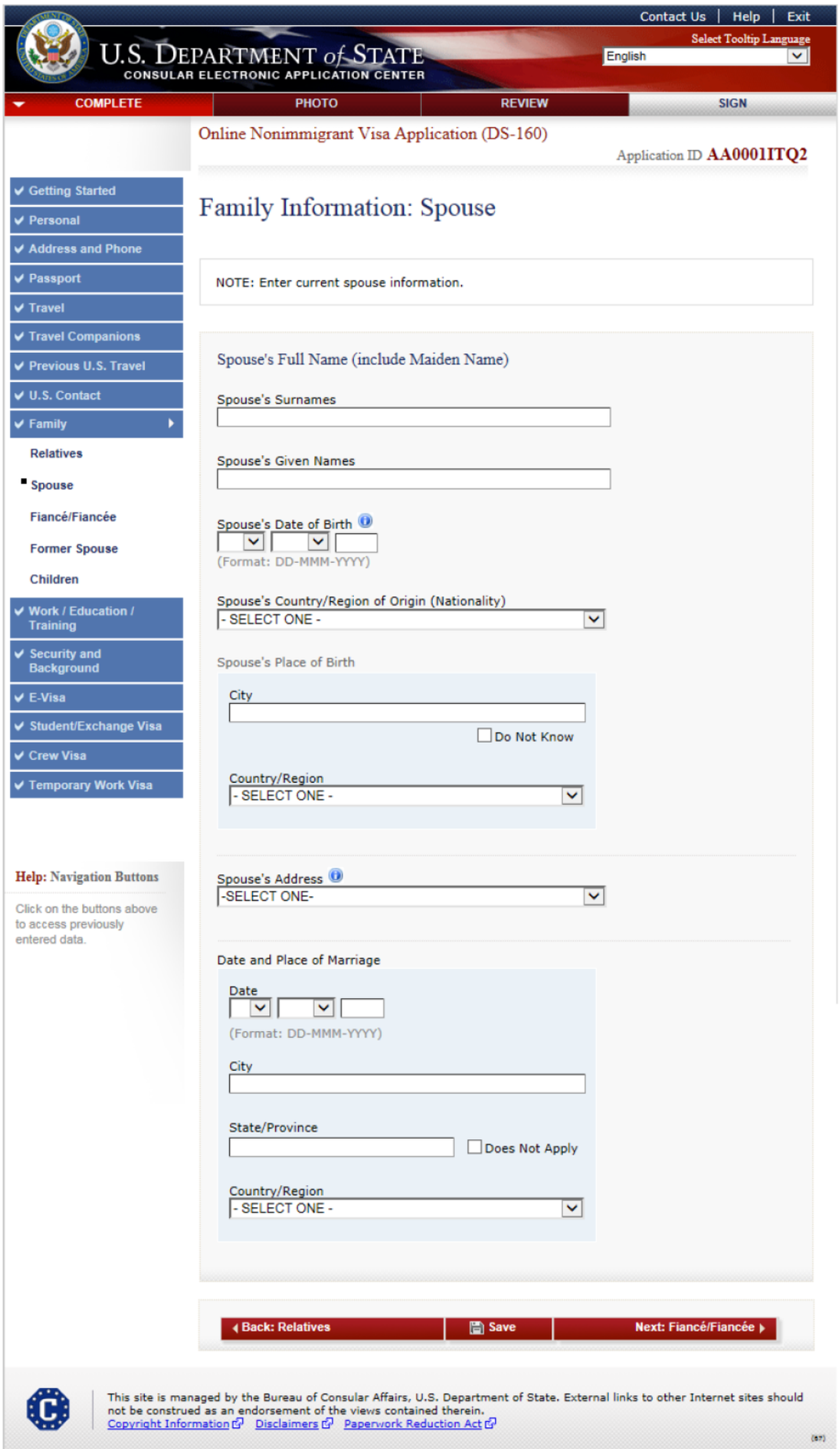
Family Information: Relatives

Displayed for all applicants.



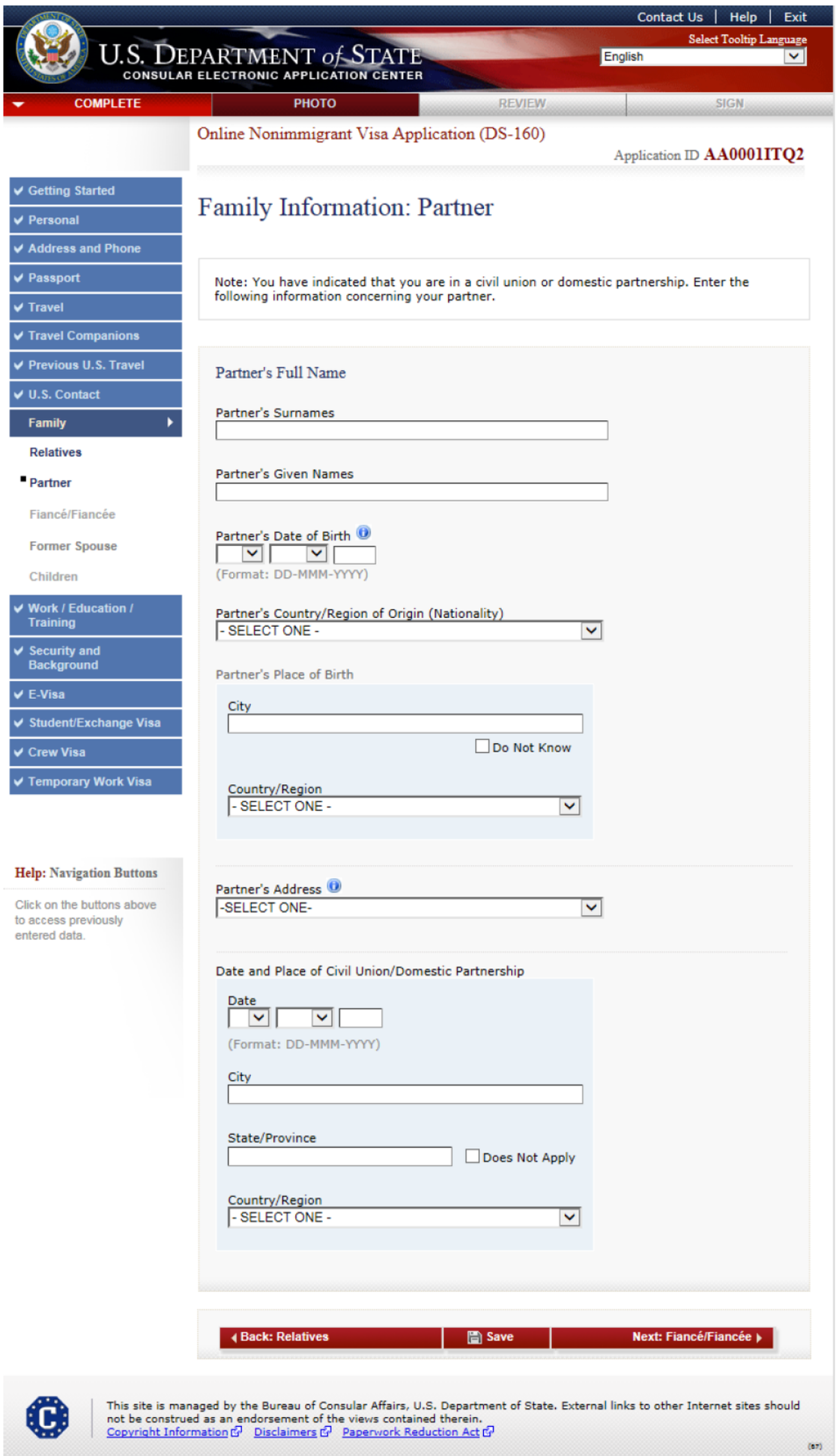
Family Information: Spouse

Displayed for all applicants who selected 'Married'/'Common Law Marriage' on the 'Personal Information 1' page.



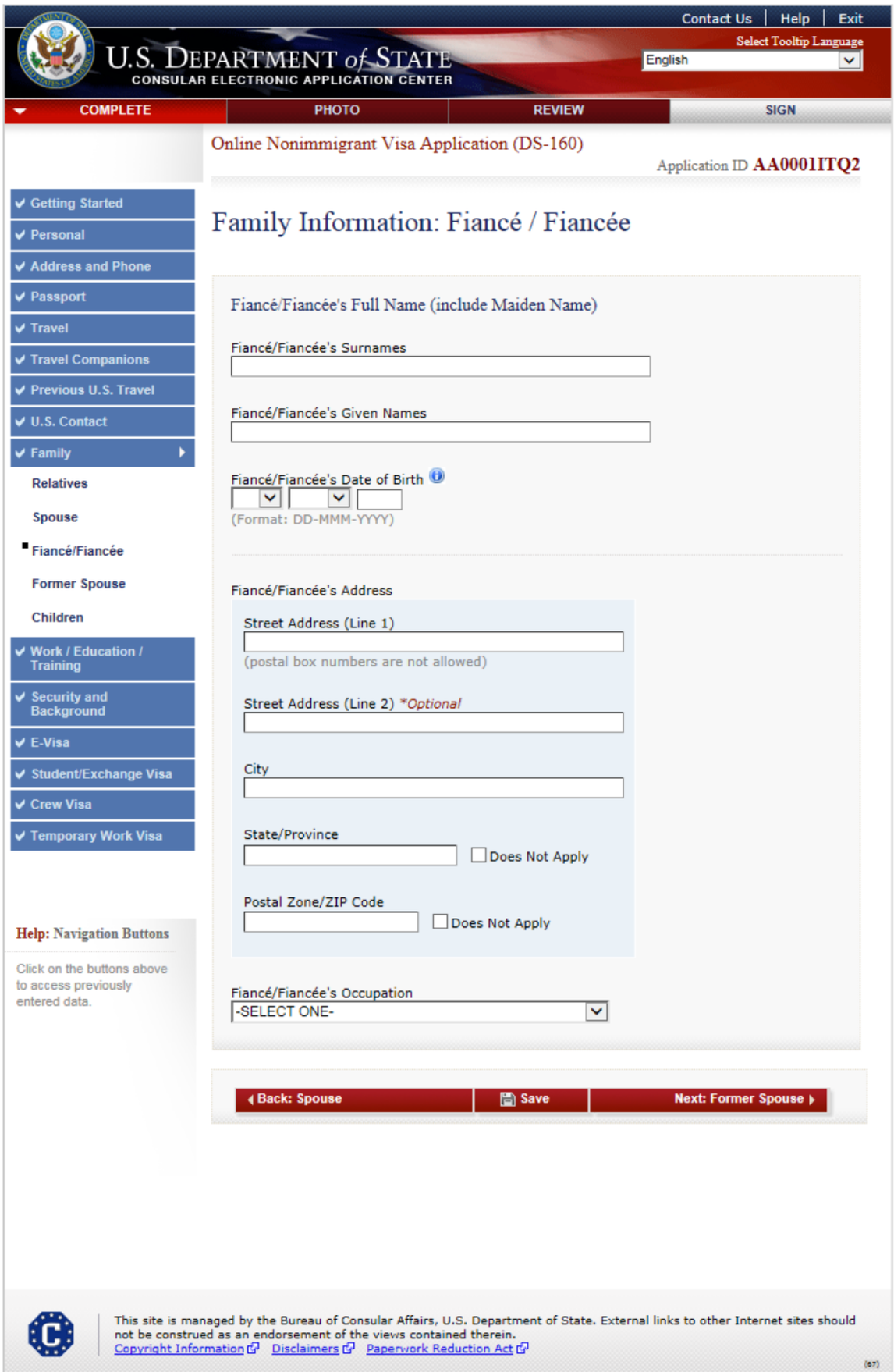
Family Information: Partner

Displayed for all applicants who selected 'Civil Union/Domestic Partnership' on the 'Personal Information 1' page.



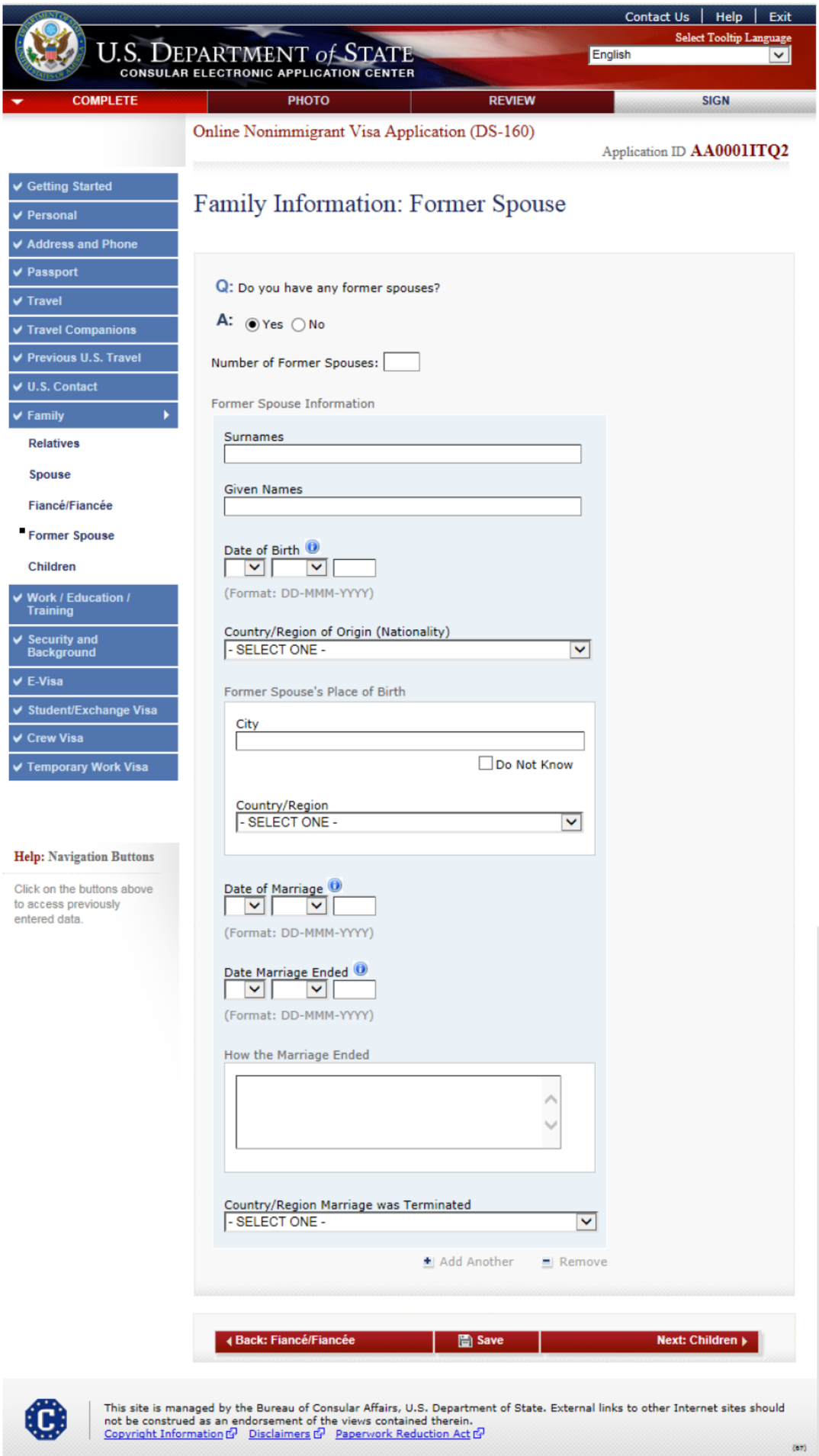
Family Information: Fiancé / Fiancée

Displayed for all K1 applicants.



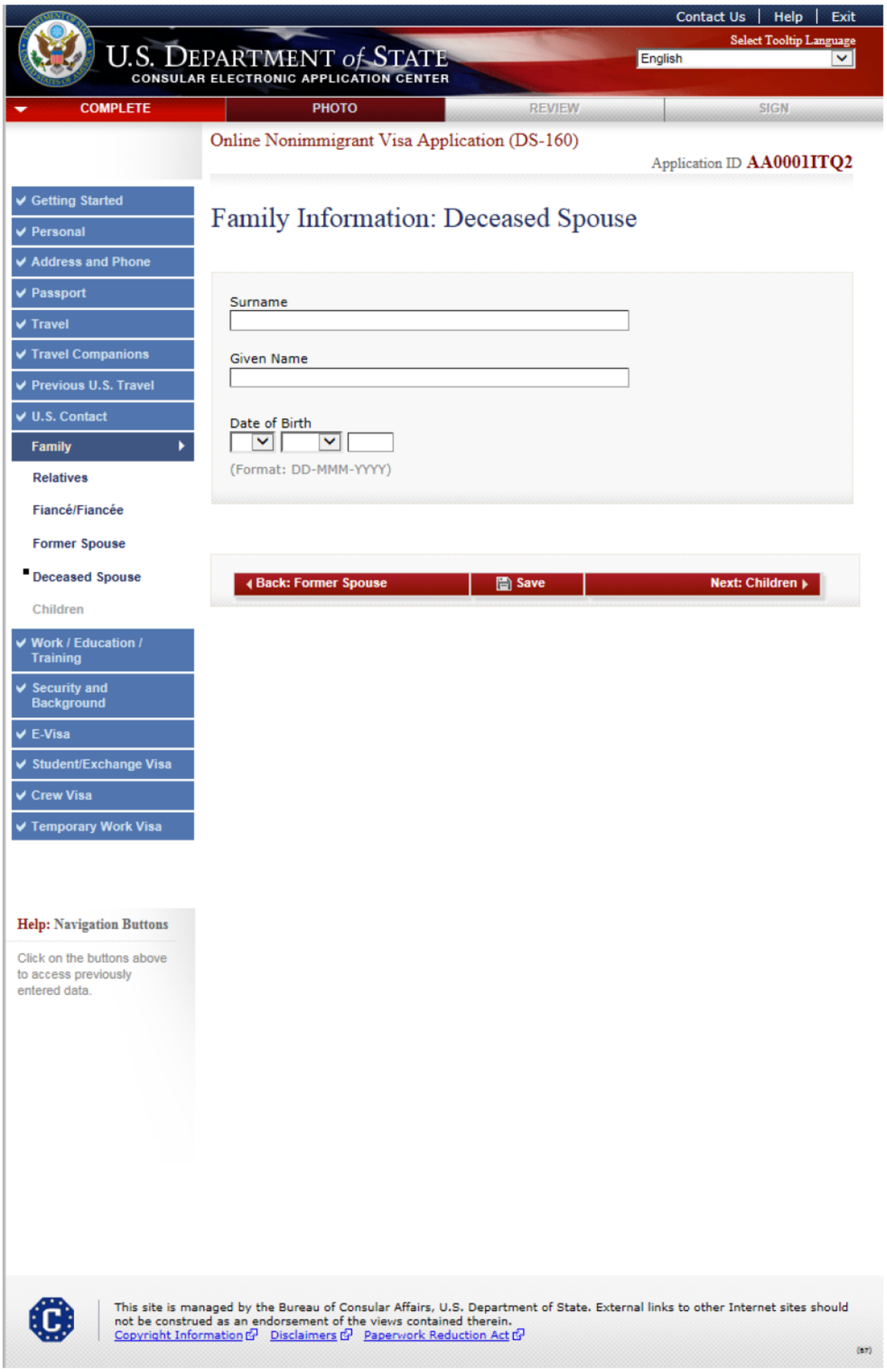
Family Information: Former Spouse

Displayed for all K1 applicants, and applicants who selected 'Divorced' or 'Legally Separated' on the 'Personal 1' page.



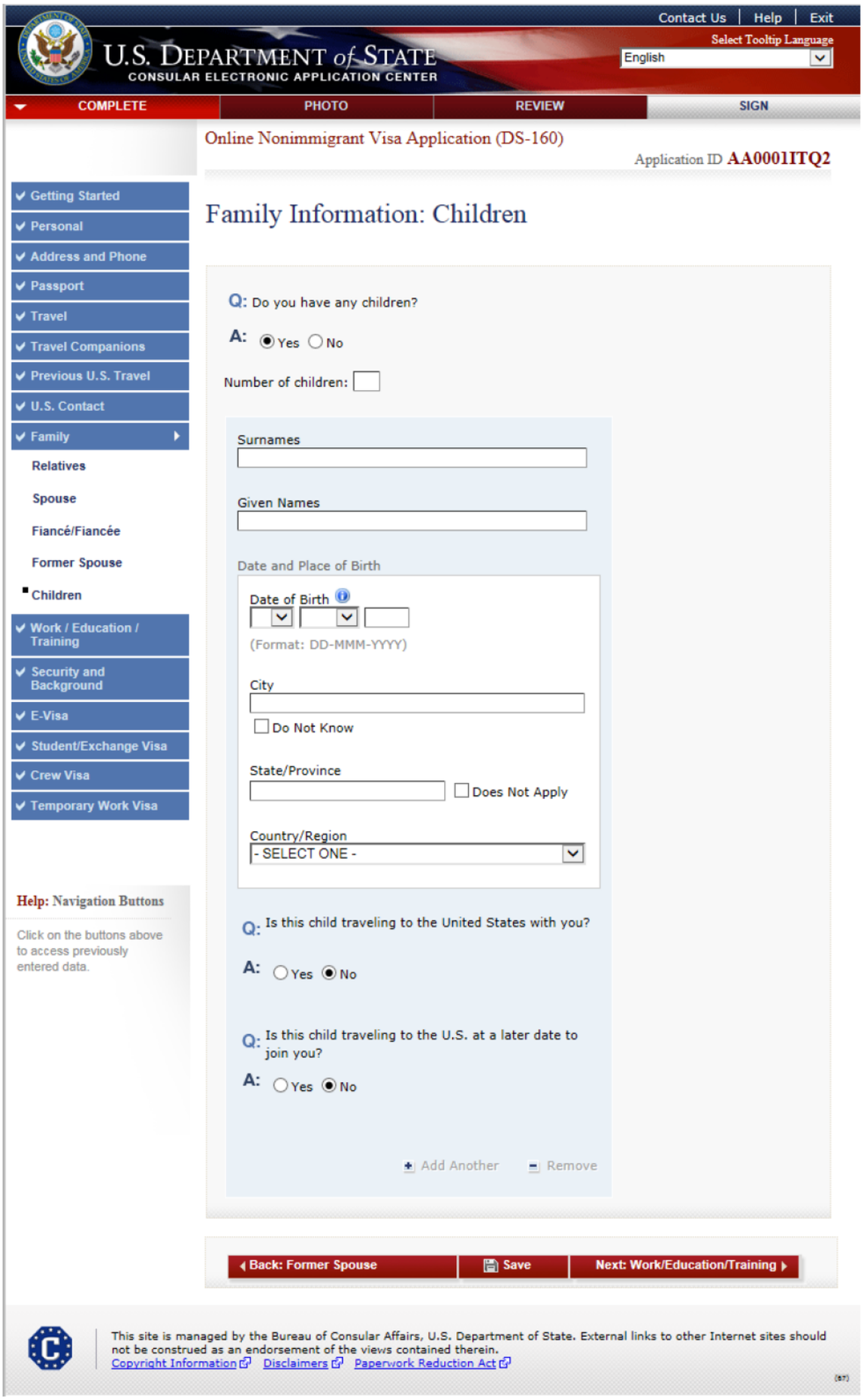
Family Information: Deceased Spouse

Displayed for applicants who selected 'Widowed' on the 'Personal 1' page.



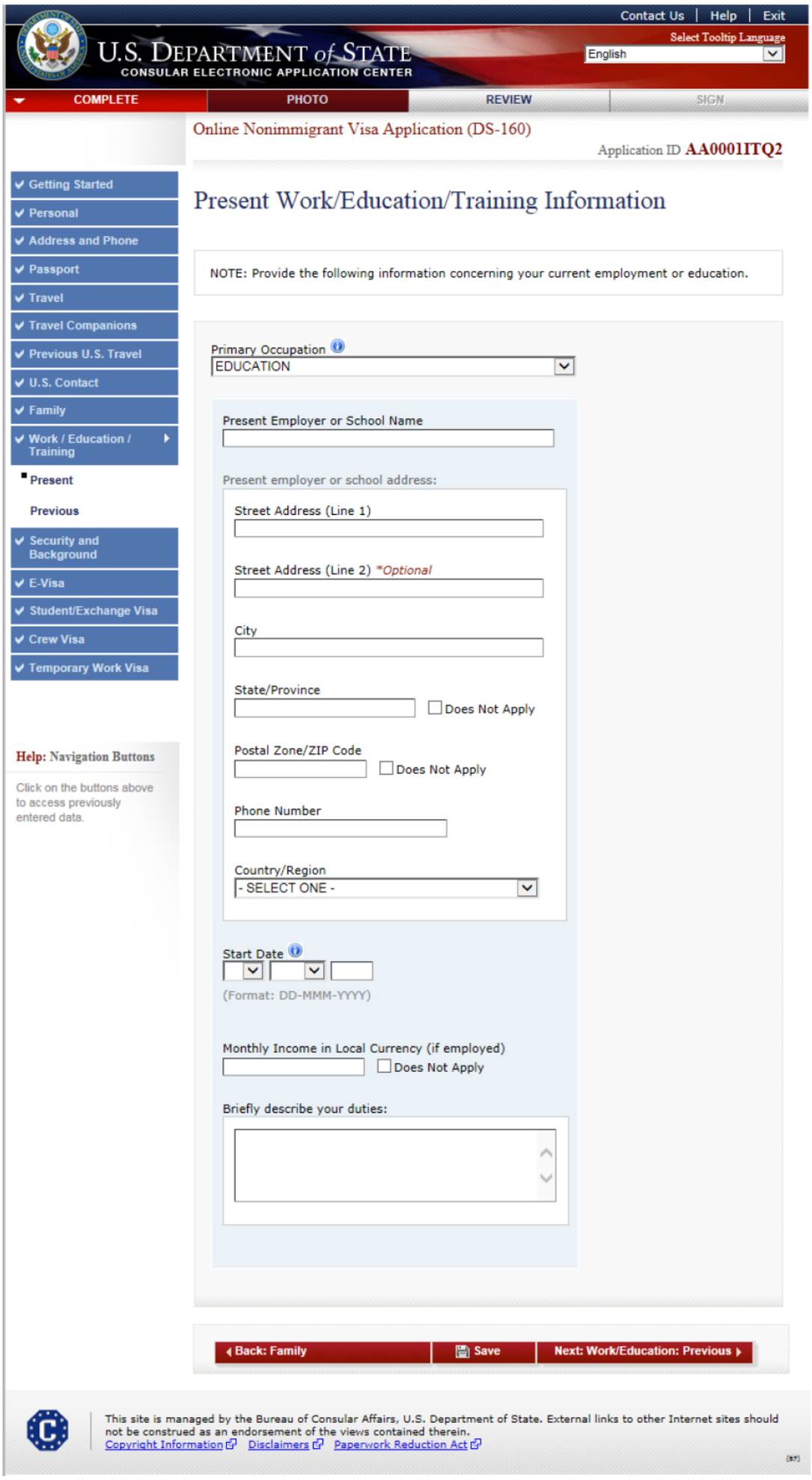
Family Information: Children

Displayed for all K1/K3 applicants.



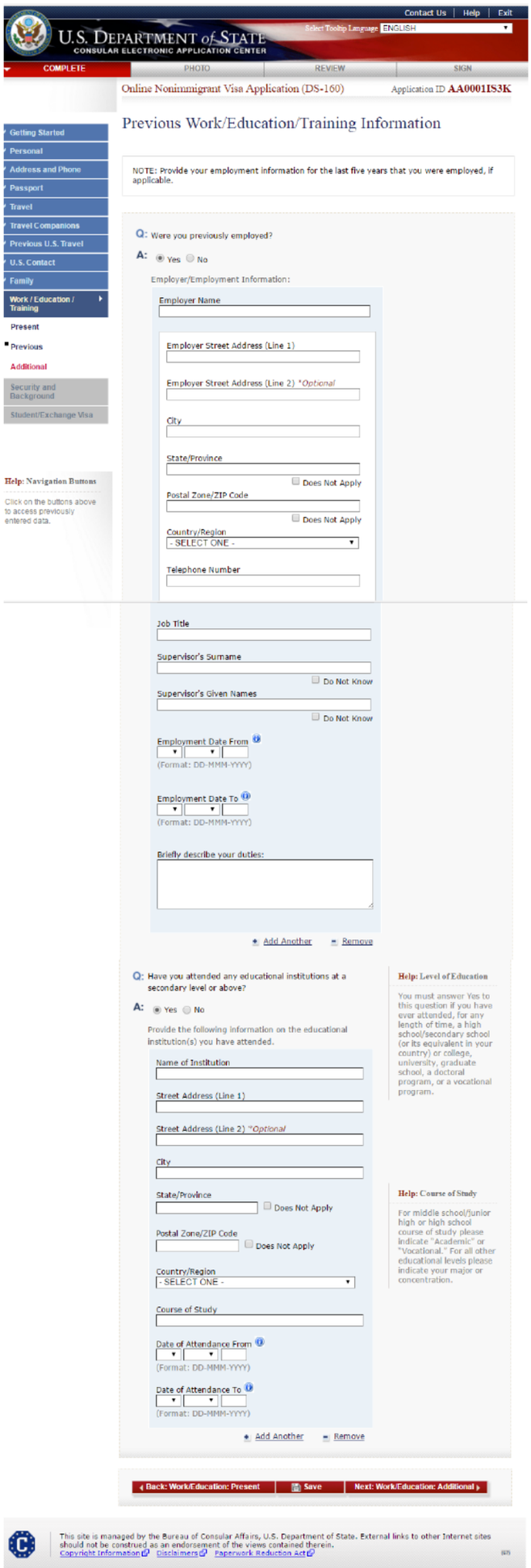
Present Work/Education/Training Information

Displayed for all applicants.



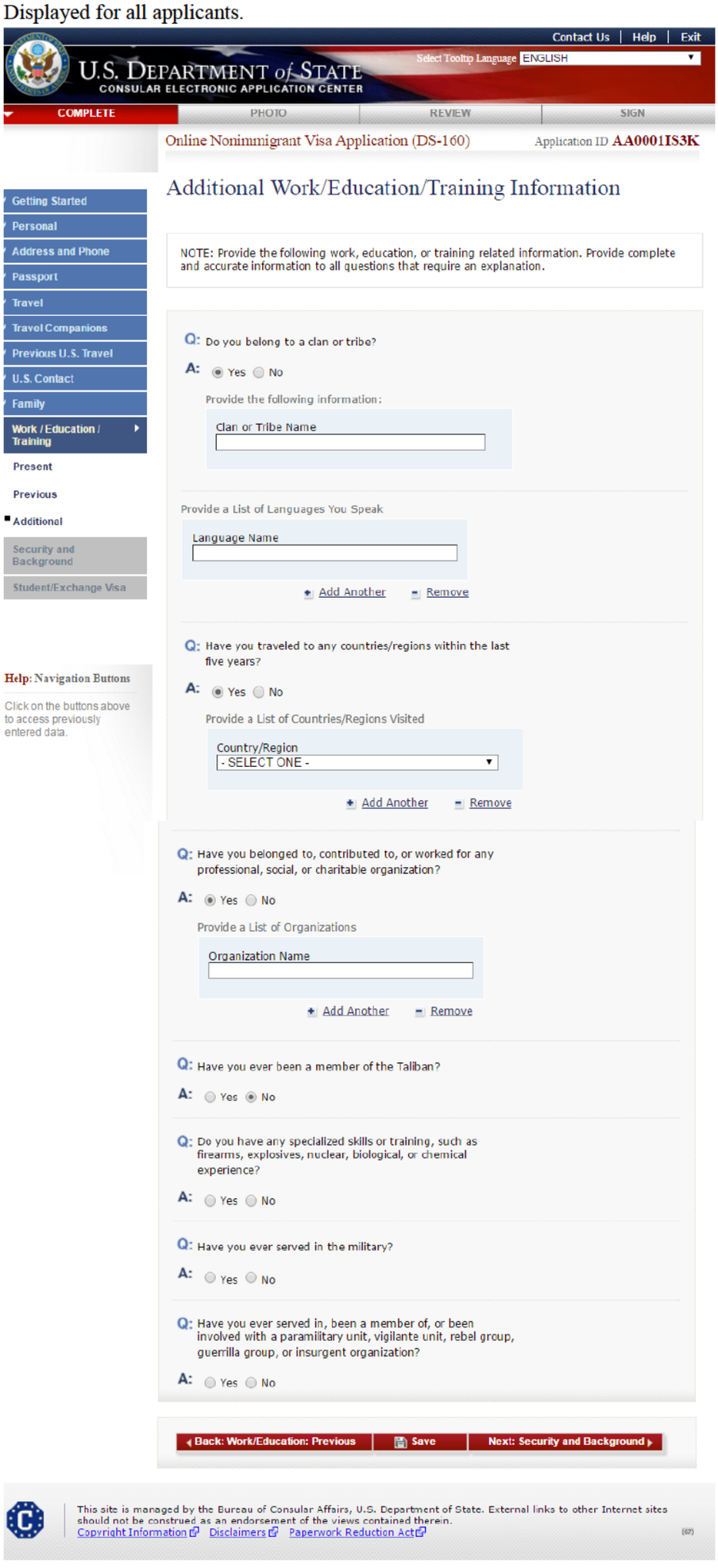
Previous Work/Education/Traning Information

Displayed for all applicants.



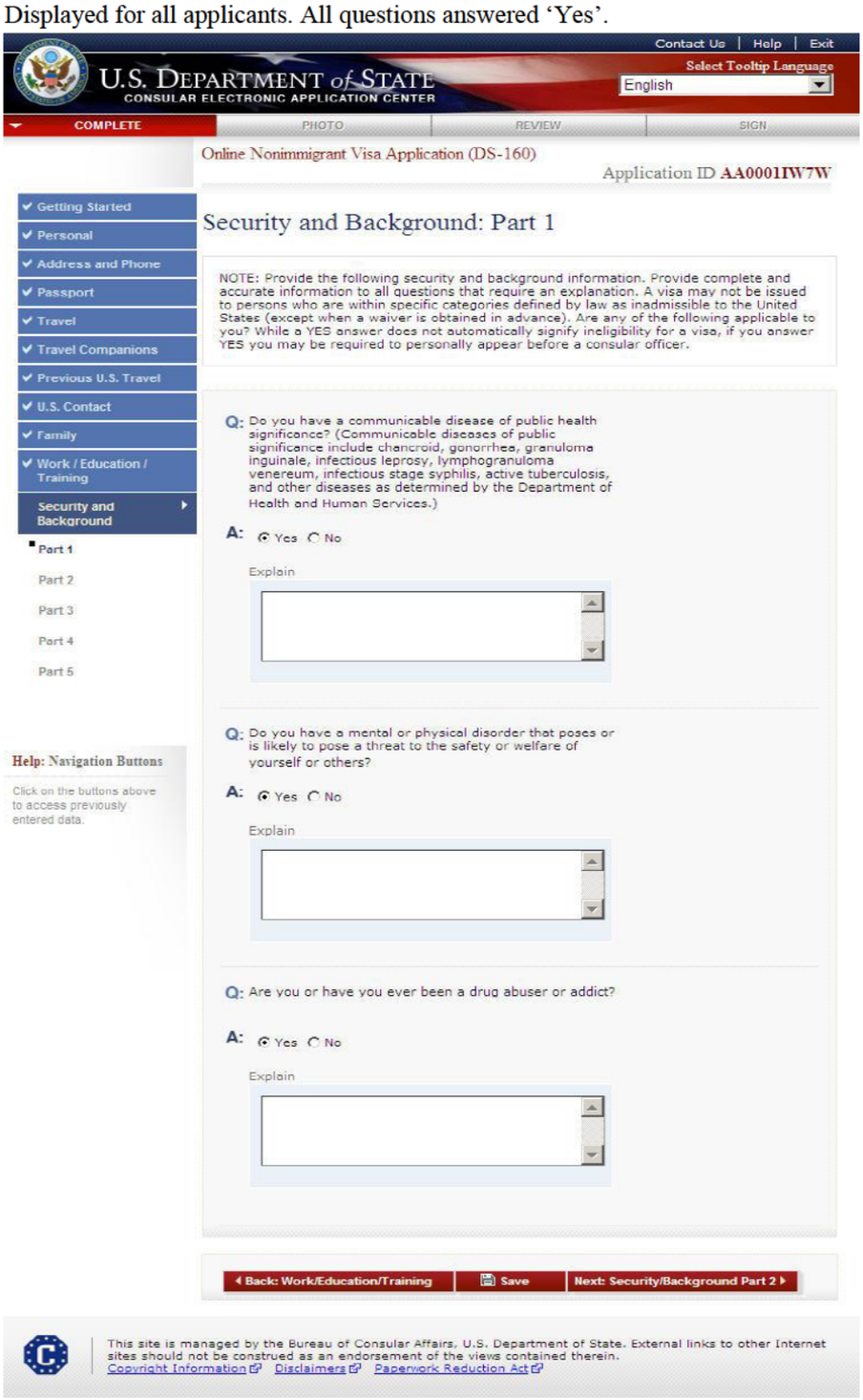
Additional Work/Education/Traning Information

Displayed for all applicants.



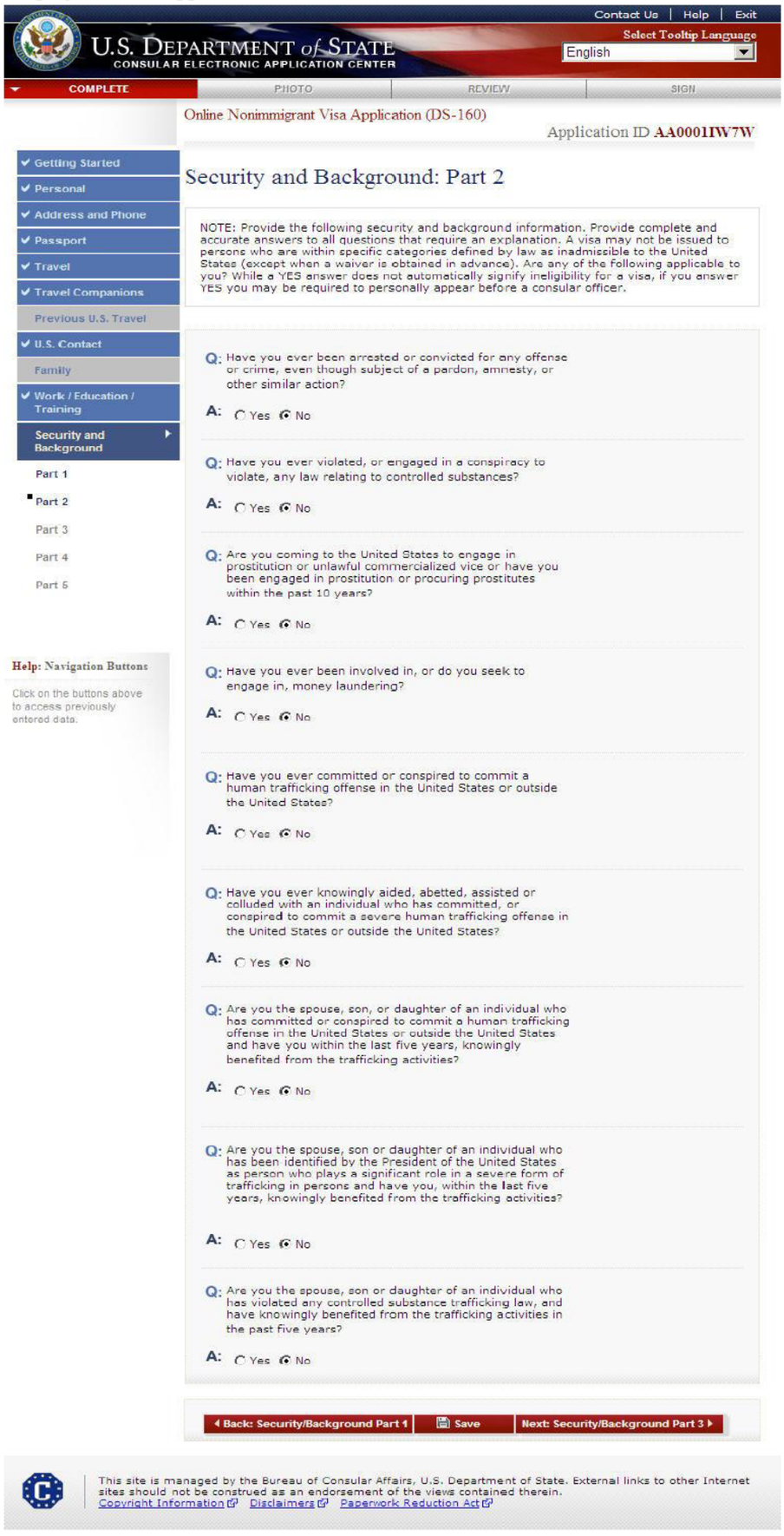
Security and Background: Part 1

Displayed for all applicants. All questions answered 'Yes'.



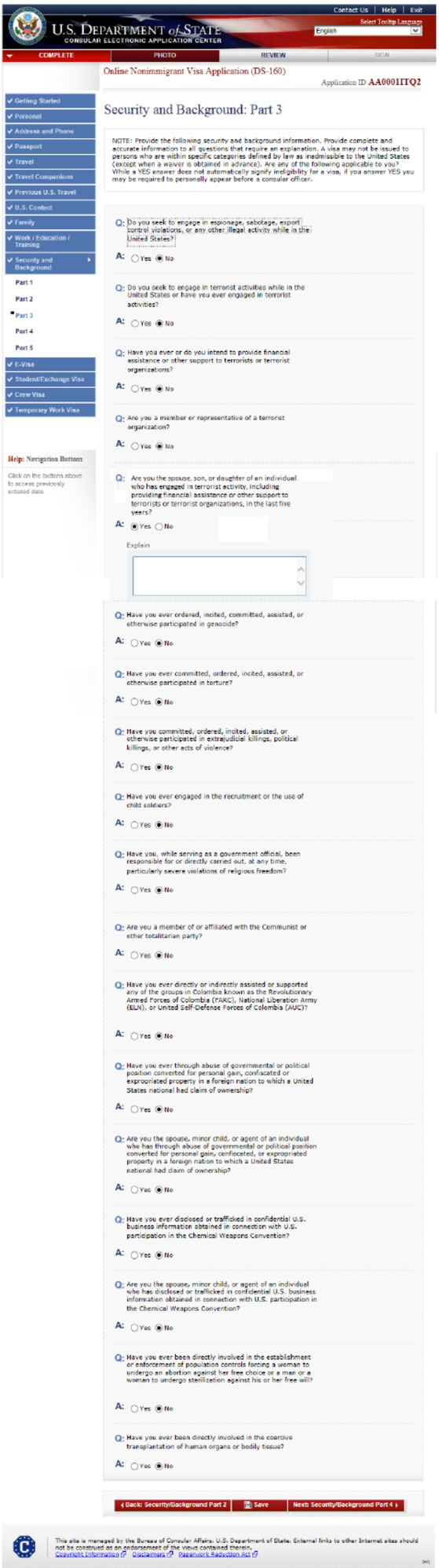
Security and Background: Part 2

Displayed for all applicants.



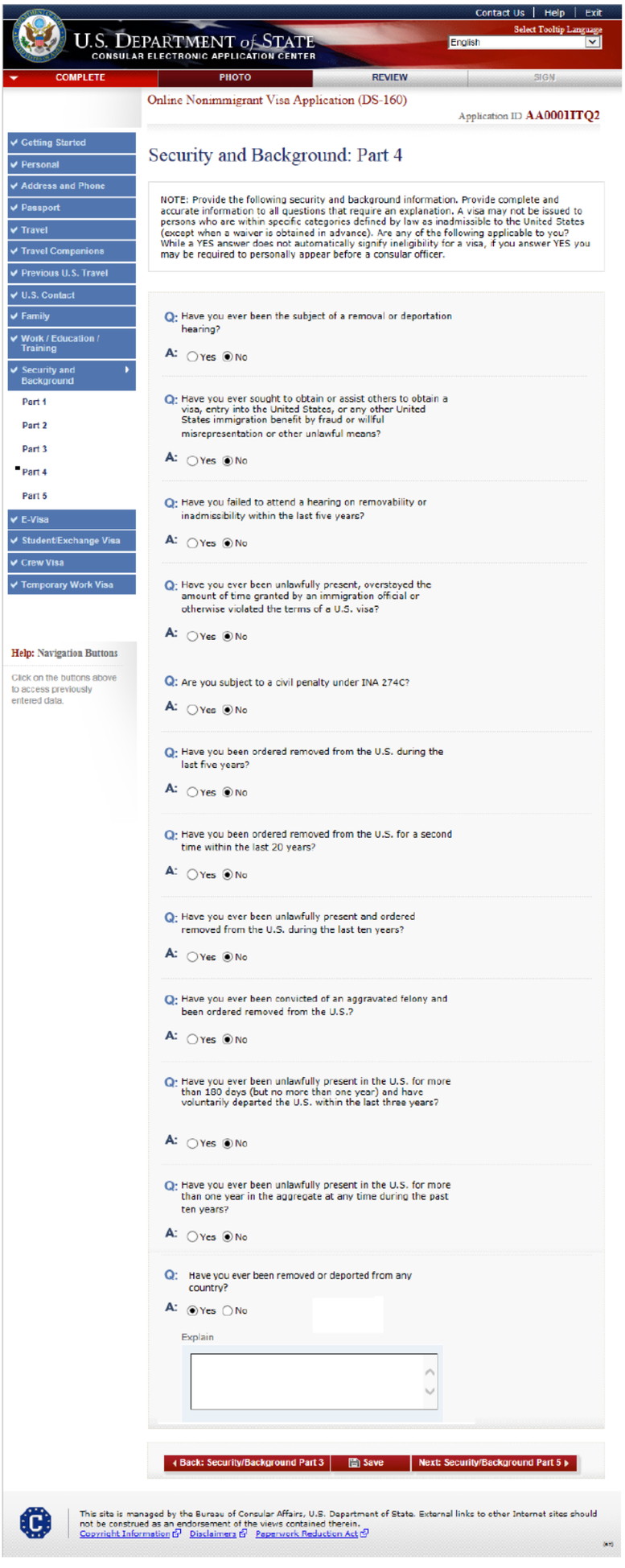
Security and Background: Part 3

Displayed for all applicants.



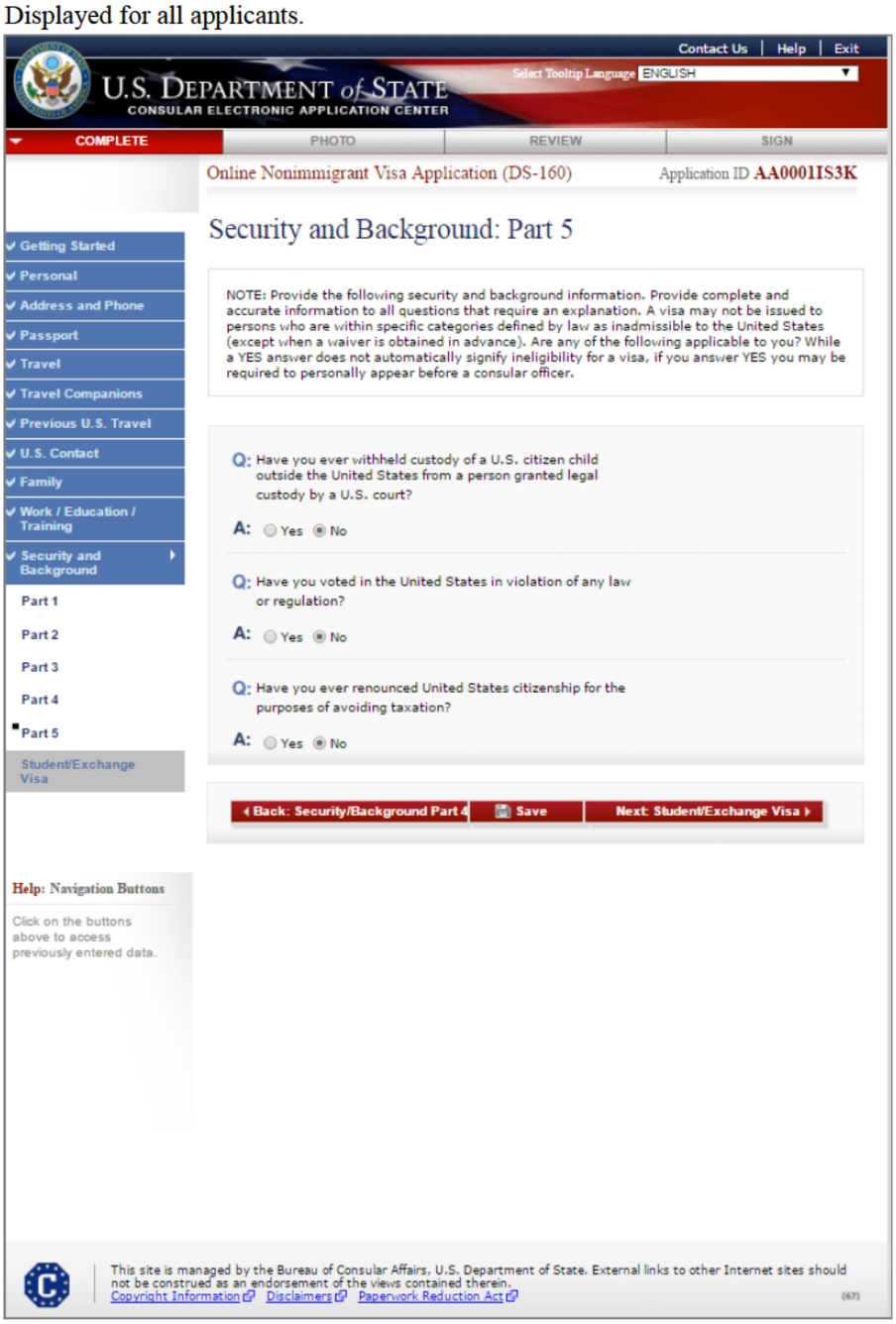
Security and Background: Part 4

Displayed for all applicants.



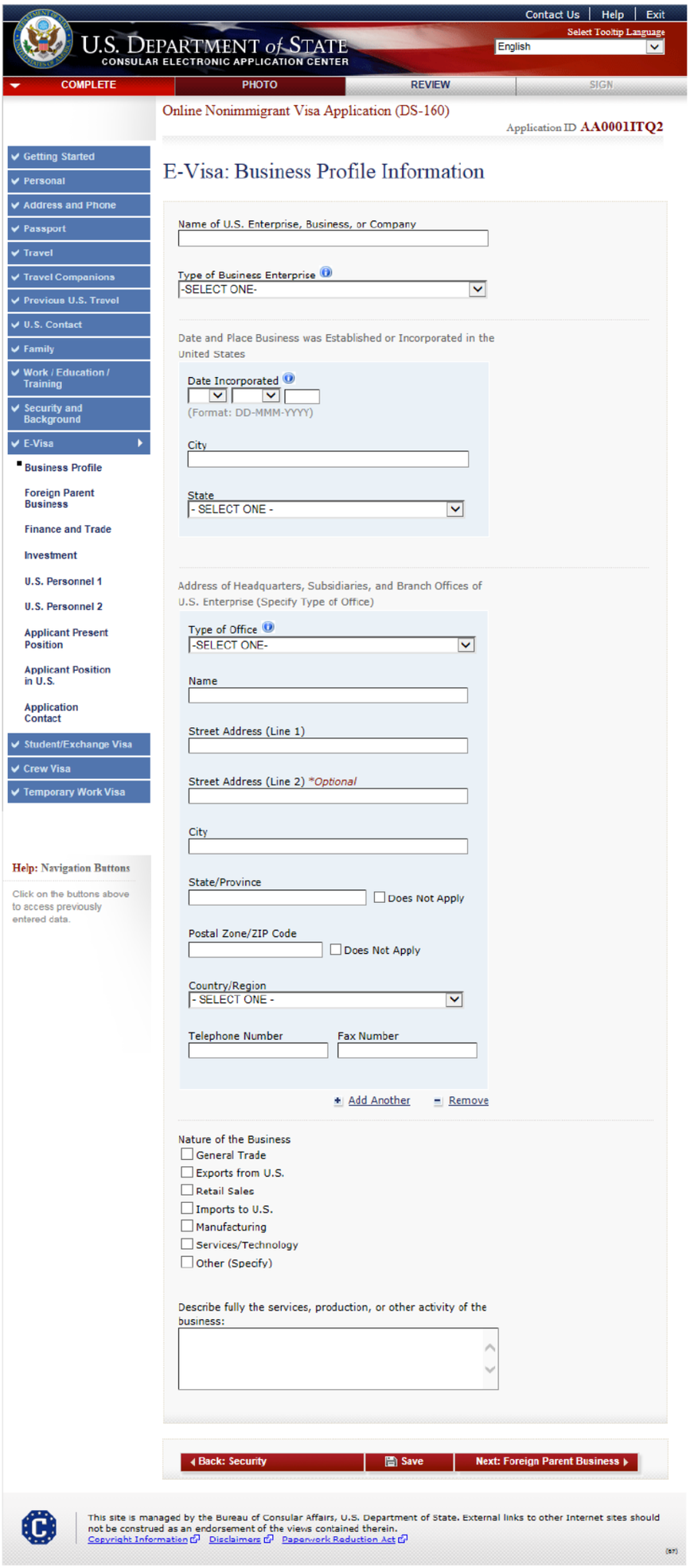
Security and Background: Part 5

Displayed for all applicants.



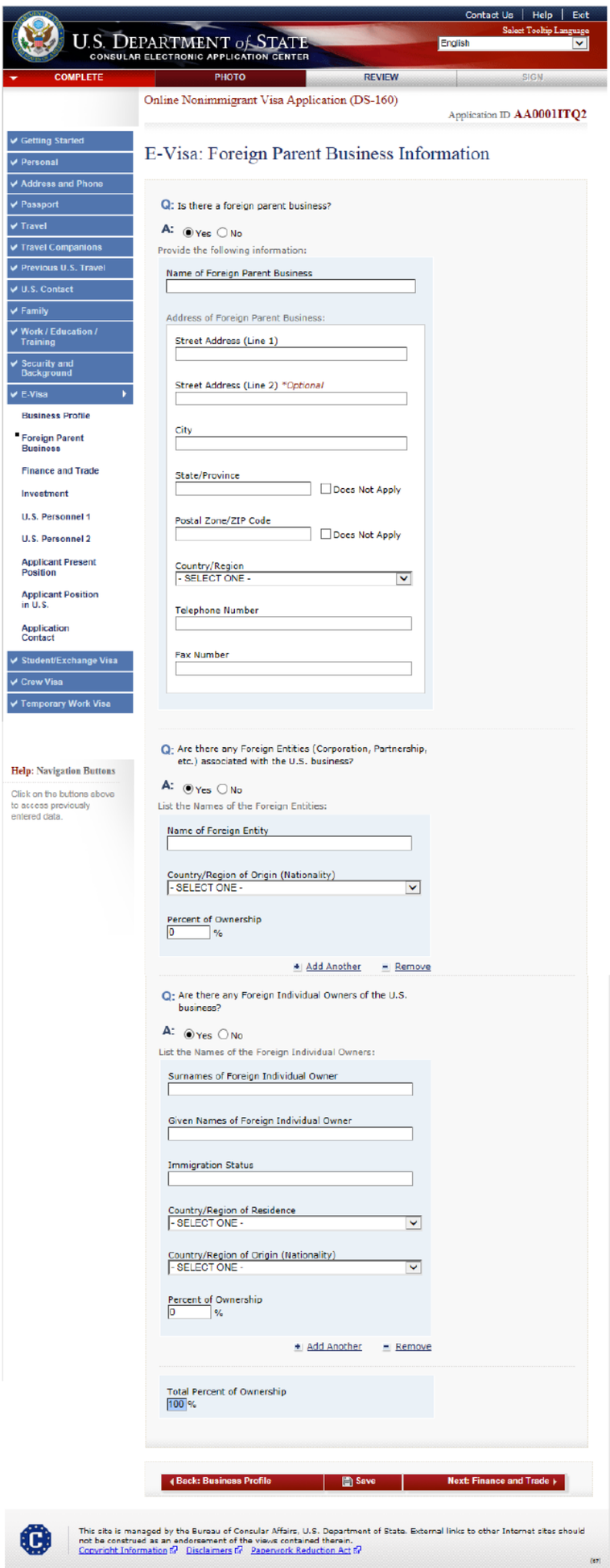
E-Visa: Business Profile

Displayed for applicants who selected the following E-Visa types: E1-TR, E2-TR, and E1-EXs who indicate they are without an E1-TR.



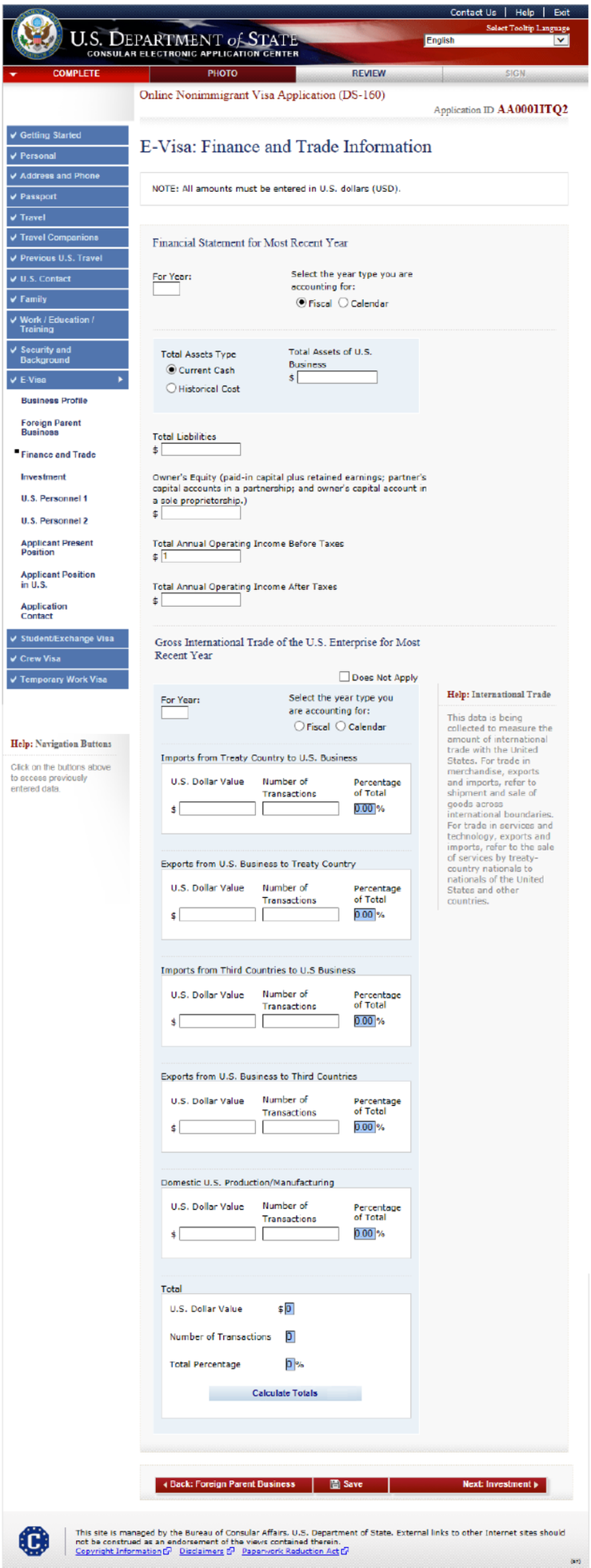
E-Visa: Foreign Parent Business

Displayed for applicants who selected the following E-Visa types: E1-TR, E2-TR, and E1-EXs who indicate they are without an E1-TR.



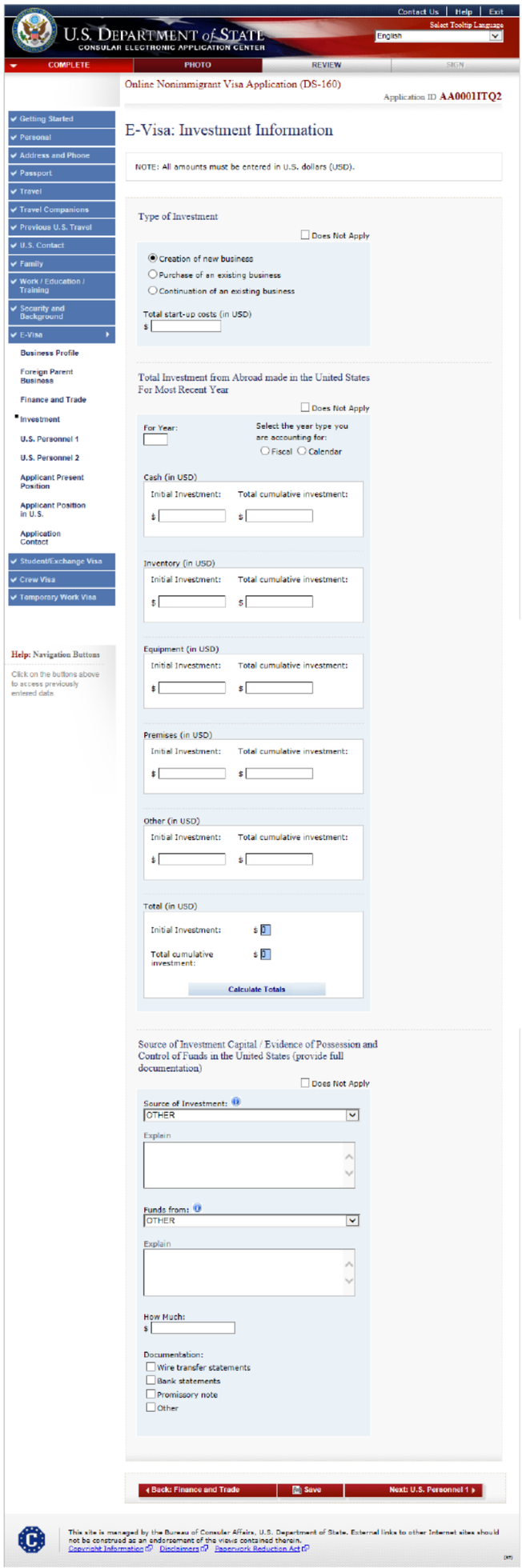
E-Visa: Finance and Trade

Displayed for applicants who selected the following E-Visa types: E1-TR and E1-EXs who indicate they are without an E1-TR.



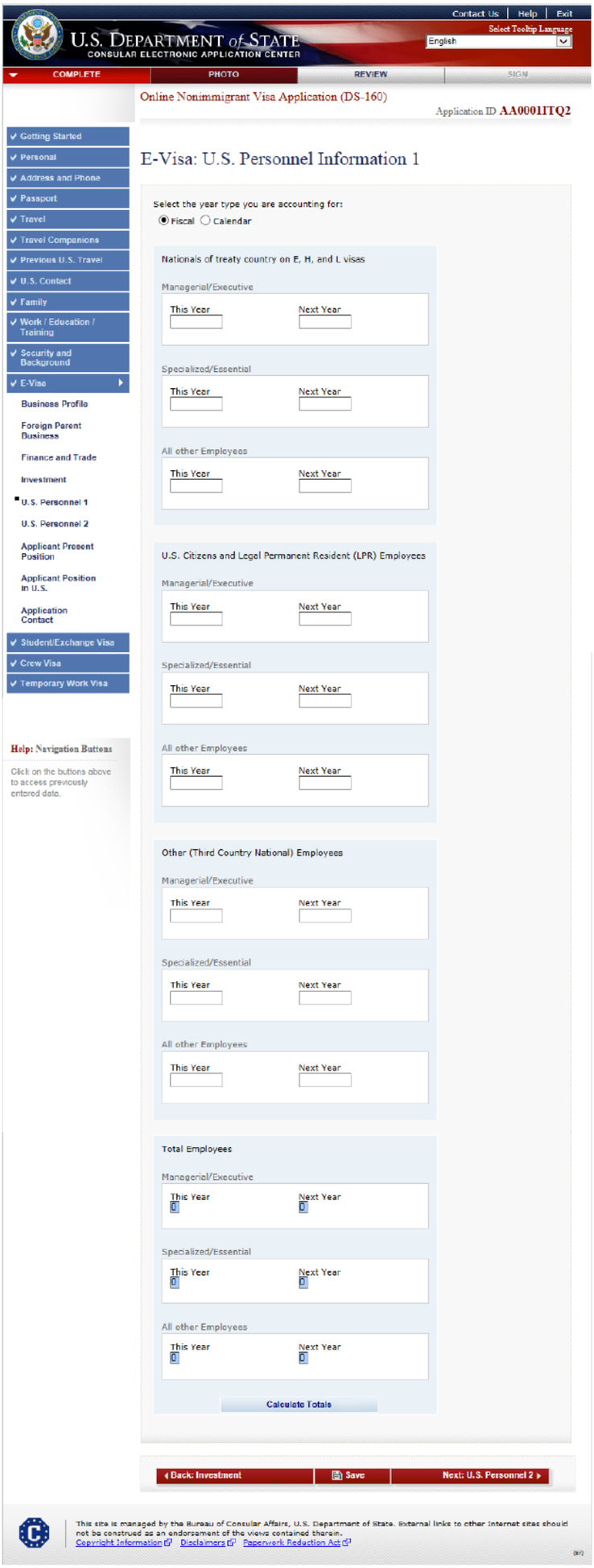
E-Visa: Investment

Displayed for E2-TR – Treaty Investors.



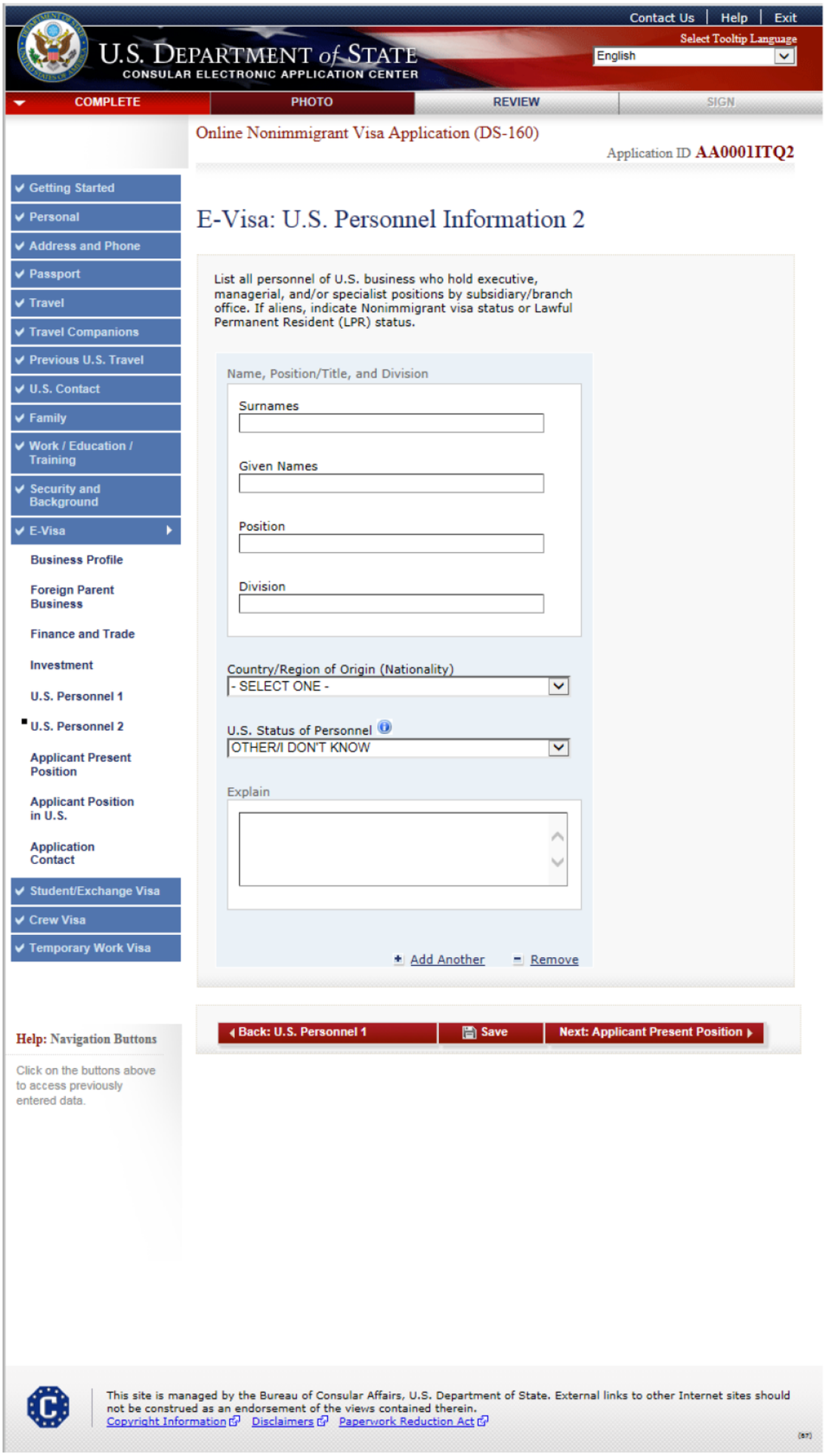
E-Visa: U.S. Personnel 1

Displayed for applicants who selected the following E-Visa types: E1-TR, E2-TR, and E1-EXs who indicate they are without an E1-TR.



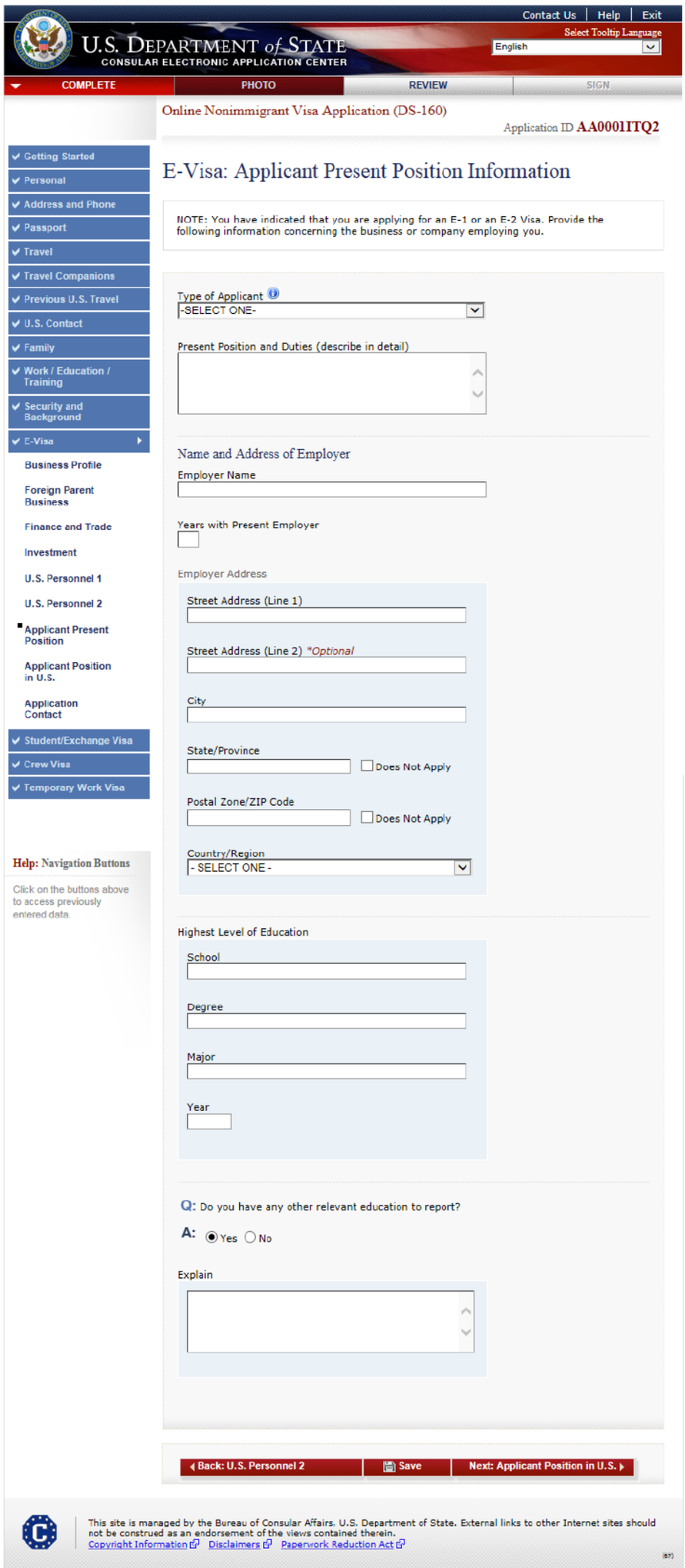
E-Visa: U.S. Personnel 2

Displayed for applicants who selected the following E-Visa types: E1-TR, E2-TR, and E1-EXs who indicate they are without an E1-TR.



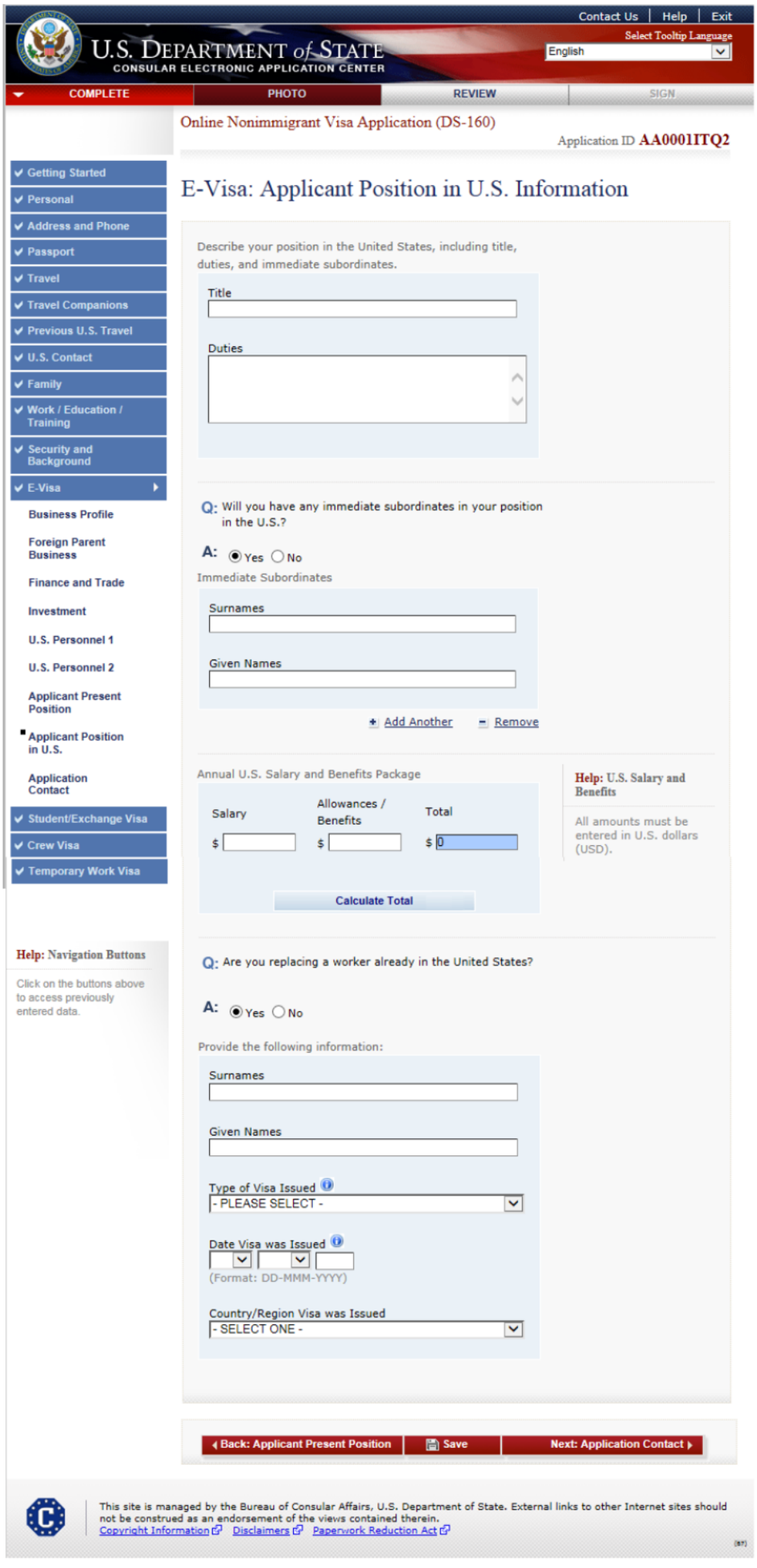
E-Visa: Applicant Present Position

Displayed for all principal E-Visa applicants.

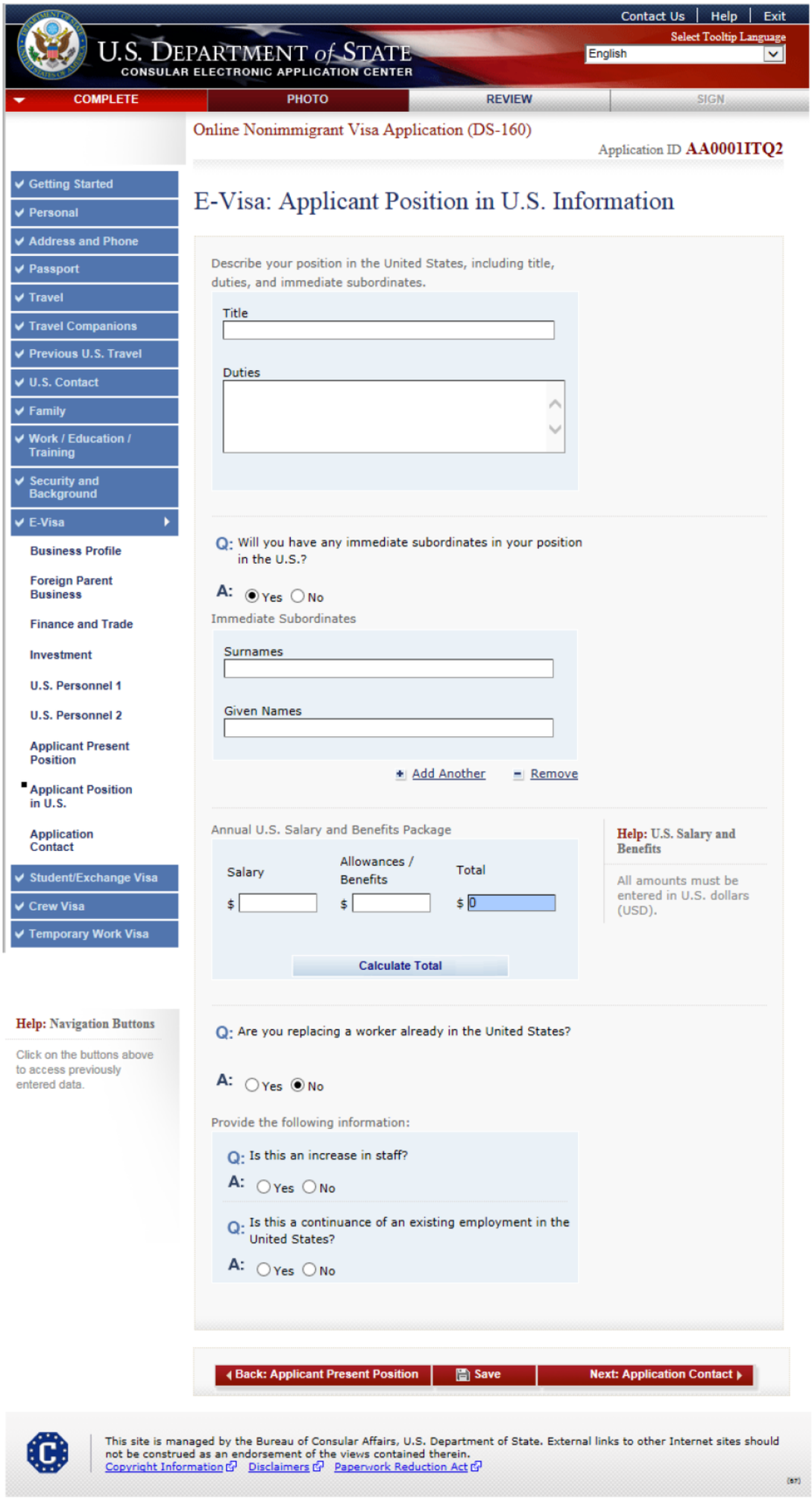


E-Visa: Applicant Position in U.S.

Displayed for all principal E-Visa applicants, replacing worker as "Yes."

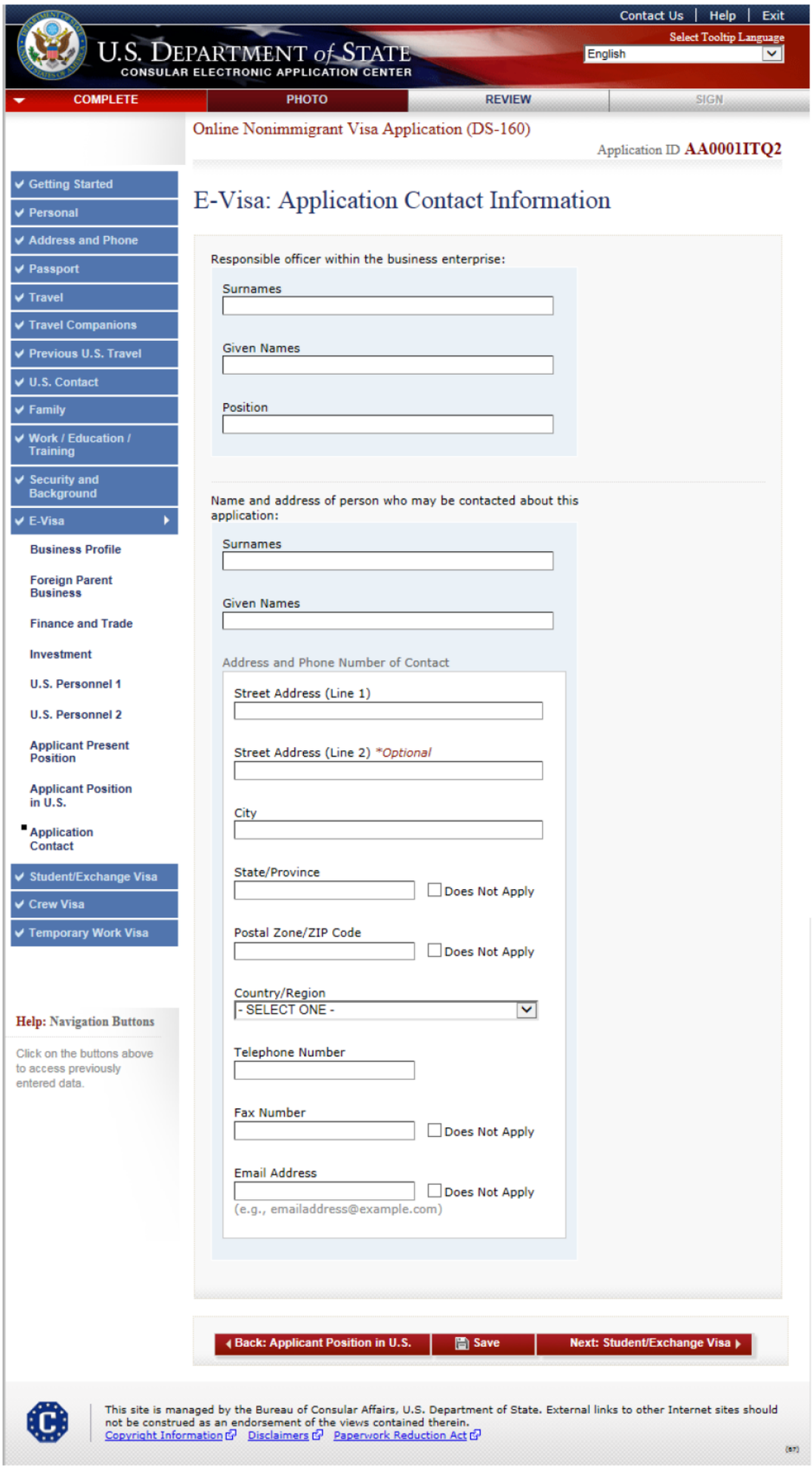


Replacing worker as "No."



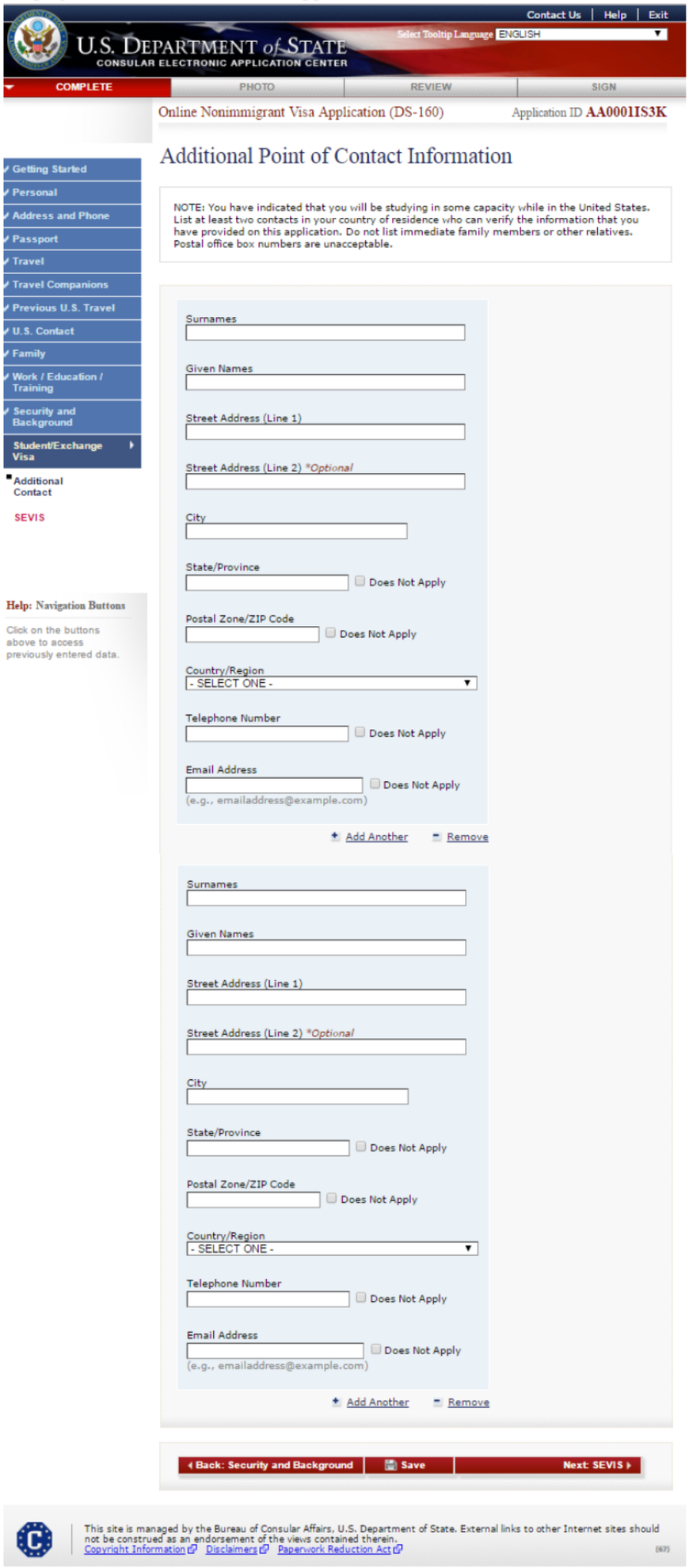
E-Visa: Application Contact

Displayed for all principal E-Visa applicants.



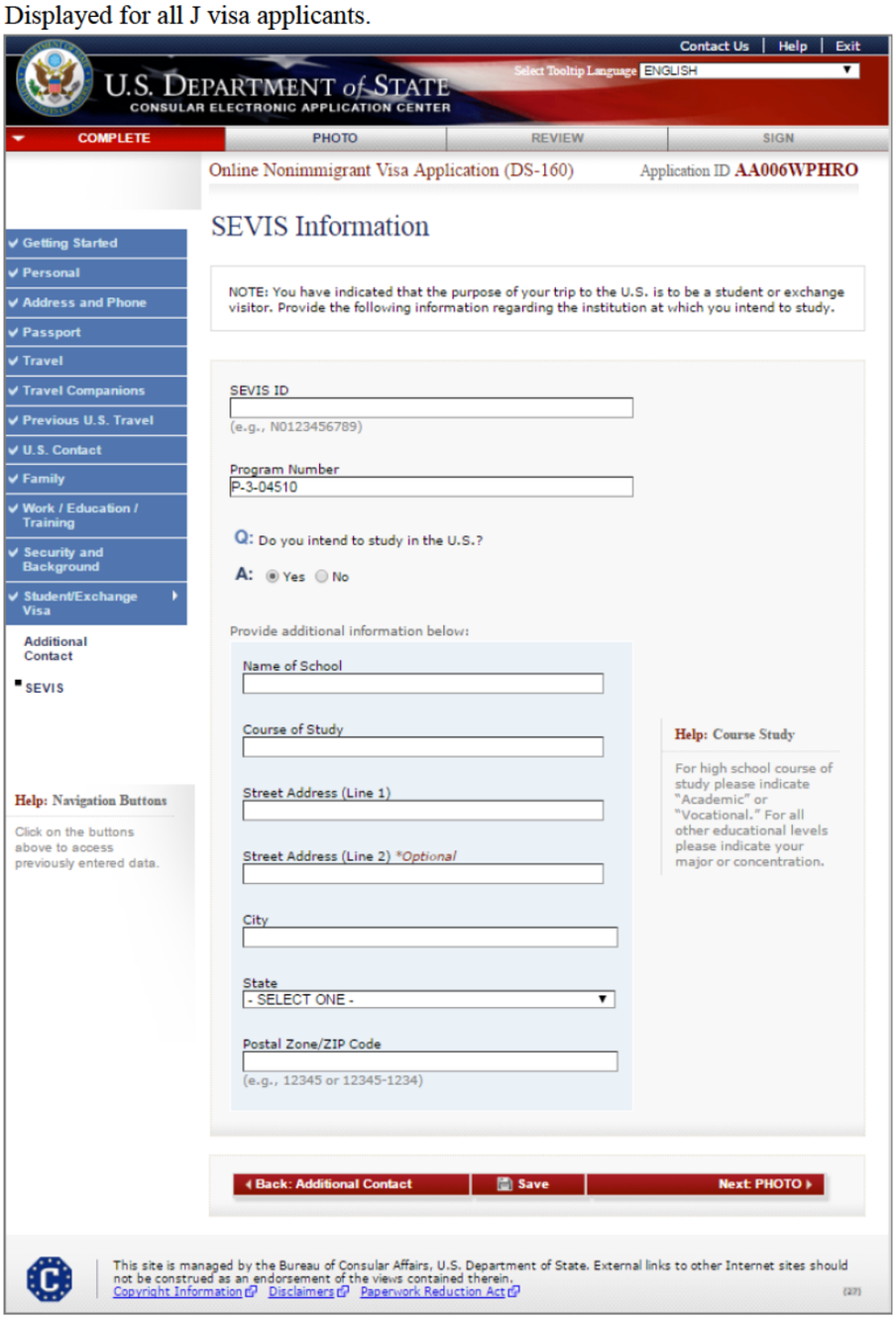
Additional Point of Contact

Displayed for all F, M, and J visa applicants.



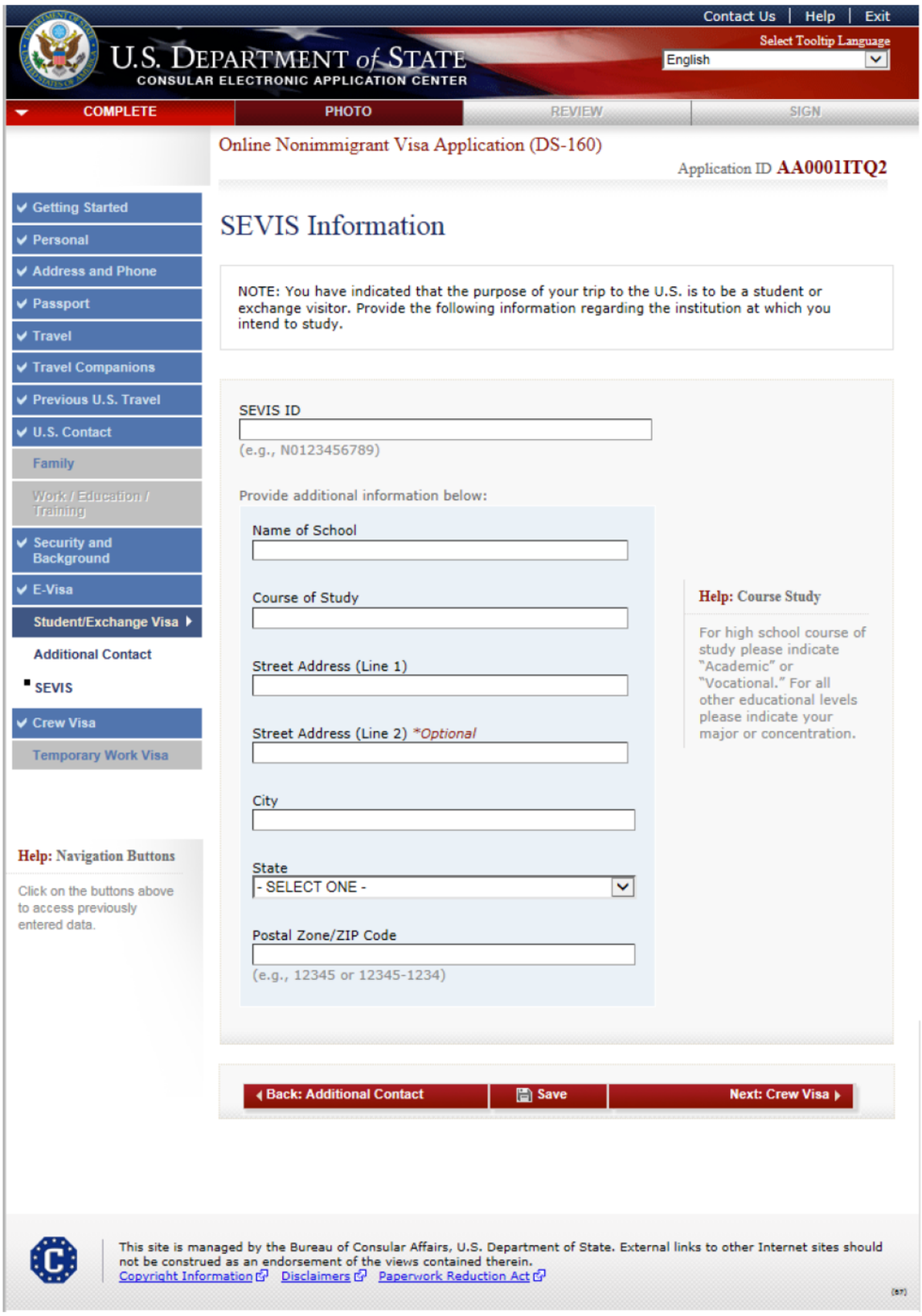
SEVIS Information

Displayed for all J visa applicants.



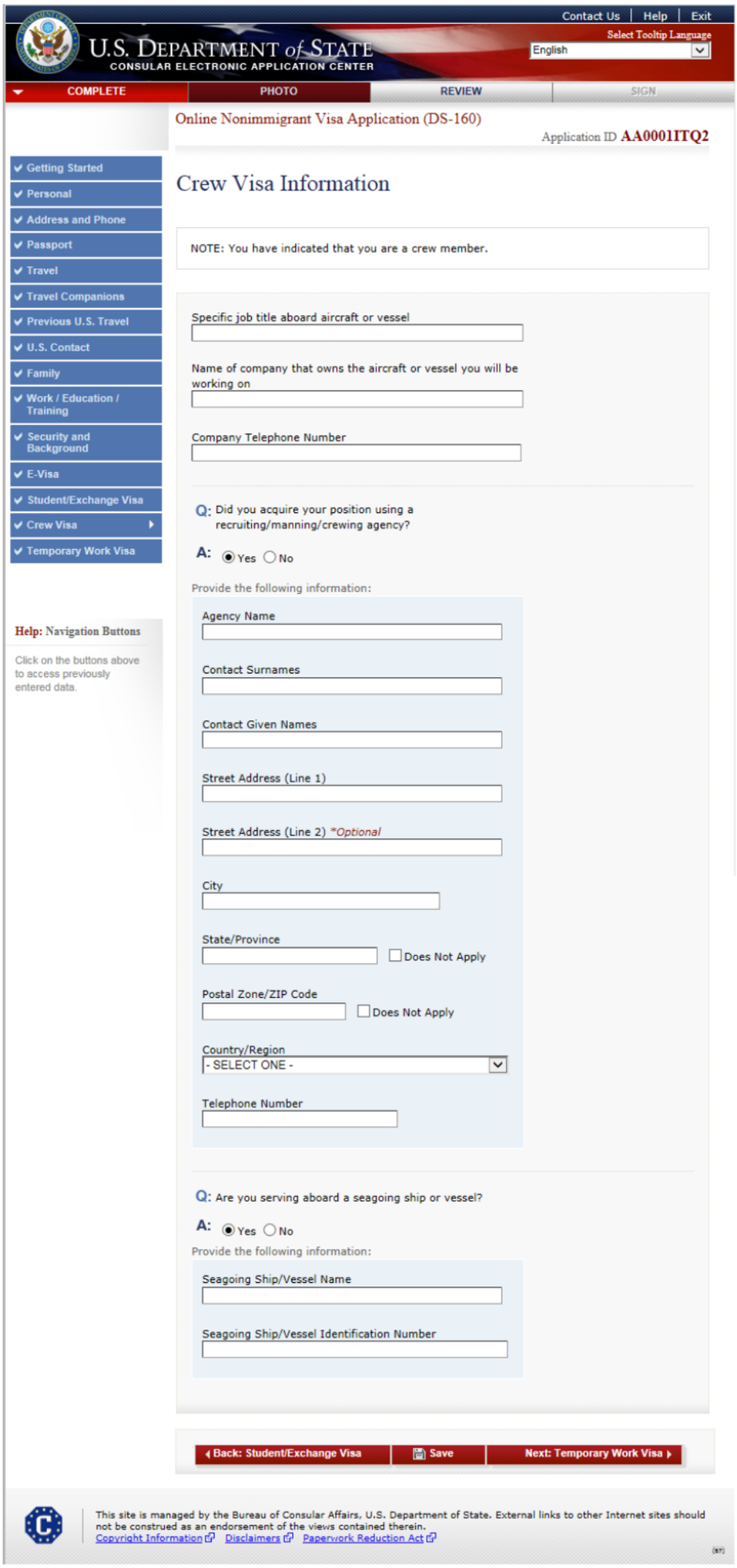
SEVIS Information

Displayed for all F and M visa applicants.



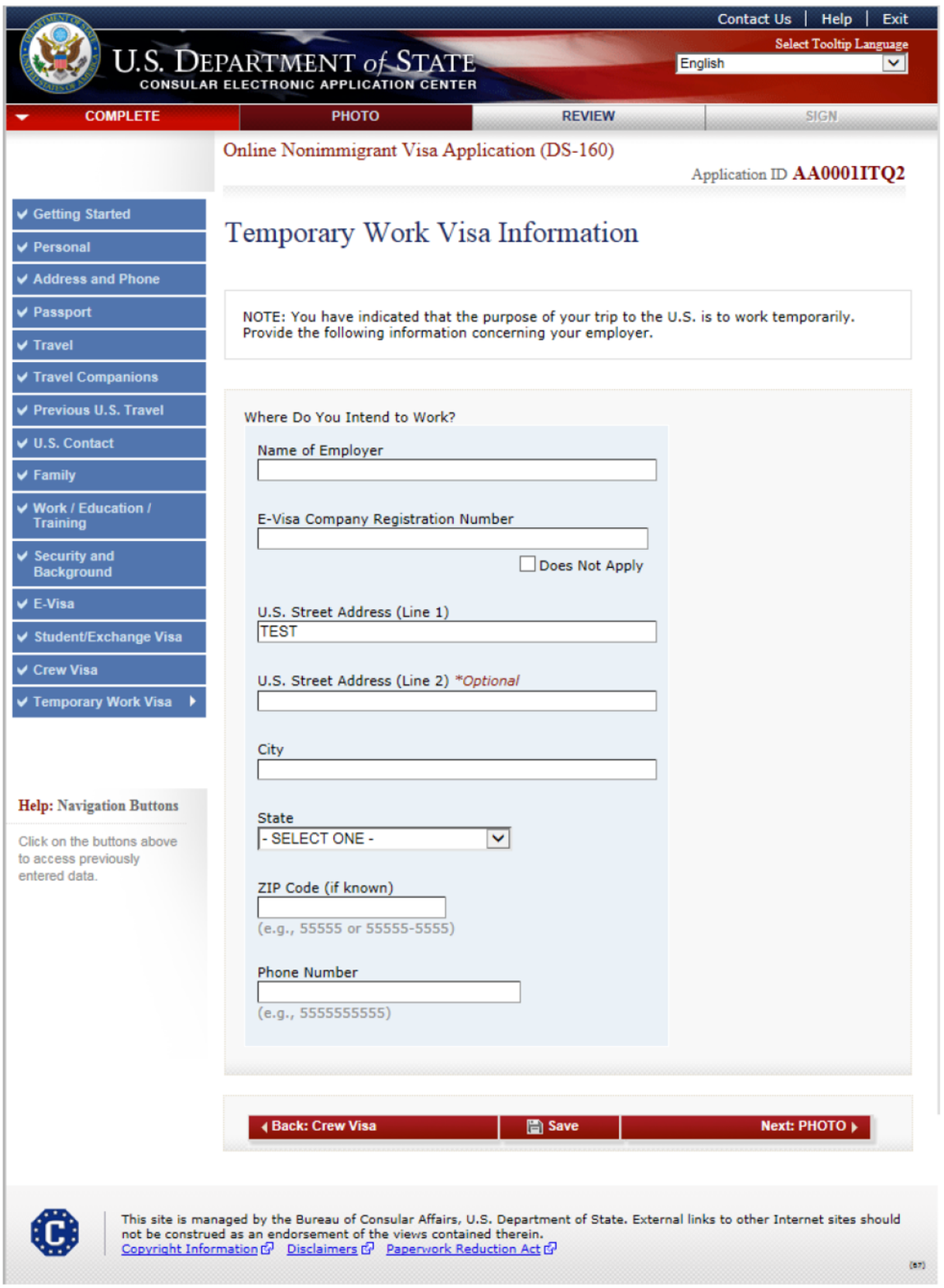
Crew Visa

Displayed for D-Visa applicants.



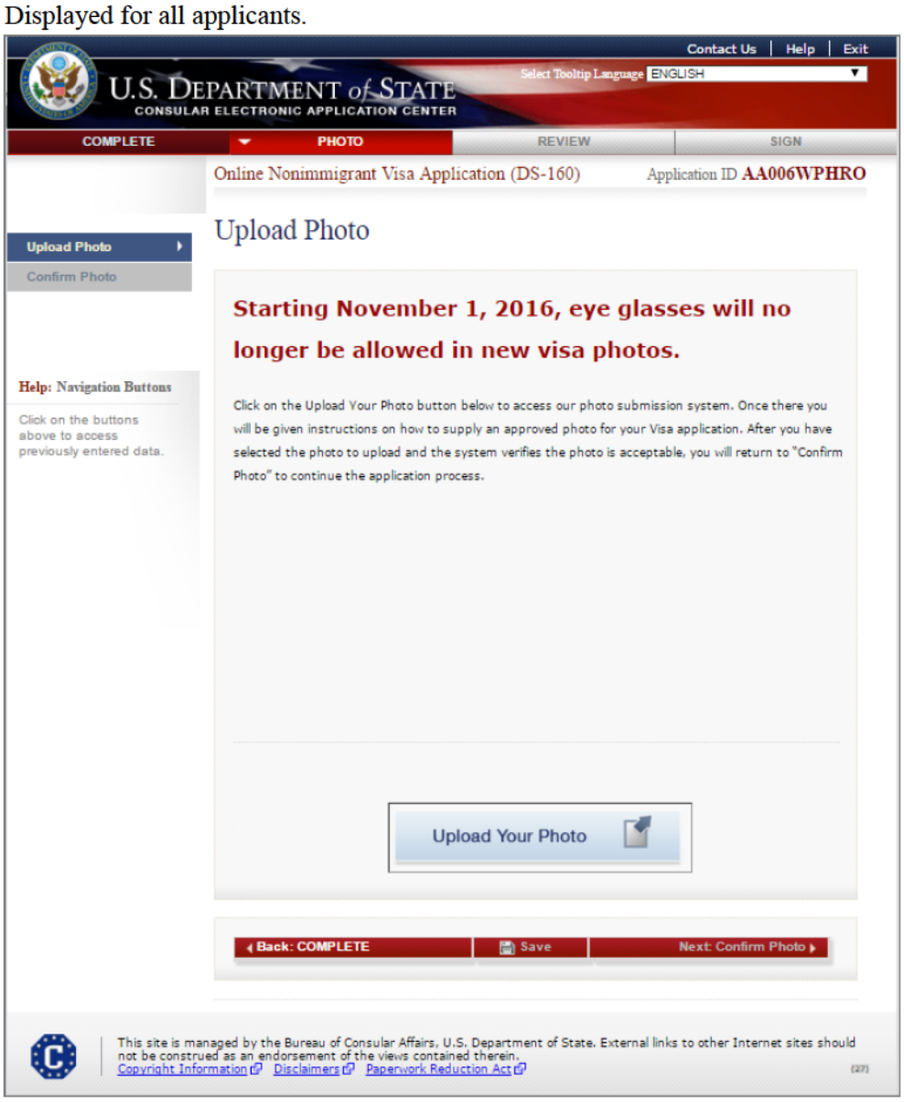
Temporary Work Visa

Displayed for the following Visa types: A3-EM, CW1-CW1, E1-EX, E1-TR, E2-EX, E2-TR, E2C-E2C, E3-AUS, E3R-RT, G5-EM, H1B-H1B, H1B1-CHL, H1B1-SGP, H1C-NR, H2A-AG, H2B-NA,H3-TR, I-FR, L1-L1, NATO7-EM, O1-EX, O2-AL, P1-P1, P2-P2, P3-P3, Q1-Q1, R1-R1, and TN-TN.

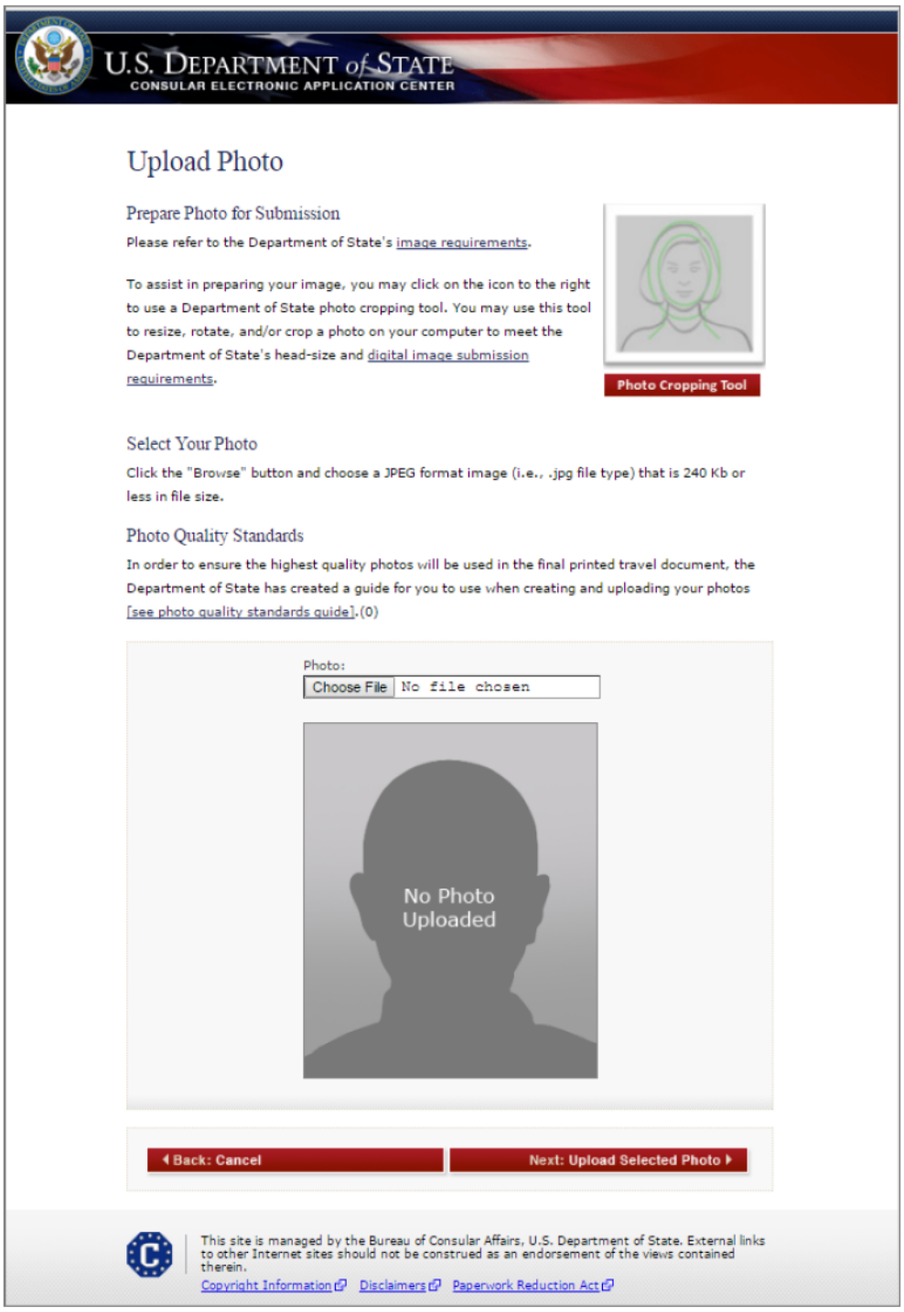


Upload Photo

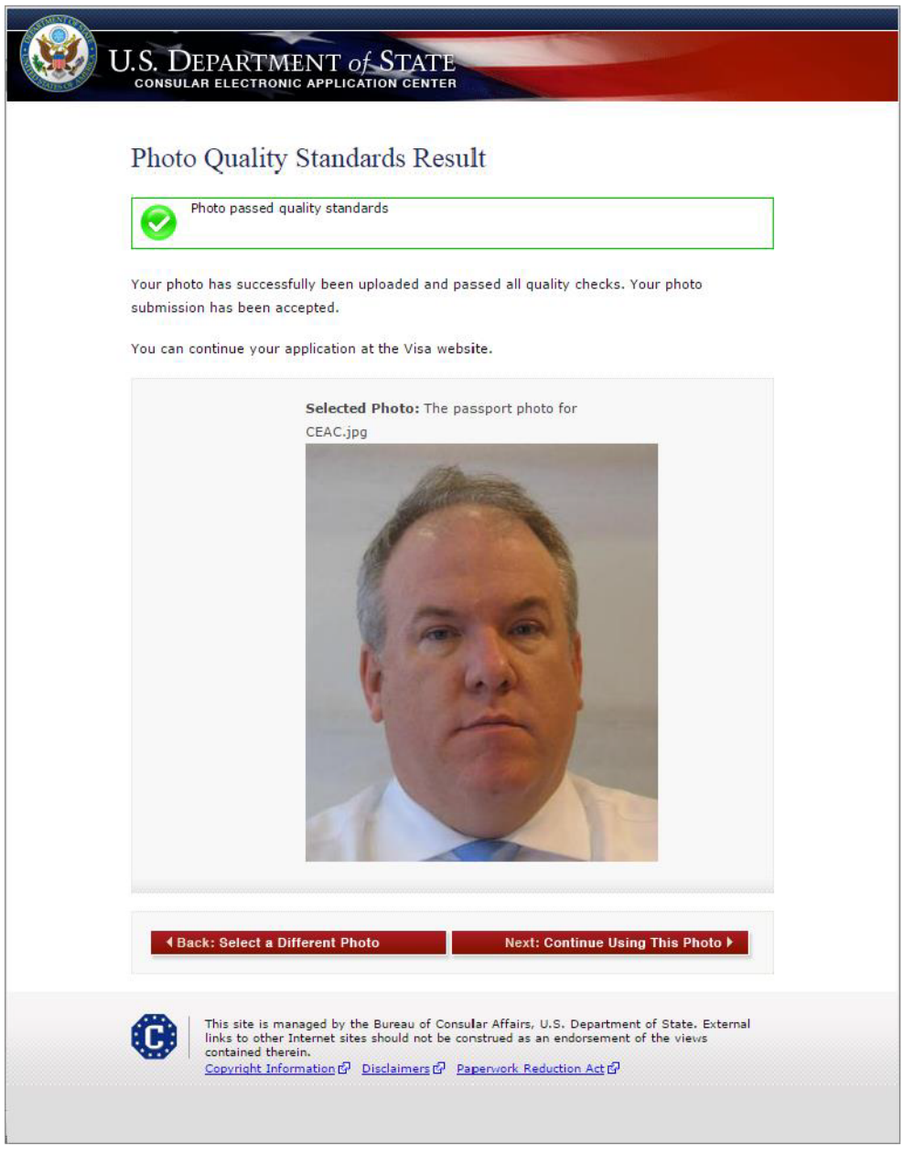
Displayed for all applicants.



Upload Photo (continued)



Upload Photo – Photo Quality Standards Result



U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Photo Quality Standards Result

Photo passed quality standards

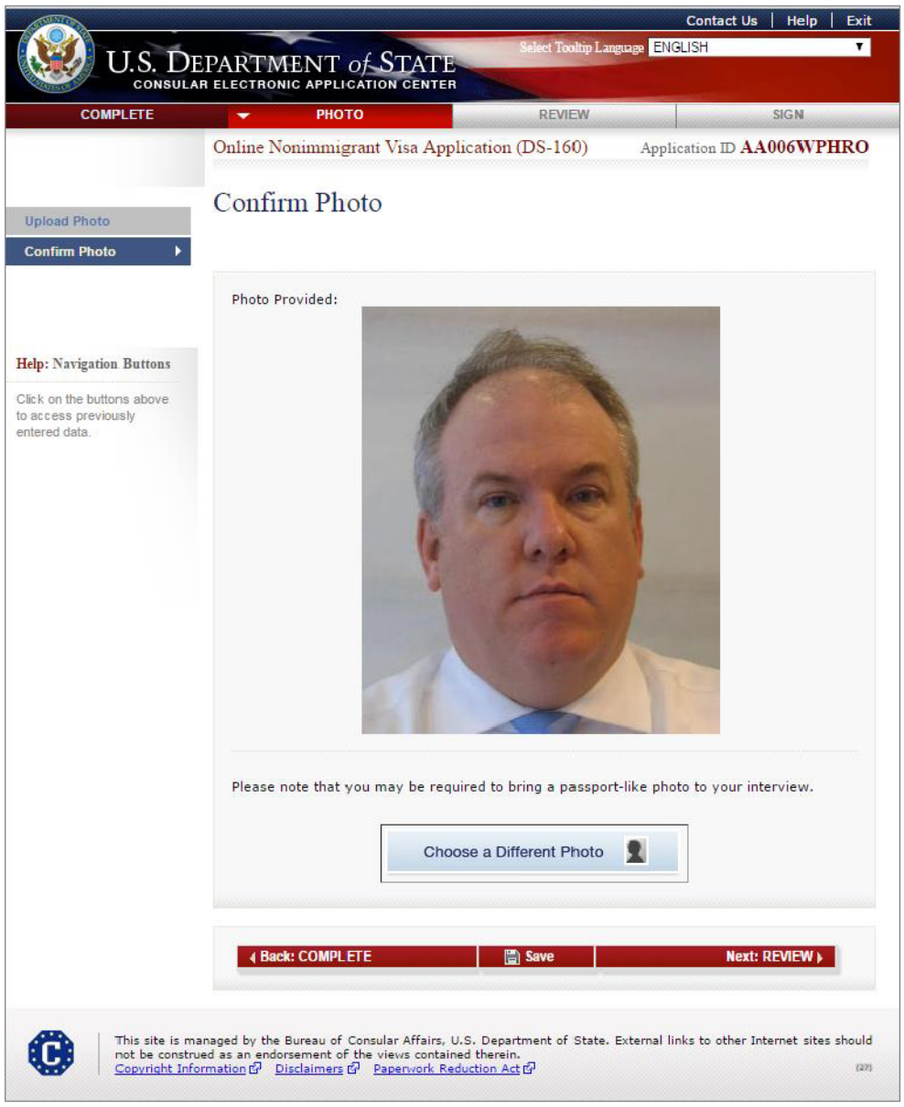
Your photo has successfully been uploaded and passed all quality checks. Your photo submission has been accepted.

You can continue your application at the Visa website.

Selected Photo: The passport photo for CEAC.jpg

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information Disclaimers Paperwork Reduction Act

Upload Photo (continued)



Application Review

Displayed for all applicants.



Contact Us | Help | Exit

U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Select Tooltip Language: ENGLISH

COMPLETE | PHOTO | REVIEW | SIGN

Online Nonimmigrant Visa Application (DS-160) Application ID AA006WPHRO

Personal/Address/ Phone/Passport
Travel
U.S. Contact
Family
Work/Education/ Training
Security and Background
Student/Exchange Visa
Location

Help: Navigation Buttons

Click on the buttons above to access previously entered data.

Personal, Address, Phone, and Passport Information

Note: You have completed data entry for your NIV application. Before submitting the application, please review your entries below. To navigate to the next section to be reviewed, click the 'Next' button on the bottom of the page. If an entry is incorrect, click on the links on the right side of the page, which will direct you to the page where you entered the data. Once you have reviewed all sections, you will be directed to the Sign and Submit page to complete the application process.

Print

Photo Provided: Upload New Photo

Edit Personal Information

Name Provided:	SNOW, JOHN
Full Name in Native Alphabet:	DOES NOT APPLY
Other Names Used:	NO
Telecode Name Used:	NO
Sex:	MALE
Marital Status:	MARRIED
Date of Birth:	01 JANUARY 1980
Country/Region of Birth:	KABUL, AFGHANISTAN
Country/Region of Origin (Nationality):	AFGHANISTAN
Do you hold or have you held any nationality other than the one indicated above on nationality?	NO
Are you a permanent resident of a country/region other than your country/region of origin (nationality) above?	NO
National Identification Number:	DOES NOT APPLY
U.S. Social Security Number:	DOES NOT APPLY
U.S. Taxpayer ID Number:	DOES NOT APPLY

Edit Address and Phone Information

Home Address:	1234 KABUL LANE
City:	KABUL
State/Province:	DOES NOT APPLY
Postal Zone/ZIP Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Same Mailing Address?	YES
Primary Phone Number:	1111111111111111111
Secondary Phone Number:	DOES NOT APPLY
Work Phone Number:	DOES NOT APPLY
Email Address:	snow@gmail.com

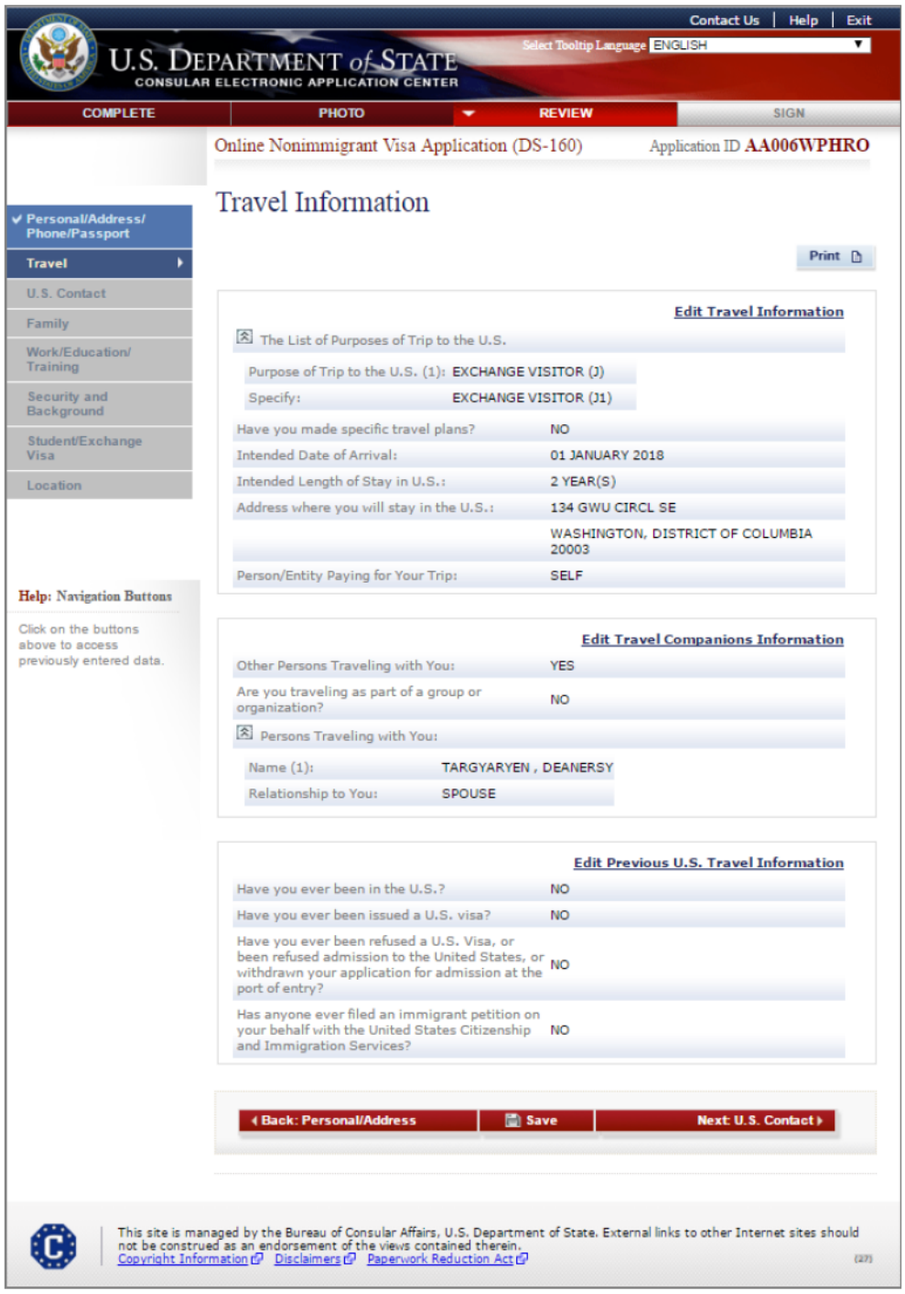
Edit Passport/Travel Document Information

Passport/Travel Document Type:	REGULAR
Passport/Travel Document Number:	M2111111111111111111
Passport Book Number:	DOES NOT APPLY
Country/Authority that Issued Passport/Travel Document:	AFGHANISTAN
City where issued:	KABUL
Country/Region where issued:	AFGHANISTAN
Issuance Date:	01 JANUARY 2016
Expiration Date:	01 JANUARY 2026
Have you ever lost a passport or had one stolen?	NO

Back: | Save | Next: Travel

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information Disclaimers Paperwork Reduction Act

Application Review (continued)



Contact Us | Help | Exit

U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Select Tooltip Language: ENGLISH

COMPLETE | PHOTO | REVIEW | SIGN

Online Nonimmigrant Visa Application (DS-160) Application ID AA006WPHRO

- Personal/Address/ Phone/Passport
- Travel
- U.S. Contact
- Family
- Work/Education/ Training
- Security and Background
- Student/Exchange Visa
- Location

Help: Navigation Buttons

Click on the buttons above to access previously entered data.

Travel Information

Print

Edit Travel Information

The List of Purposes of Trip to the U.S.

Purpose of Trip to the U.S. (1):	EXCHANGE VISITOR (J)
Specify:	EXCHANGE VISITOR (J1)
Have you made specific travel plans?	NO
Intended Date of Arrival:	01 JANUARY 2018
Intended Length of Stay in U.S.:	2 YEAR(S)
Address where you will stay in the U.S.:	134 GWU CIRCL SE WASHINGTON, DISTRICT OF COLUMBIA 20003
Person/Entity Paying for Your Trip:	SELF

Edit Travel Companions Information

Other Persons Traveling with You:	YES
Are you traveling as part of a group or organization?	NO

Persons Traveling with You:

Name (1):	TARGYARYEN , DEANERSY
Relationship to You:	SPOUSE

Edit Previous U.S. Travel Information

Have you ever been in the U.S.?	NO
Have you ever been issued a U.S. visa?	NO
Have you ever been refused a U.S. Visa, or been refused admission to the United States, or withdrawn your application for admission at the port of entry?	NO
Has anyone ever filed an immigrant petition on your behalf with the United States Citizenship and Immigration Services?	NO

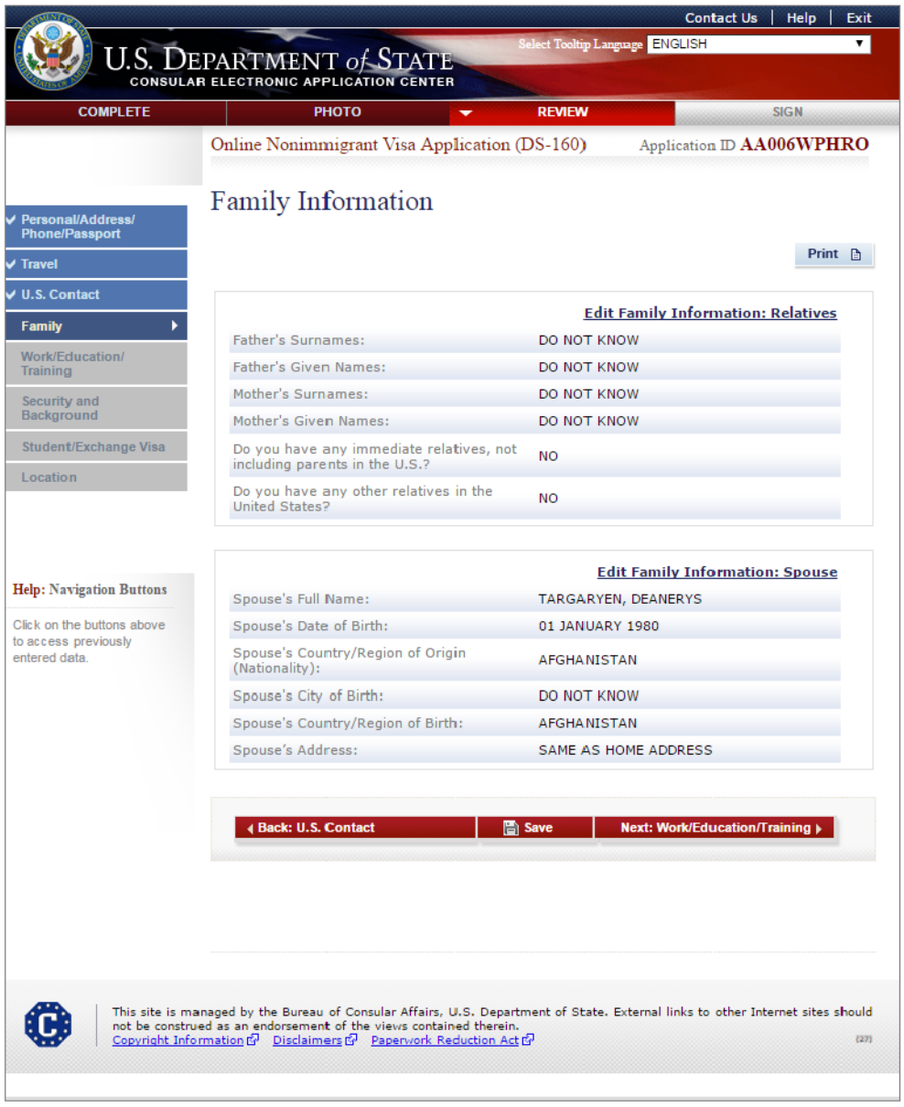
Back: Personal/Address | Save | Next: U.S. Contact

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information Disclaimers Paperwork Reduction Act

Application Review (continued)



Application Review (continued)



Application Review (continued)



Contact Us | Help | Exit

U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Select Tooltip Language: English

COMPLETE | PHOTO | REVIEW | SIGN

Online Nonimmigrant Visa Application (DS-160)

Application ID AA0001ITQ2

- Personal/Address/ Phone/Passport
- Travel
- U.S. Contact
- Family
- Work/Education/ Training
- Security and Background
- E-Visa
- Student/Exchange Visa
- Crew Visa
- Temporary Work Visa
- Location

Help: Navigation Buttons

Click on the buttons above to access previously entered data.

Work / Education / Training Information

Print

Edit Present Work Information

Primary Occupation:	EDUCATION
Present Employer or School Name:	TEST
Present Employer or School Address:	TEST
City:	TEST
State/Province:	DOES NOT APPLY
Postal Zone/Zip Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Start Date:	01 JANUARY 2010
Work Phone Number:	1234567890
Monthly Salary in Local Currency (if employed):	DOES NOT APPLY
Briefly Describe your Duties:	TEST

Edit Previous Work Information

Were you previously employed?	YES
Employer Name (1):	TEST
Employer Address:	TEST
City:	TEST
State/Province:	DOES NOT APPLY
Postal Zone/Zip Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Telephone Number:	1234567890
Job Title:	TEST
Supervisor's Surname:	DO NOT KNOW
Supervisor's Given Name:	DO NOT KNOW
Employment Date From:	01 JANUARY 1975
Employment Date To:	01 JANUARY 1980
Briefly describe your duties:	TEST
Employer Name (2):	TEST
Employer Address:	TEST
City:	TEST
State/Province:	DOES NOT APPLY
Postal Zone/Zip Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Telephone Number:	123457890
Job Title:	TEST
Supervisor's Surname:	DO NOT KNOW
Supervisor's Given Name:	DO NOT KNOW
Employment Date From:	01 JANUARY 1975
Employment Date To:	01 JANUARY 1980
Briefly describe your duties:	TEST
Have you attended any educational institutions at a secondary level or above?	NO

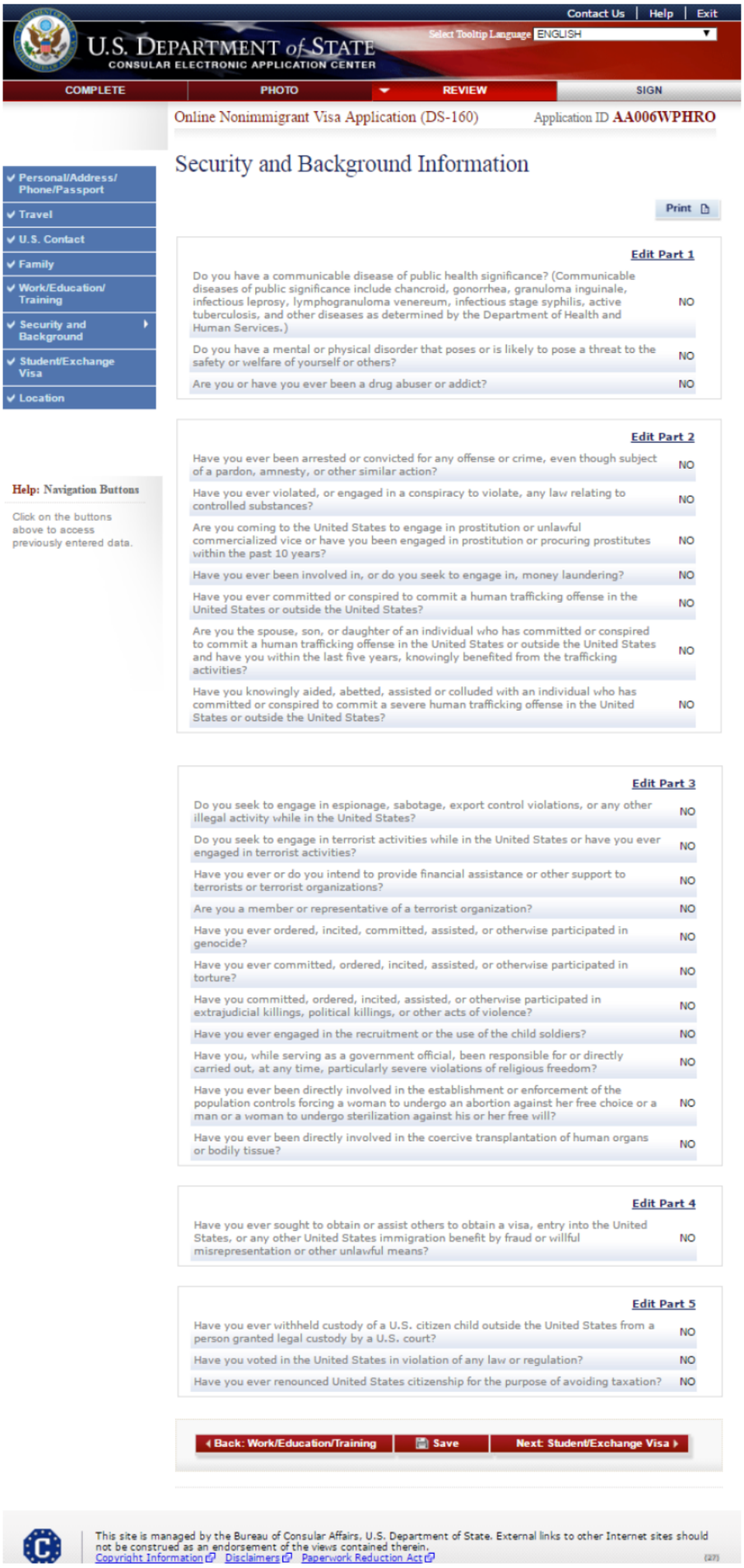
Edit Additional Information

Do you belong to a clan or tribe?	NO
Provide a List of Languages You Speak:	
Language Name (1):	TEST
Have you traveled to any countries/regions within the last five years?	NO
Have you resided in any country/region for six months or longer since you attained 16 years of age?	NO
Have you belonged to, contributed to, or worked for any professional, social, or charitable organization?	NO
Do you have any specialized skills or training, such as firearms, explosives, nuclear, biological, or chemical experience?	NO
Have you ever served in the military?	NO
Have you ever served in, been a member of, or been involved with a paramilitary unit, vigilante unit, rebel group, guerrilla group, or insurgent organization?	NO

◂ Back: Family | Save | Next: Security and Background ▸

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information | Disclaimers | Paperwork Reduction Act

Application Review (continued)



Contact Us | Help | Exit

U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Select Tooltip Language: ENGLISH

COMPLETE | PHOTO | REVIEW | SIGN

Online Nonimmigrant Visa Application (DS-160) Application ID AA006WPHRO

- Personal/Address/ Phone/Passport
- Travel
- U.S. Contact
- Family
- Work/Education/ Training
- Security and Background
- Student/Exchange Visa
- Location

Help: Navigation Buttons

Click on the buttons above to access previously entered data.

Security and Background Information

Print

Edit Part 1

Do you have a communicable disease of public health significance? (Communicable diseases of public significance include chancroid, gonorrhea, granuloma inguinale, infectious leprosy, lymphogranuloma venereum, infectious stage syphilis, active tuberculosis, and other diseases as determined by the Department of Health and Human Services.)	NO
Do you have a mental or physical disorder that poses or is likely to pose a threat to the safety or welfare of yourself or others?	NO
Are you or have you ever been a drug abuser or addict?	NO

Edit Part 2

Have you ever been arrested or convicted for any offense or crime, even though subject of a pardon, amnesty, or other similar action?	NO
Have you ever violated, or engaged in a conspiracy to violate, any law relating to controlled substances?	NO
Are you coming to the United States to engage in prostitution or unlawful commercialized vice or have you been engaged in prostitution or procuring prostitutes within the past 10 years?	NO
Have you ever been involved in, or do you seek to engage in, money laundering?	NO
Have you ever committed or conspired to commit a human trafficking offense in the United States or outside the United States?	NO
Are you the spouse, son, or daughter of an individual who has committed or conspired to commit a human trafficking offense in the United States or outside the United States and have you within the last five years, knowingly benefited from the trafficking activities?	NO
Have you knowingly aided, abetted, assisted or colluded with an individual who has committed or conspired to commit a severe human trafficking offense in the United States or outside the United States?	NO

Edit Part 3

Do you seek to engage in espionage, sabotage, export control violations, or any other illegal activity while in the United States?	NO
Do you seek to engage in terrorist activities while in the United States or have you ever engaged in terrorist activities?	NO
Have you ever or do you intend to provide financial assistance or other support to terrorists or terrorist organizations?	NO
Are you a member or representative of a terrorist organization?	NO
Have you ever ordered, incited, committed, assisted, or otherwise participated in genocide?	NO
Have you ever committed, ordered, incited, assisted, or otherwise participated in torture?	NO
Have you committed, ordered, incited, assisted, or otherwise participated in extrajudicial killings, political killings, or other acts of violence?	NO
Have you ever engaged in the recruitment or the use of the child soldiers?	NO
Have you, while serving as a government official, been responsible for or directly carried out, at any time, particularly severe violations of religious freedom?	NO
Have you ever been directly involved in the establishment or enforcement of the population controls forcing a woman to undergo an abortion against her free choice or a man or a woman to undergo sterilization against his or her free will?	NO
Have you ever been directly involved in the coercive transplantation of human organs or bodily tissue?	NO

Edit Part 4

Have you ever sought to obtain or assist others to obtain a visa, entry into the United States, or any other United States immigration benefit by fraud or willful misrepresentation or other unlawful means?	NO

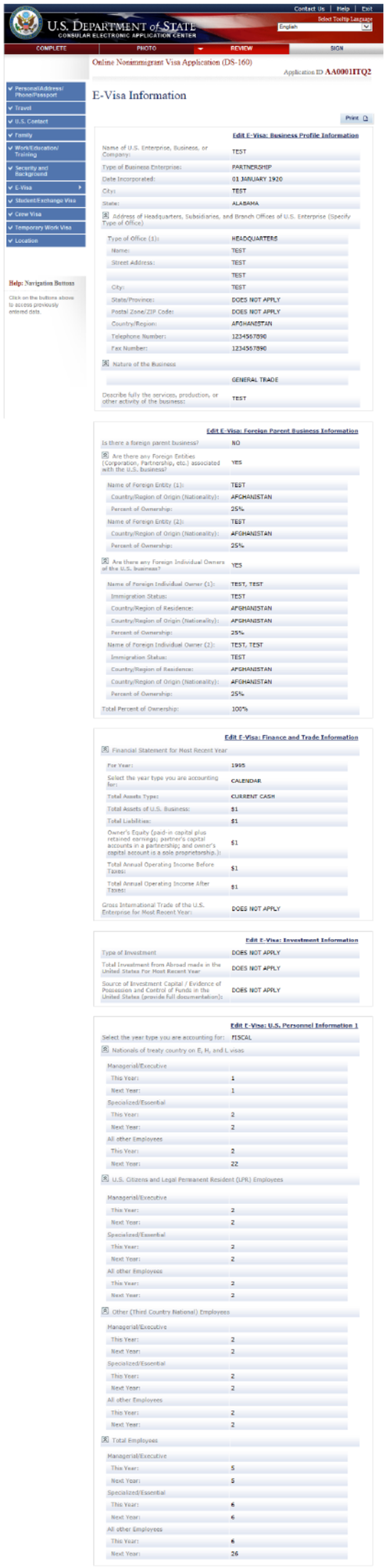
Edit Part 5

Have you ever withheld custody of a U.S. citizen child outside the United States from a person granted legal custody by a U.S. court?	NO
Have you voted in the United States in violation of any law or regulation?	NO
Have you ever renounced United States citizenship for the purpose of avoiding taxation?	NO

Back: Work/Education/Training | Save | Next: Student/Exchange Visa

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information | Disclaimers | Paperwork Reduction Act

Application Review (continued)



U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Contact Us | Help | Exit
Select Tooltip Language: English

COMPLETE | PHOTO | REVIEW | SIGN

Online Nonimmigrant Visa Application (DS-160)
Application ID: AA0001ITQ2

- Personal/Address/ Phone/Passport
- Travel
- U.S. Contact
- Family
- Work/Education/ Training
- Security and Background
- E-Visa
- Student/Exchange Visa
- Crew Visa
- Temporary Work Visa
- Location

Help: Navigation Buttons
Click on the buttons above to access previously entered data.

E-Visa Information

Print

Edit E-Visa: Business Profile Information

Name of U.S. Enterprise, Business, or Company:	TEST
Type of Business Enterprise:	PARTNERSHIP
Date Incorporated:	01 JANUARY 1920
City:	TEST
State:	ALABAMA

Address of Headquarters, Subsidiaries, and Branch Offices of U.S. Enterprise (Specify Type of Office)

Type of Office (1):	HEADQUARTERS
Name:	TEST
Street Address:	TEST
	TEST
City:	TEST
State/Province:	DOES NOT APPLY
Postal Zone/ZIP Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Telephone Number:	1234567890
Fax Number:	1234567890

Nature of the Business

	GENERAL TRADE
Describe fully the services, production, or other activity of the business:	TEST

Edit E-Visa: Foreign Parent Business Information

Is there a foreign parent business?	NO
Are there any Foreign Entities (Corporation, Partnership, etc.) associated with the U.S. business?	YES
Name of Foreign Entity (1):	TEST
Country/Region of Origin (Nationality):	AFGHANISTAN
Percent of Ownership:	25%
Name of Foreign Entity (2):	TEST
Country/Region of Origin (Nationality):	AFGHANISTAN
Percent of Ownership:	25%
Are there any Foreign Individual Owners of the U.S. business?	YES
Name of Foreign Individual Owner (1):	TEST, TEST
Immigration Status:	TEST
Country/Region of Residence:	AFGHANISTAN
Country/Region of Origin (Nationality):	AFGHANISTAN
Percent of Ownership:	25%
Name of Foreign Individual Owner (2):	TEST, TEST
Immigration Status:	TEST
Country/Region of Residence:	AFGHANISTAN
Country/Region of Origin (Nationality):	AFGHANISTAN
Percent of Ownership:	25%
Total Percent of Ownership:	100%

Edit E-Visa: Finance and Trade Information

Financial Statement for Most Recent Year

For Year:	1995
Select the year type you are accounting for:	CALENDAR
Total Assets Type:	CURRENT CASH
Total Assets of U.S. Business:	$1
Total Liabilities:	$1
Owner's Equity (paid-in capital plus retained earnings; partner's capital accounts in a partnership; and owner's capital account is a sole proprietorship.):	$1
Total Annual Operating Income Before Taxes:	$1
Total Annual Operating Income After Taxes:	$1
Gross International Trade of the U.S. Enterprise for Most Recent Year:	DOES NOT APPLY

Edit E-Visa: Investment Information

Type of Investment	DOES NOT APPLY
Total Investment from Abroad made in the United States For Most Recent Year	DOES NOT APPLY
Source of Investment Capital / Evidence of Possession and Control of Funds in the United States (provide full documentation):	DOES NOT APPLY

Edit E-Visa: U.S. Personnel Information 1

Select the year type you are accounting for: FISCAL

Nationals of treaty country on E, H, and L visas

Managerial/Executive	
This Year:	1
Next Year:	1
Specialized/Essential	
This Year:	2
Next Year:	2
All other Employees	
This Year:	2
Next Year:	22

U.S. Citizens and Legal Permanent Resident (LPR) Employees

Managerial/Executive	
This Year:	2
Next Year:	2
Specialized/Essential	
This Year:	2
Next Year:	2
All other Employees	
This Year:	2
Next Year:	2

Other (Third Country National) Employees

Managerial/Executive	
This Year:	2
Next Year:	2
Specialized/Essential	
This Year:	2
Next Year:	2
All other Employees	
This Year:	2
Next Year:	2

Total Employees

Managerial/Executive	
This Year:	5
Next Year:	5
Specialized/Essential	
This Year:	6
Next Year:	6
All other Employees	
This Year:	6
Next Year:	26

Edit E-Visa: U.S. Personnel Information 2

List all personnel of U.S. business who hold executive, managerial, and/or specialist positions by subsidiary/branch office. If aliens, indicate Nonimmigrant visa status or Lawful Permanent Resident (LPR) status

Name, Position/Title, and Division (1)	
Name:	TEST, TEST
Position:	TEST
Division:	TEST
Country/Region of Origin (Nationality):	ANTIGUA AND BARBUDA
U.S. Status of Personnel:	U.S. CITIZEN
Name, Position/Title, and Division (2)	
Name:	TEST, TEST
Position:	TEST
Division:	TEST
Country/Region of Origin (Nationality):	ANTIGUA AND BARBUDA
U.S. Status of Personnel:	U.S. CITIZEN

Edit E-Visa: Applicant Present Position Information

Type of Applicant:	EXECUTIVE
Present Position and Duties (describe in detail):	TEST
Employer Name:	TEST
Years with Present Employer:	4
Employer Address	
Street Address:	TEST
City:	TEST
State/Province:	DOES NOT APPLY
Postal Code/ZIP Code:	DOES NOT APPLY
Country/Region:	ALGERIA
Highest Level of Education	
School:	TEST
Degree:	TEST
Major:	TEST
Year:	1985
Do you have any other relevant education to report?	NO

Edit E-Visa: Applicant Position in U.S. Information

Title:	TEST
Duties:	TEST
Will you have any immediate subordinates in your position in the U.S.?	NO
Annual U.S. Salary and Benefits Package	
Salary:	$1
Allowances / Benefits:	$1
Total:	$2
Are you replacing a worker already in the United States?	NO
Is this an increase in staff?	NO
Is this a continuance of an existing employment in the United States?	NO

Edit E-Visa: Application Contact Information

Responsible officer within the business enterprise	
Name:	TEST, TEST
Position:	TEST
Name and address of person who may be contacted about this application	
Name:	TEST, TEST
Street Address:	TEST
City:	TEST
State/Province:	DOES NOT APPLY
Postal Zone/ZIP Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Telephone Number:	1234567890
Fax Number:	DOES NOT APPLY
Email Address:	DOES NOT APPLY

Back: Security and Background | Save | Next: Student/Exchange Visa

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information Disclaimers Paperwork Reduction Act

Application Review (continued)



Contact Us | Help | Exit

U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Select Tooltip Language: ENGLISH

COMPLETE | PHOTO | REVIEW | SIGN

Online Nonimmigrant Visa Application (DS-160) Application ID AA006WPHRO

- Personal/Address/ Phone/Passport
- Travel
- U.S. Contact
- Family
- Work/Education/ Training
- Security and Background
- Student/Exchange Visa
- Location

Help: Navigation Buttons

Click on the buttons above to access previously entered data.

Student/Exchange Visa Information

Print

Edit Additional Point of Contact Information

Additional Point of Contact Information:

Name(1):	STARK, ARYA
Street Address:	1234 STARK STREET
City:	KABUL
State/Province:	DOES NOT APPLY
Postal Zone/ZIP Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Telephone Number:	DOES NOT APPLY
Email Address:	DOES NOT APPLY
Name(2):	STARK, SANSA
Street Address:	1234 STARK STREET
City:	KABUL
State/Province:	DOES NOT APPLY
Postal Zone/ZIP Code:	DOES NOT APPLY
Country/Region:	AFGHANISTAN
Telephone Number:	DOES NOT APPLY
Email Address:	DOES NOT APPLY

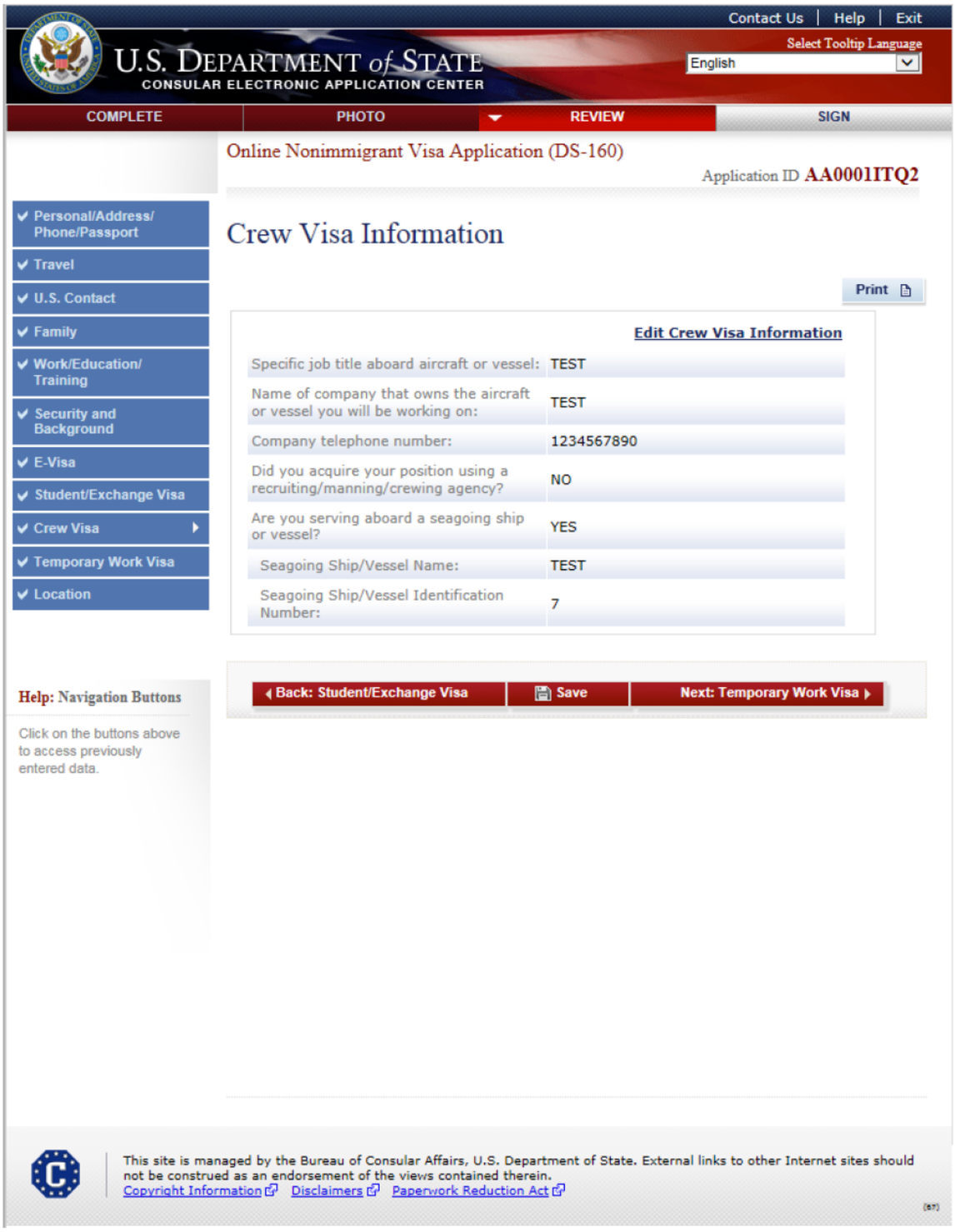
Edit SEVIS Information

SEVIS ID:	N1111111111
Program Number:	P-3-04510
Do you intend to study in the U.S.?	YES
Name of School:	GWU
Course of Study:	INTERNATIONAL AFFAIRS
Street Address:	2255 EYE STREET NW
	WASHINGTON, DISTRICT OF COLUMBIA 22242

Back: Security and Background | Save | Next: Location

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information Disclaimers Paperwork Reduction Act

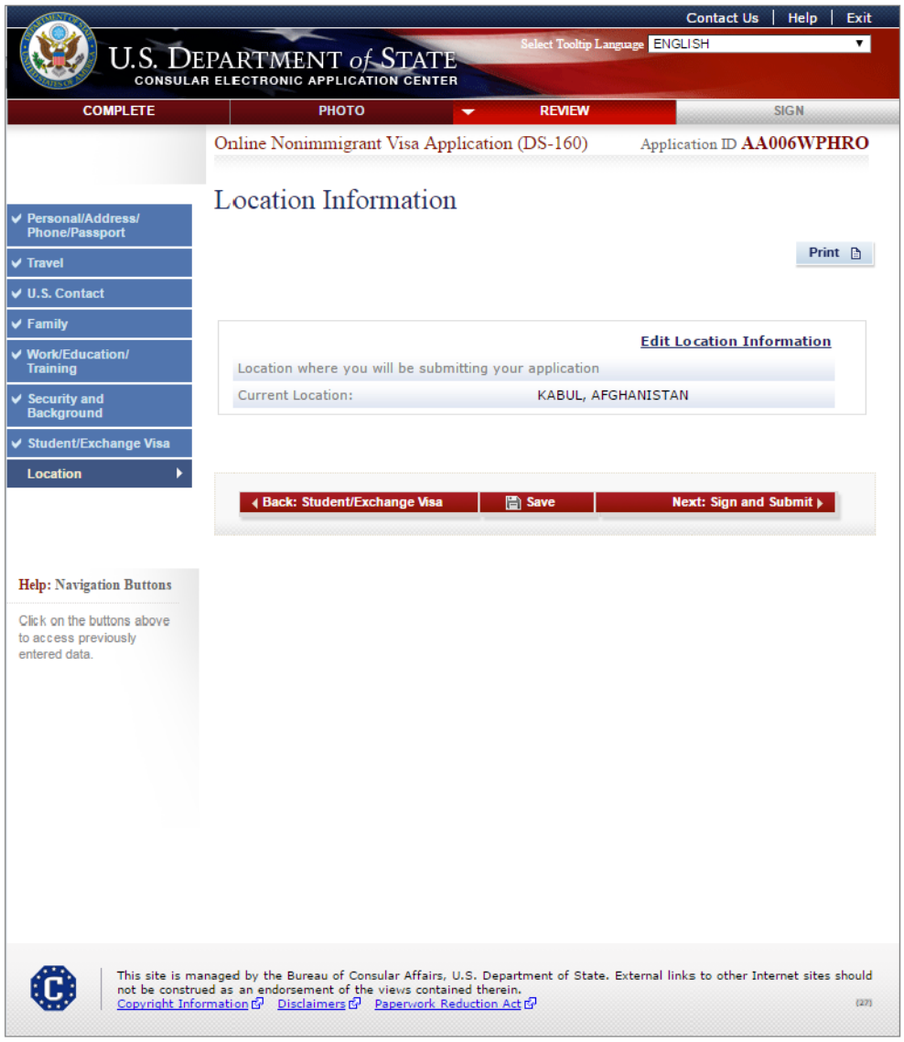
Application Review (continued)



Application Review (continued)

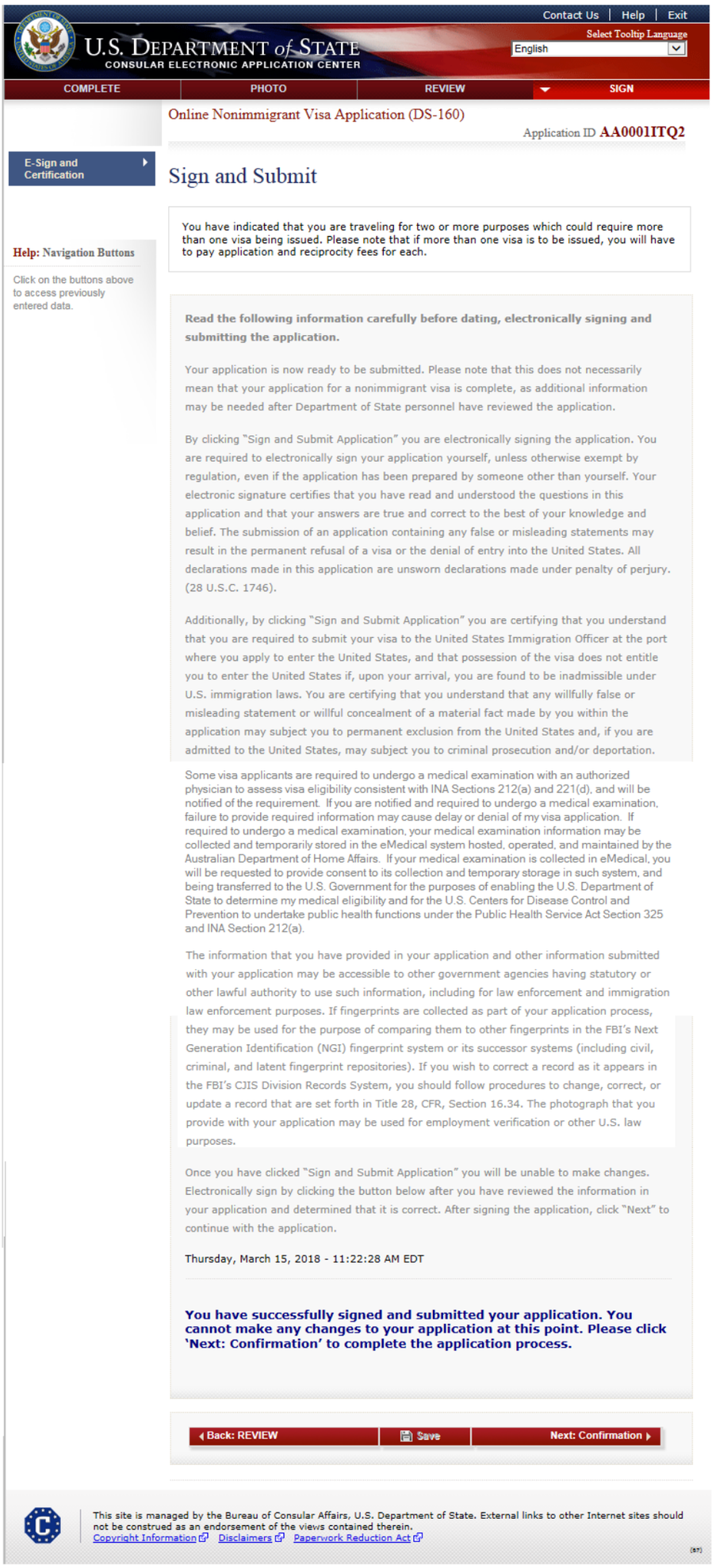


Application Review (continued)



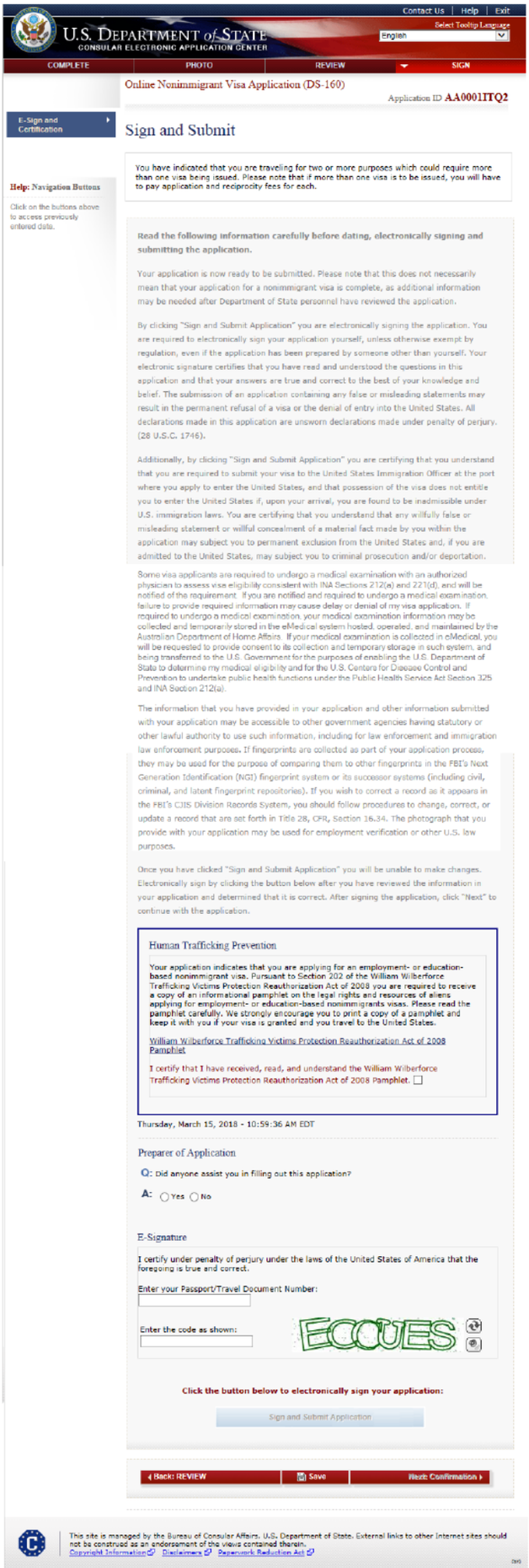
Sign and Submit – Successful Signed and Submitted page

Displayed for all applicants.



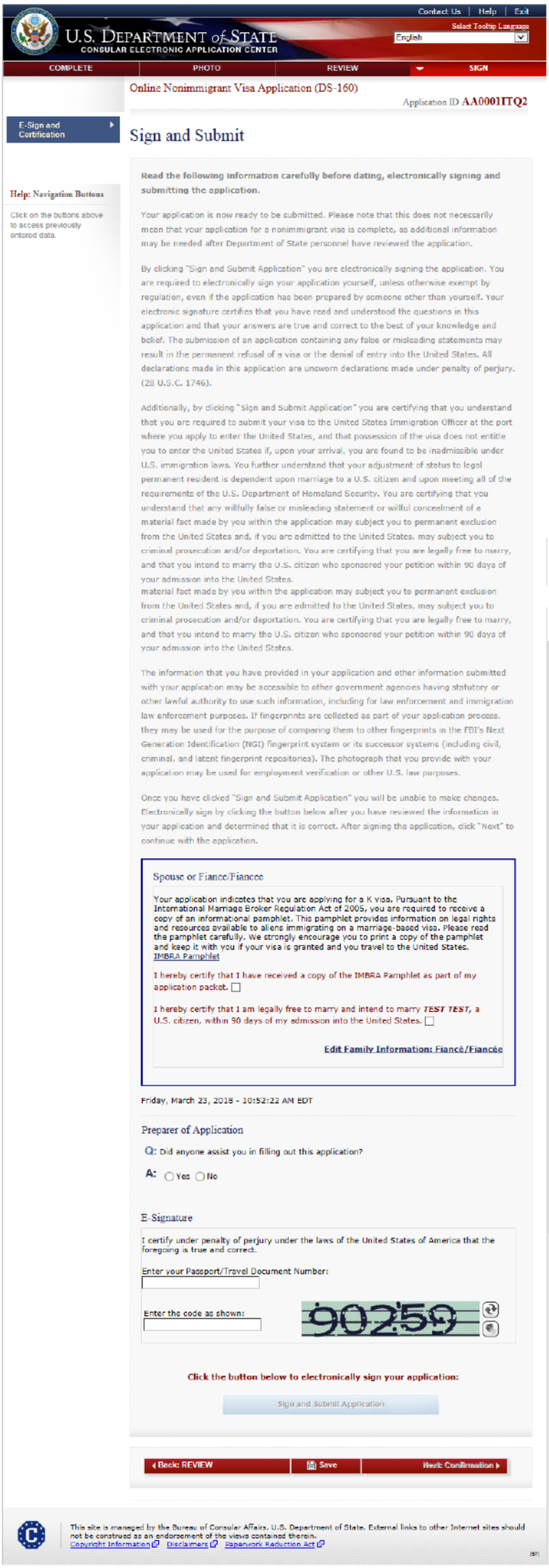
Sign and Submit– Wilberforce Pamphlet

Displayed for A3-CH, A3-EM, A3-SP, G2-CH, G2-RP, G2-SP, H1B-H1B, H1B1-CHL, H1B1-SGP, H1C-NR, H2A-AG, H2B-NA, H3-TR, J1-J1, J2-CH, J2-SP, NATO1-CH, NATO1-PR, NATO1-SP, NATO2-CH, NATO2-RP, NATO2-SP, NATO3-CH, NATO3-SP, NATO3-ST, NATO4-CH, NATO4-OF, NATO4-SP, NATO5-CH, NATO5-EX, NATO5-SP, NATO6-CH, NATO6-SP, NATO6-ST, NATO7-CH, NATO7-EM, NATO7-SP



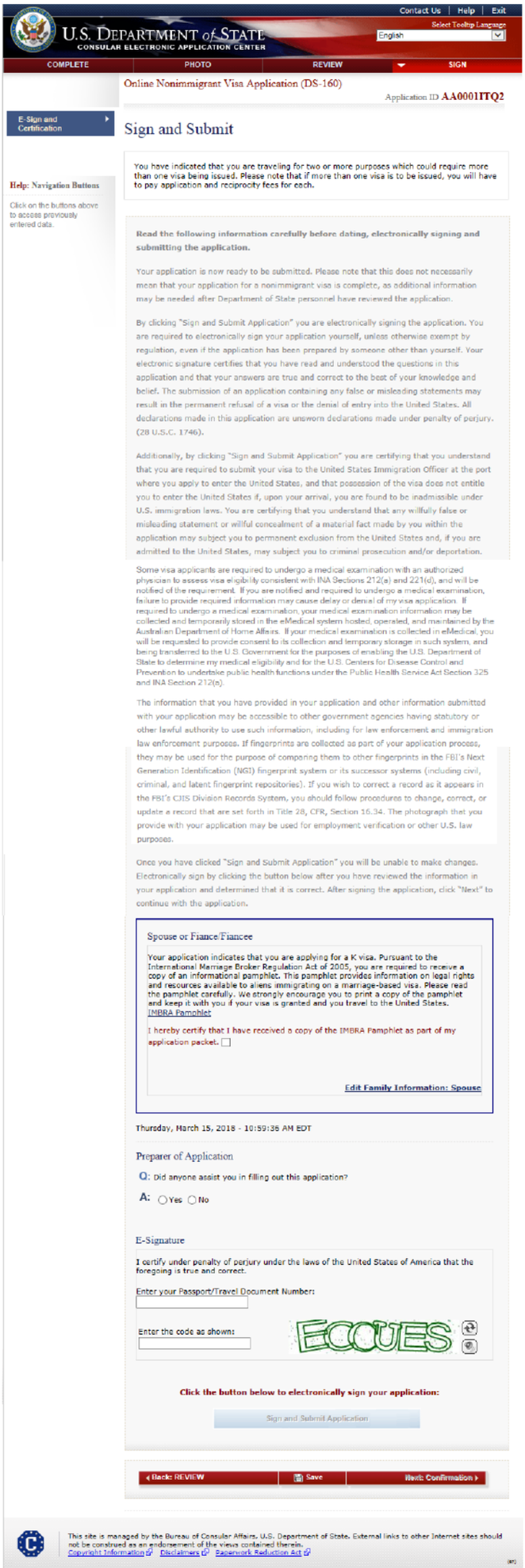
Sign and Submit– IMBRA

Displays for K1 applicants.



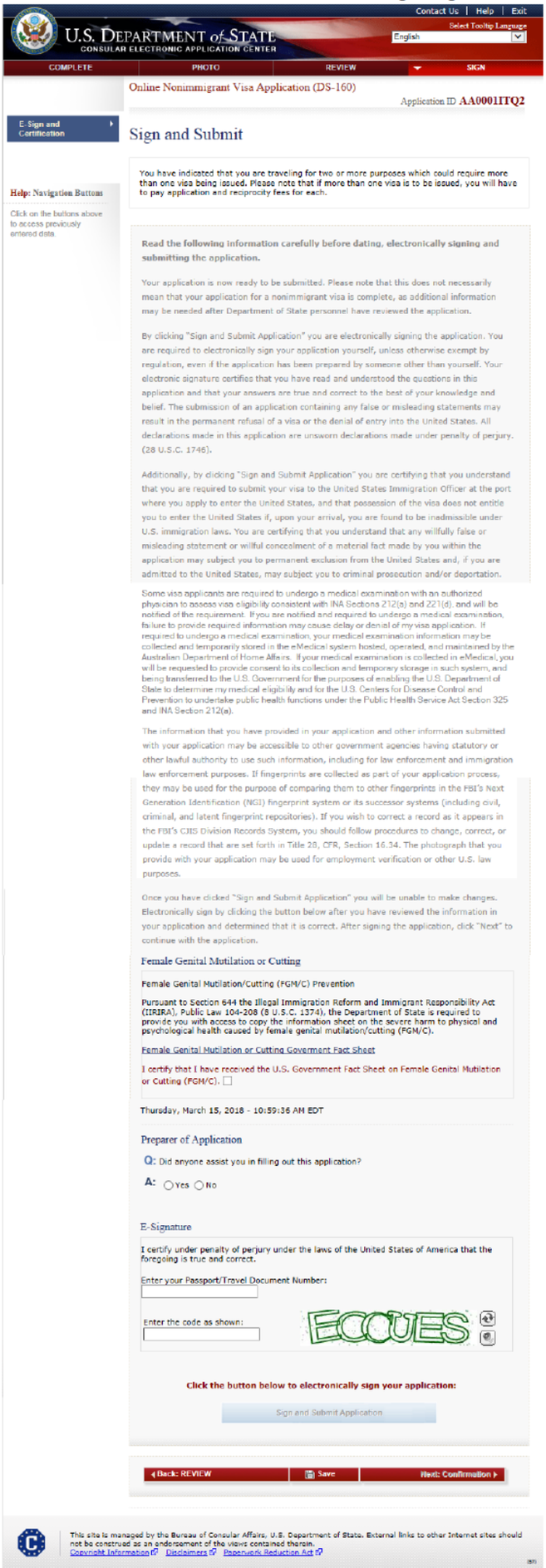
Sign and Submit– IMBRA

Displays for K3 applicants.



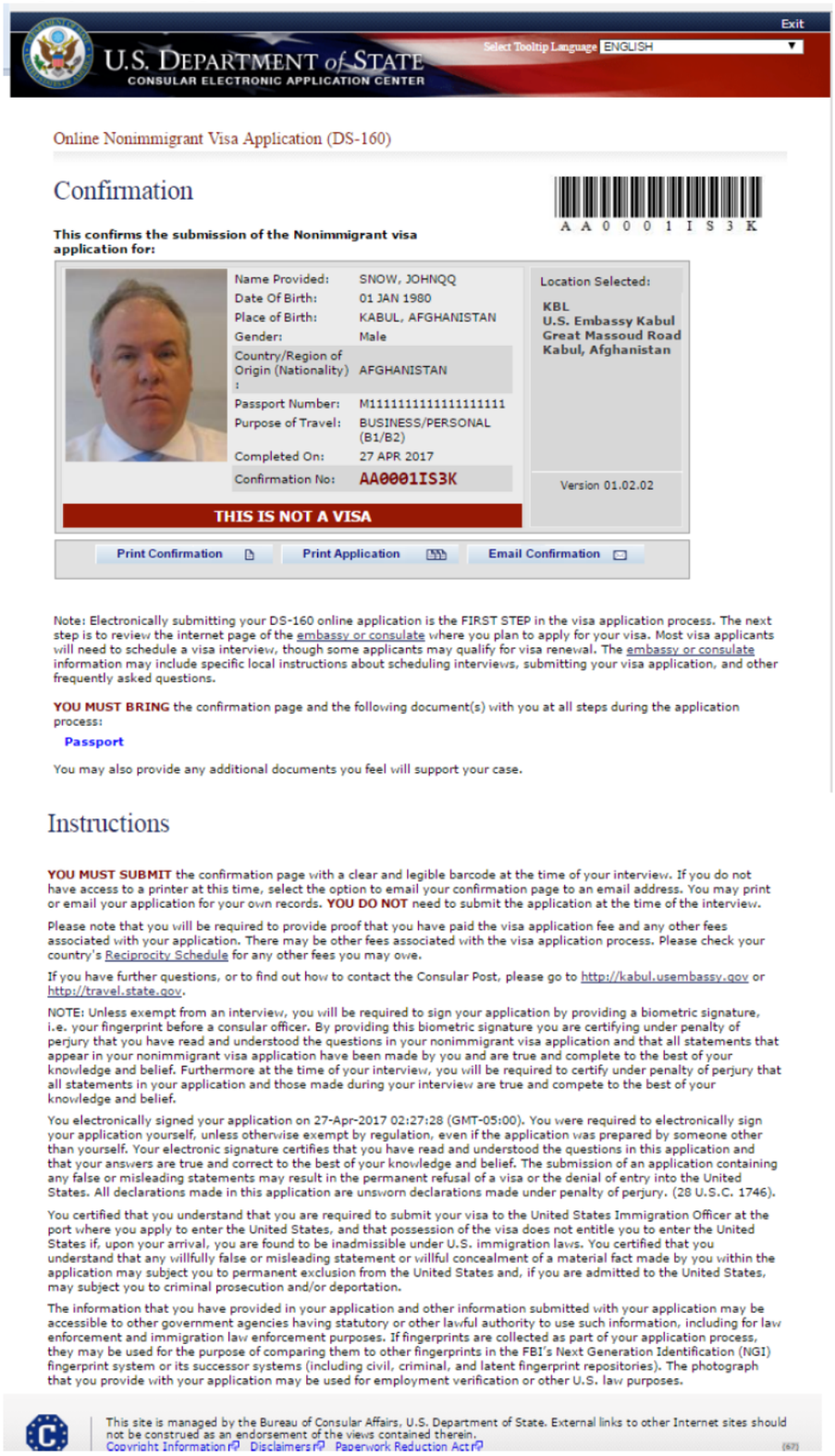
Sign and Submit – FGM/C

Displayed for applicants of following nationalities: Benin, Burkina Faso, Cameroon, Central African Republic, Chad, Cote d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Eritrea, Ethiopia, Gambia, Ghana, Guinea, Guinea-Bissau, Iraq, Kenya, Liberia, Mali, Mauritania, Niger, Nigeria, Senegal, Sierra Leone, Somalia, Sudan, Tanzania, Togo, Uganda, Yemen



Confirmation

Displayed for all applicants.



Exit

U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Select Tooltip Language ENGLISH

Online Nonimmigrant Visa Application (DS-160)

Confirmation

A A 0 0 0 1 I S 3 K

This confirms the submission of the Nonimmigrant visa application for:

Name Provided:	SNOW, JOHNQQ
Date Of Birth:	01 JAN 1980
Place of Birth:	KABUL, AFGHANISTAN
Gender:	Male
Country/Region of Origin (Nationality) :	AFGHANISTAN
Passport Number:	M111111111111111111
Purpose of Travel:	BUSINESS/PERSONAL (B1/B2)
Completed On:	27 APR 2017
Confirmation No:	AA0001IS3K

Location Selected:

KBL
U.S. Embassy Kabul
Great Massoud Road
Kabul, Afghanistan

Version 01.02.02

THIS IS NOT A VISA

Print Confirmation | Print Application | Email Confirmation

Note: Electronically submitting your DS-160 online application is the FIRST STEP in the visa application process. The next step is to review the internet page of the embassy or consulate where you plan to apply for your visa. Most visa applicants will need to schedule a visa interview, though some applicants may qualify for visa renewal. The embassy or consulate information may include specific local instructions about scheduling interviews, submitting your visa application, and other frequently asked questions.

YOU MUST BRING the confirmation page and the following document(s) with you at all steps during the application process:

Passport

You may also provide any additional documents you feel will support your case.

Instructions

YOU MUST SUBMIT the confirmation page with a clear and legible barcode at the time of your interview. If you do not have access to a printer at this time, select the option to email your confirmation page to an email address. You may print or email your application for your own records. **YOU DO NOT** need to submit the application at the time of the interview.

Please note that you will be required to provide proof that you have paid the visa application fee and any other fees associated with your application. There may be other fees associated with the visa application process. Please check your country's Reciprocity Schedule for any other fees you may owe.

If you have further questions, or to find out how to contact the Consular Post, please go to http://kabul.usembassy.gov or http://travel.state.gov.

NOTE: Unless exempt from an interview, you will be required to sign your application by providing a biometric signature, i.e. your fingerprint before a consular officer. By providing this biometric signature you are certifying under penalty of perjury that you have read and understood the questions in your nonimmigrant visa application and that all statements that appear in your nonimmigrant visa application have been made by you and are true and complete to the best of your knowledge and belief. Furthermore at the time of your interview, you will be required to certify under penalty of perjury that all statements in your application and those made during your interview are true and compete to the best of your knowledge and belief.

You electronically signed your application on 27-Apr-2017 02:27:28 (GMT-05:00). You were required to electronically sign your application yourself, unless otherwise exempt by regulation, even if the application was prepared by someone other than yourself. Your electronic signature certifies that you have read and understood the questions in this application and that your answers are true and correct to the best of your knowledge and belief. The submission of an application containing any false or misleading statements may result in the permanent refusal of a visa or the denial of entry into the United States. All declarations made in this application are unsworn declarations made under penalty of perjury. (28 U.S.C. 1746).

You certified that you understand that you are required to submit your visa to the United States Immigration Officer at the port where you apply to enter the United States, and that possession of the visa does not entitle you to enter the United States if, upon your arrival, you are found to be inadmissible under U.S. immigration laws. You certified that you understand that any willfully false or misleading statement or willful concealment of a material fact made by you within the application may subject you to permanent exclusion from the United States and, if you are admitted to the United States, may subject you to criminal prosecution and/or deportation.

The information that you have provided in your application and other information submitted with your application may be accessible to other government agencies having statutory or other lawful authority to use such information, including for law enforcement and immigration law enforcement purposes. If fingerprints are collected as part of your application process, they may be used for the purpose of comparing them to other fingerprints in the FBI's Next Generation Identification (NGI) fingerprint system or its successor systems (including civil, criminal, and latent fingerprint repositories). The photograph that you provide with your application may be used for employment verification or other U.S. law purposes.

This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.
Copyright Information | Disclaimers | Paperwork Reduction Act

Link – Paper Reduction Act

Displayed for all applicants.



Online Nonimmigrant Visa Application (DS-160)

Paperwork Reduction Act

Public reporting burden for this collection of information is estimated to average 90 minutes per response, including time required for searching existing data sources, gathering the necessary documentation, providing the information and/or documents required, and reviewing the final collection. You do not have to supply this information unless this collection displays a currently valid OMB control number. If you have comments on the accuracy of this burden estimate and/or recommendations for reducing it, please send them to:

PRA_BurdenComments@state.gov

Confidentiality Statement

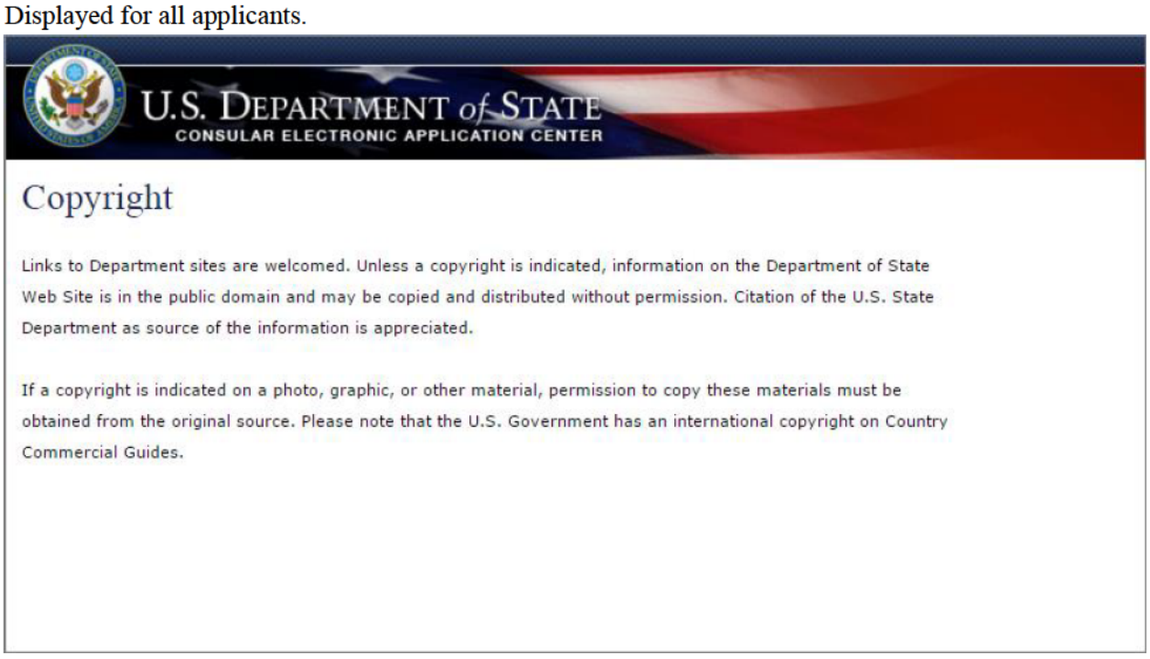
The information asked for on this form is requested pursuant to Section 222 of the Immigration and Nationality Act. INA Section 222(f) provides that the records of the Department of States and of diplomatic and consular offices of the United States pertaining to the issuance and refusal of visas or permits to enter the United States shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of such records may be made available to a court provided the court certifies that the information contained in such records is needed in a case pending before the court.



This site is managed by the Bureau of Consular Affairs, U.S. Department of State. External links to other Internet sites should not be construed as an endorsement of the views contained therein.

Link – Copyright Information

Displayed for all applicants.



U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

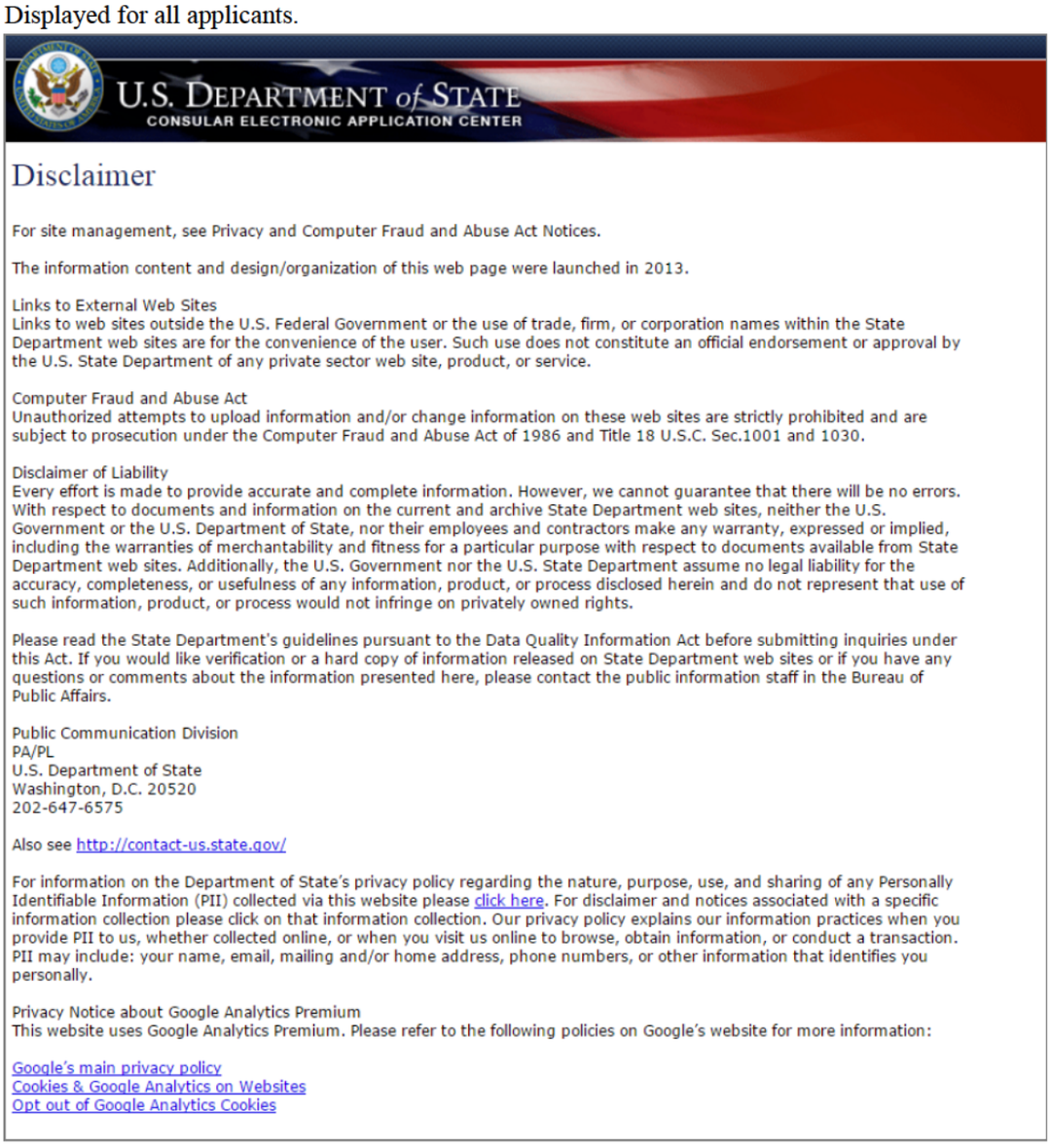
Copyright

Links to Department sites are welcomed. Unless a copyright is indicated, information on the Department of State Web Site is in the public domain and may be copied and distributed without permission. Citation of the U.S. State Department as source of the information is appreciated.

If a copyright is indicated on a photo, graphic, or other material, permission to copy these materials must be obtained from the original source. Please note that the U.S. Government has an international copyright on Country Commercial Guides.

Link – Disclaimers

Displayed for all applicants.



U.S. DEPARTMENT of STATE
CONSULAR ELECTRONIC APPLICATION CENTER

Disclaimer

For site management, see Privacy and Computer Fraud and Abuse Act Notices.

The information content and design/organization of this web page were launched in 2013.

Links to External Web Sites
Links to web sites outside the U.S. Federal Government or the use of trade, firm, or corporation names within the State Department web sites are for the convenience of the user. Such use does not constitute an official endorsement or approval by the U.S. State Department of any private sector web site, product, or service.

Computer Fraud and Abuse Act
Unauthorized attempts to upload information and/or change information on these web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sec.1001 and 1030.

Disclaimer of Liability
Every effort is made to provide accurate and complete information. However, we cannot guarantee that there will be no errors. With respect to documents and information on the current and archive State Department web sites, neither the U.S. Government or the U.S. Department of State, nor their employees and contractors make any warranty, expressed or implied, including the warranties of merchantability and fitness for a particular purpose with respect to documents available from State Department web sites. Additionally, the U.S. Government nor the U.S. State Department assume no legal liability for the accuracy, completeness, or usefulness of any information, product, or process disclosed herein and do not represent that use of such information, product, or process would not infringe on privately owned rights.

Please read the State Department's guidelines pursuant to the Data Quality Information Act before submitting inquiries under this Act. If you would like verification or a hard copy of information released on State Department web sites or if you have any questions or comments about the information presented here, please contact the public information staff in the Bureau of Public Affairs.

Public Communication Division
PA/PL
U.S. Department of State
Washington, D.C. 20520
202-647-6575

Also see http://contact-us.state.gov/

For information on the Department of State's privacy policy regarding the nature, purpose, use, and sharing of any Personally Identifiable Information (PII) collected via this website please click here. For disclaimer and notices associated with a specific information collection please click on that information collection. Our privacy policy explains our information practices when you provide PII to us, whether collected online, or when you visit us online to browse, obtain information, or conduct a transaction. PII may include: your name, email, mailing and/or home address, phone numbers, or other information that identifies you personally.

Privacy Notice about Google Analytics Premium
This website uses Google Analytics Premium. Please refer to the following policies on Google's website for more information:

Google's main privacy policy
Cookies & Google Analytics on Websites
Opt out of Google Analytics Cookies

EXHIBIT 13:

DHS OIG Report

OFFICE OF INSPECTOR GENERAL

DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success

(Redacted)

Homeland Security

February 27, 2017

OIG-17-40

~~FOR OFFICIAL USE ONLY~~

DHS OIG HIGHLIGHTS

DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success

February 27, 2017

Why We Did This Inspection

Following the December 2015 terrorist attack in San Bernardino, California, Congress raised concerns about the use of social media by terrorist groups and requested that the Department of Homeland Security expand social media background checks. We conducted this inspection to review DHS' social media pilot programs.

What We Recommend

We made one recommendation to help ensure DHS develops an effective social media screening program.

For Further Information:
Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

DHS has established a task force for using social media to screen applicants for immigration benefits. In connection with that effort, U.S. Citizenship and Immigration Services (USCIS) began pilots to expand social media screening of immigration applicants. Additionally, Immigration and Customs Enforcement (ICE) independently began a pilot to use social media screening during the visa issuance process. However, these pilots, on which DHS plans to base future department-wide use of social media screening, lack criteria for measuring performance to ensure they meet their objectives. Although the pilots include some objectives, such as determining the effectiveness of an automated search tool and assessing data collection and dissemination procedures, it is not clear DHS is measuring and evaluating the pilots' results to determine how well they are performing against set criteria. Absent measurement criteria, the pilots may provide limited information for planning and implementing an effective, department-wide future social media screening program.

DHS Response

I&A, on behalf of itself, USCIS, and ICE, concurred with the recommendation and has begun taking corrective actions.

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

February 27, 2017

MEMORANDUM FOR: David J. Glawe
Acting Under Secretary
Office of Intelligence and Analysis

Lori Scialabba
Acting Director
U.S. Citizenship and Immigration Services

Thomas D. Homan
Acting Director
U.S. Immigration and Customs Enforcement

FROM: John Roth
Inspector General

SUBJECT: *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success – For Official Use Only*

For your action is our final report, *DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success*. We incorporated the formal comments provided by your office.

The report contains one recommendation aimed at improving DHS' social media screening pilots. The Office of Intelligence and Analysis (I&A) concurred with the recommendation. Based on information provided in the response to the draft report, we consider the recommendation open and resolved. Once the recommendation has been fully implemented, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your response or closure request to OIGInspectionsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post a redacted version of the report on our website.

Please call me with any questions, or your staff may contact Laurel Rimon, Acting Assistant Inspector General for Inspections and Evaluations or Angela Garvin, Deputy Assistant Inspector General, at (202) 254-4100.

Background

Following the December 2, 2015 terrorist attack in San Bernardino, California, lawmakers became increasingly concerned about the use of social media by terrorist groups. On December 15, 2015, Senator Jeanne Shaheen and 24 other Senators sent a letter to the Secretary of Homeland Security requesting that, as soon as possible, DHS expand social media background checks, focused on possible connections to terrorist activity, to screening for visa determinations for visitors and immigrants. In response, the then DHS Secretary and Deputy Secretary asked the Under Secretary for Intelligence and Analysis (I&A) to lead a task force to review the Department's current use of social media and identify options to optimize its use across DHS. The task force comprises senior representatives and staff from DHS, U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), U.S. Customs and Border Protection, the Transportation Security Administration, and DHS oversight offices including the Office of General Counsel, Privacy Office, and Office for Civil Rights and Civil Liberties, which have a vested interest in DHS' use of social media.

According to the task force's implementation plan, the first priority was to conduct a pilot at USCIS to test systematic screening of applicants for immigration benefits.[1] USCIS had used social media in a limited capacity but had no experience using it as a large-scale screening tool. In December 2015, USCIS started screening the social media accounts of a limited number of [redacted] applying for [redacted] status, using both manual and automated screening. The task force intended to use the December 2015 pilot and lessons learned from other DHS components' use of social media to develop policies and processes for standardized use of social media department-wide. Additionally, to expand social media screening across all DHS components, the task force recommended, and the Secretary approved, creation of a DHS Social Media Center of Excellence (COE).[2] (Appendix B contains details about the COE.) In April 2016, USCIS expanded social media screening, testing another automated tool together with manual screening. In

[1] USCIS grants immigration benefits to people who meet the eligibility requirements to stay in the United States temporarily or permanently. These benefits include granting U.S. citizenship to eligible individuals, authorizing individuals to reside permanently in the United States, and authorizing aliens to work in the United States.
[2] During our review it was called the "Center of Excellence"; however, the name was later changed to "Shared Social Media Screening Service". We refer to it as the "Center of Excellence" in this report.

August 2016, ICE began using a different automated tool to screen the social media of nonimmigrant visa holders [redacted].[3]

Results of Inspection

DHS has established a task force for using social media to screen applicants for immigration benefits. In connection with that effort, USCIS began pilots to expand social media screening of immigration applicants. Additionally, ICE independently began a pilot to use social media screening during the visa issuance process. However, these pilots, on which DHS plans to base future department-wide use of social media screening, lack criteria for measuring performance to ensure they meet their objectives. Although the pilots include some objectives, such as determining the effectiveness of an automated search tool and assessing data collection and dissemination procedures, it is not clear DHS is measuring and evaluating the pilots' results to determine how well they are performing. Absent measurement criteria, the pilots will be of limited use in planning and implementing an effective, department-wide future social media screening program.

The Government Accountability Office (GAO) has issued best practices for an effective pilot phase of a program. According to GAO, "The pilot phase allows for a check on whether program operations occur as expected."[4] GAO has also stated that pilot programs should have well-defined, clear, and measurable objectives; criteria or standards for determining pilot performance; and a plan to track the pilot's performance and evaluate the final results.[5] Following these best practices can increase the rigor of the pilots to ensure scalability and long-term success.

USCIS started a pilot in December 2015 to screen the social media accounts of [redacted] and [redacted] applicants for [redacted] status. The pilot's objective was to examine the feasibility of using social media screening with an automated search tool called [redacted] and determine whether useful information for adjudicating refugee applications could be obtained.[6] Although the pilot had an objective, it did not define what would constitute a successful outcome, nor did it identify metrics against which to benchmark its findings. For example, the pilot discovered that [redacted] individuals had confirmed social media accounts; [redacted] likely had a social media account; [redacted] individuals had unconfirmed

[3] American embassies and consulates issue nonimmigrant visas authorizing temporary visits to the United States for individuals who do not intend to become permanent residents.
[4] GAO-12-208G, January 2012
[5] GAO-09-45, November 2008
[6] [redacted], a social media analytics tool, covers a large number of social media platforms, has access to third-party information providers, and can access web-based information.

accounts; and [redacted] individuals had no identified social media account. USCIS concluded that the [redacted] individuals had a minimal presence on [redacted] social media platforms accessible through [redacted]. Because the pilot did not have metrics to measure success, it is difficult to conclude whether finding [redacted] individuals with confirmed social media accounts constitutes success.

The purpose of another USCIS pilot, which began in April 2016, was to expand screening to an additional [redacted], predominately [redacted], [redacted] applicants through use of the Defense Advanced Research Projects Agency (DARPA) [redacted] tool.[7] The applicants were asked to voluntarily give their social media user names.[8] USCIS then screened the user names against [redacted] using the [redacted] tool; USCIS also manually screened the user names against [redacted]. USCIS assessed identified accounts to determine whether the refugees were linked to derogatory social media information that could impact their eligibility for immigration benefits or admissibility into the United States. Using the [redacted] tool and manual screening, USCIS identified [redacted] individuals with confirmed social media accounts and [redacted] individuals with unconfirmed accounts. In reviewing the pilot, USCIS concluded that the [redacted] tool was not a viable option for automated social media screening and that manual review was more effective at identifying accounts. USCIS based its conclusion on the [redacted] tool's low "match confidence." Because the resulting accounts identified by the tool did not always match up with the applicants, officers had to manually check the results. However, USCIS did not establish match benchmarks for the tool, so it does not know what level of match confidence would signify success or failure.

In August 2016, ICE independently began a pilot to screen the social media activity of [redacted] nonimmigrant visa applicants from [redacted]. The intent of this pilot is to evaluate the capability of [redacted] to conduct initial screening of social media activity during visa application and continue social media monitoring during the [redacted].[9] According to the pilot plan, this approach will complement existing background

[7] DARPA [redacted] is a social media screening platform that screens against [redacted].
[8] National Security Council staff requested USCIS and the Department of State, which also participated, to pilot the elicitation of the applicants' social media identifiers. USCIS is [redacted] to access social media platforms by DHS Privacy regulations and using government accounts on social media platforms may introduce additional risk to government systems. DHS and its components have [redacted] of identifying social media account for individuals [redacted] that may not be appropriate or viable for large scale screening of applicants for immigration benefits.
[9] [redacted] is a web search tool that specializes in social media data exploitation by analyzing social media data and funneling it into actionable information.

checks conducted in conjunction with the Department of State and help identify potential derogatory information not found in Government databases. Although ICE has identified several measurable criteria for data that will be collected during the pilot, it has not articulated a plan to use these metrics to evaluate performance and determine overall program effectiveness. In our opinion, a clearly defined performance evaluation is essential to determining whether, how, and when to integrate pilot activities into overall efforts and will enable the Department to implement a more effective social media screening program.

DHS and the task force are planning department-wide use of social media for screening based on these pilots. Because components are not measuring their pilots against clear success criteria, DHS may not be able to make informed decisions when it designs its social media screening program. The task force needs to better manage ongoing efforts to pilot social media screening to help ensure an effective and successful social media screening program in the future.

Recommendation

We recommend that the Under Secretary of Intelligence and Analysis coordinate with USCIS and ICE to develop and implement a plan to evaluate the performance of social media screening pilots that includes features such as well-defined, clear, and measurable objectives and standards for determining pilot performance to help ensure DHS develops an effective social media screening program.

Management Comments and OIG Analysis

I&A responded on behalf of itself, ICE, and USCIS. The components concurred with our recommendation and provided comments to the draft report. A summary of the management response and our analysis follows. We have included a copy of the management comments in their entirety in appendix A. I&A also provided technical comments to our report, which we incorporated, as appropriate.

I&A's Response to the Recommendation: I&A concurred with the recommendation and stated that DHS has taken steps to improve its social media screening pilots by implementing a four-pronged approach that measures performance to develop consistent benchmarks and continue improving performance to ensure rigor and scalability for long-term success. This approach includes using qualitative and quantitative criteria for measuring tool performance; collecting and analyzing comprehensive

performance metrics of ongoing research and development pilots; reporting project milestones to the task force; and reporting select metrics measuring pilot performance in a weekly task force agenda. Additionally, DHS will continue to identify and refine new and existing metrics to measure social media screening pilots' performance, to include identifying benchmarks for the various tools tested.

OIG Analysis: I&A's planned actions are partially responsive to this recommendation. This recommendation is resolved, but will remain open until I&A provides documentation of well-defined, clear, and measurable objectives and standards for determining pilot performance. I&A's response indicated that a new social media screening pilot was scheduled to begin in January 2017. I&A should take this opportunity to develop and implement GAO's best practices for an effective pilot program to ensure scalability and long-term success of the pilot.

I&A also emphasized that, at the launch of the task force, neither the private sector nor the U.S. Government possessed the capabilities for large-scale social media screening. OIG recognizes that DHS has made strides in identifying and assessing social media screening technology and conducting pilots that will enable the development of such capabilities. The Homeland Security Systems Engineering & Development Institute report, *Social Media Analytics Capability Testing: Independent Assessment*, referenced in I&A's response, provides evidence of some of the progress that has been made in leveraging technology to meet the Department's needs. The report was not received by OIG until January 6, 2017, and therefore was not included in our analysis. We note that this independent assessment includes many metrics that may be useful in establishing benchmarks and determining performance of future pilot programs. The assessment included seven steps in conducting evaluations for quantitative analysis: (1) define the purpose of the evaluation; (2) elaborate a task model; (3) define top-level quality characteristics; (4) produce system requirements; (5) define metrics to measure requirements; (6) define techniques to measure metrics; and (7) carry out and interpret the evaluation. This framework was followed for the independent assessment and should be continued with testing pilots.

Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

The initial objective of this inspection was to evaluate DHS' progress in developing social media screening policies, procedures, and capabilities.

However, upon discovering the lack of performance measures in USCIS' and ICE's pilots for social media screening for immigration benefits, we adjusted our scope and reviewed DHS' social media task force and DHS' use of pilots to help create a social media screening program. Although we reviewed DHS policies relevant to social media screening, including DHS Instruction Number 110–01-001, *Privacy Policy for Operational Use of Social Media*, we could not evaluate specific policies and procedures for the pilots because they had not been written. Likewise, we reviewed the task force's concept of operations for the role of the COE, but could not evaluate the COE at this time because it has not been set up or funded.

We interviewed DHS staff from the Office of Policy, USCIS' Fraud Detection and National Security Directorate, ICE's Visa Security Program and Homeland Security Investigations, Science and Technology Directorate, Privacy Office, Office for Civil Rights and Civil Liberties, and the Chair of the Social Media task force to determine their roles in social media screening.

We conducted this inspection between July and October 2016 pursuant to the *Inspector General Act of 1978*, as amended, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

The Office of Inspections and Evaluations major contributors to this report are William McCarron, Chief Inspector; Natalie Fussell Enclade, Lead Inspector; Carie Mellies, Lead Inspector; Stephen Farrell, Inspector; Adam Robinson, Inspector; James Alver, Inspector; Kelly Herberger, Communications Analyst; and Elizabeth Kingma, Independent Referencer.

Appendix A
I&A's Comments to the Draft Report

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

Homeland Security

DEC 29 2016

MEMORANDUM FOR: John Roth
Inspector General

FROM: Francis X. Taylor
Under Secretary for Intelligence and Analysis
Counterterrorism Coordinator
Co-Chair, DHS Social Media Task Force

SUBJECT: OIG Draft Report, "DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success" (Project No. 16-079-ISP-USCIS)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS or "Department") appreciates the Office of the Inspector General's (OIG) work in planning and conducting its review and issuing this draft report.

We are pleased that the OIG recognizes the importance of developing an effective Departmental social media screening capability across various DHS mission sets using clear success criteria. However, DHS believes that the OIG's overall characterization that the Department's social media screening pilots lack performance measurement is misleading.

On December 15, 2015, the DHS Social Media Task Force ("Task Force") was established to assess the current state of the Department's social media policies, processes, and capabilities. The Task Force identified a Departmental need to develop the capacity to conduct systematic social media screening in areas where DHS has a responsibility to screen and vet applicants (e.g., travelers, refugees, immigrants, etc.). As such, social media screening is a new undertaking for DHS and the environment continues to rapidly evolve in terms of available technology and process refinement.

When the Task Force was established, neither clearly defined processes nor robust technical capabilities for large-scale, automated social media screening existed in industry or within the U.S. Government. Accordingly, the Department leveraged a systematic, multi-phased approach to identify and assess potential social media screening capabilities, including a number of research and development projects, referred to as "pilots," to assess the feasibility of developing such a capability. DHS chose to pursue these research and development projects and did not iniatiate fully operational pilots, as defined by the Government Accountability Office and referenced in the OIG draft report, because the technology was not yet available for such an endeavor to have been successful. Specifically, the technology available at the time was not

capable of processing DHS screening mission sets in a scalable manner. As part of its feasibility testing, DHS (1) conducted a market survey of 275 tools to identify existing vendors in the social media analytical tool space that met minimum capability requirements; (2) assessed tools that met key requirements for the screening capability; and (3) completed an in-depth qualitative and quantitative assessment of the capabilities provided by each tool, which allowed the Department to identify five tools for further testing and research on operational data based on Component mission requirements.

The OIG's draft report states that the "pilots did not have metrics to measure success" and "did not establish [...] benchmarks." However, the Department's pilots were designed to assess tool performance and advance the technical capabilities for large-scale, automated social media screening. Although the draft report only references three pilots, DHS has completed seven pilots between December 15, 2015 to present under the purview of the Task Force. Specifically, DHS completed five USCIS pilots plus another that remains ongoing, one U.S. Customs and Border Protection (CBP) pilot with another currently in the initiation phase, and one Immigration and Customs Enforcement (ICE) pilot. Of note, each pilot was evaluated to identify lessons learned and generate relevant performance measures to improve tool performance and understand workload requirements. The Department is currently monitoring multiple performance measures for the ongoing USCIS pilot to evaluate the effectiveness of USCIS social media screening operations and as the CBP pilot begins in January 2017, the same measures will be used to assess performance across both screening mission sets.

The Department will continue to iterate on best practices generated from each pilot and prioritize evolving performance measures to evaluate overall program effectiveness. DHS concurs with the one recommendation contained in the draft report. Attached, please find our detailed response to the recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Attachment

UNCLASSIFIED

Attachment: DHS Management Response to Recommendation Contained in OIG-16-070-ISP-USCIS

OIG recommended that the Under Secretary of Intelligence and Analysis:

Recommendation: Coordinate with USCIS and ICE to develop and implement a plan to evaluate the performance of social media screening pilots that includes features such as well-defined, clear, and measurable objectives and standards for determining pilot performance to help ensure DHS develops an effective social media screening program.

Response: Concur. Consistent with the OIG's recommendation, DHS has taken prudent steps to improve the functioning of the DHS Social Media Task Force and execution of its social media screening pilots by implementing a four-pronged approach that measures performance to develop consistent benchmarks and continue improving performance, ensuring sufficient rigor for scalability and long-term success.

- First, DHS used and will continue to use a rigorous and repeatable qualitative and quantitative criteria for measuring tool performance. The results of these efforts were presented in a Homeland Security Advanced Research Projects Agency interim report titled, "Social Media Analytics Capability Testing: Independent Assessment," dated June 30, 2016, and a final report, dated October 28, 2016 (copies of which have been provided to the OIG under separate cover). Specifically, various metrics were used to characterize tool performance in the following categories: Analysis, Data Management, Information Sources, Language Technology, Reporting, System, and Usability.

- Second, although DHS Component pilots have not yet identified true benchmarks for future operational pilots' success, they do consistently collect and analyze a comprehensive collection of metrics to measure the performance of ongoing research and development pilots, including the (a) processing time per case, (b) number of queries conducted, (c) number of cases where relevant information was returned, (d) number of returned documents for each query, (e) number of social media accounts found, (f) number of documents collected, (g) number of travel confirmations, and (h) number of Social Media Assessment reports written when information of interest is found. By June 2017, DHS intends to have developed mechanisms to collect metrics on the outcome of cases where relevant social media information was returned to determine how frequently social media information is relied on during the screening process.

- Third, performance measures such as project milestones are reported on a weekly basis to the Task Force using a Plan of Action and Milestones reporting function. Further, the DHS effort goes beyond conducting pilots by including the creation of a new entity, the centralized, shared screening and vetting capability referred to in the draft report as the Center of Excellence.

- Fourth, the Task Force's activities and pilots' performance are memorialized in a weekly agenda, discussed during a weekly conference call with Task Force members, and disseminated to the Task Force and DHS leadership in weekly summaries. Specifically, DHS Components report select metrics measuring their respective pilot performance (e.g., case processing throughput measures and the number of social media assessments completed).

UNCLASSIFIED

DHS will continue to identify and refine new and existing metrics to measure social media screening pilots' performance, to include identifying benchmarks for the various tools tested. Currently, the Under Secretary for Intelligence and Analysis, in his delegated role by the Secretary as the Department's Counterterrorism Coordinator, is Co-Chairing the Task Force and overseeing the pilots. Developing the Department's social media screening capability is a counterterrorism function and will be overseen by the DHS Counterterrorism Coordinator to ensure continuity when the Task Force eventually sunsets and its responsibilities are transitioned into DHS operational functions.

The next DHS social media screening pilot is scheduled to begin in January 2017, and the Department will continue to identify clearly defined successful outcomes from the technological, research, and productivity perspectives. DHS will also increase its efforts to improve the transparency and appropriate socialization of metrics used by Components by attaching them to the Task Force's weekly conference call readouts.

DHS believes that the actions detailed above address the OIG's recommendation and respectfully requests it be considered resolved and closed.

Appendix B
Center of Excellence

The COE concept of operations envisions the center conducting social media activities on behalf of components that lack resources or expertise and supporting component-level social media screening programs. The COE will also identify new social media tools and opportunities, test and evaluate new and emerging technologies, and identify best practices for the appropriate sharing and collaborative use of social media within DHS and with external partners. The COE will set standards for social media use in relevant DHS operations while ensuring privacy and civil rights and civil liberties protections.

The task force also developed a proposal for the creation of a social media board and social media council to replace the existing task force and oversee the future governance of DHS' social media use and the COE. According to the proposed charter, the social media board will be a senior-level independent group that will ensure awareness of social media use and capabilities among DHS leadership and control DHS' social media use programs. The social media council will ensure working-level communication for social media use and capabilities, develop new policies and procedures, oversee performance management, and promote information sharing.

Appendix C
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Office of Intelligence and Analysis Audit Liaison
USCIS Audit Liaison
ICE Audit Liaison
S&T Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.

OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

EXHIBIT 14:

CCD Privacy Impact Statement

PRIVACY IMPACT ASSESSMENT

Consular Consolidated Database (CCD)

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Consular Consolidated Database (CCD)

(b) Bureau: Consular Affairs (CA)

(c) System acronym: CA CCD

(d) iMatrix Asset ID Number: 9

(e) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
CCD is currently undergoing an Assessment and Authorization (A&A) to renew its Authorization to Operate (ATO) status. The estimated ATO date is Winter 2018.

(c) Describe the purpose of the system:

CCD is a data warehouse that stores current and archived data from all of the Consular Affairs (CA) post databases around the world. CCD provides CA a near real-time aggregate of consular transaction activity collected domestically and at post databases worldwide.

CCD provides a database solution for centralized visa and American citizen services. The data is replicated from post databases to central CCD databases, and serves as a backup for post's

transaction activity. In addition, the data provides authorized CCD users the ability to create advanced metrics such as workload statistics and trend analysis.

CCD provides users with easy-to-use interfaces via the CCD web portal, and allows emergency recovery of post databases. Authorized Department of State and interagency users utilize the CCD Web Portal to view centralized data through various reports and to gain access to other CA and interagency applications.

CCD is the consolidated storage for the Bureau of Consular Affairs' visa and passport data. CCD uses Visa Opinion Information Service (VOIS) as a Graphical User Interface (GUI) for simplified access to visa data stored within the CCD. The Visa Office (VO) is the main user of VOIS for creating Security Advisory Opinions (SAOs) and Advisory Opinions (AOs) for visa applicants. VOIS does not collect data from individuals, but accesses information contained within the CCD.

CCD is also the repository of data flows between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), and other federal agencies that provide input into the visa and passport review and approval process.

As part of the visa adjudication process, visa applications generate biographic and biometric checks that are replicated to the central CCD databases. Central CCD then processes the checks or routes them to other agencies. Biometric checks include facial recognition and fingerprint checks. Biographic data is used for namechecks against data within central CCD and for interagency vetting. External agencies provide responses to central CCD, and central CCD returns the results to submitting posts.

CCD is used by internal and the external users/systems for the following purposes:

- Automated screening of applicants in the Consular Lookout and Support System (CLASS)
- Automated checking of applicant fingerprints
- Registration of applicant images for Facial Recognition (FR)
- Reports requesting data on a particular applicant or post, or data from multiple applicants or posts
- Reports that provide reference information for Department of State users, such as post codes and post directory information
- Supervisor and administrator reports to track work or review applicant data
- Distributing data to interagency partners for visa and passport vetting
- Reports which display the status of post databases and post upgrades
- Security Advisory Opinion (SAO)/Improvement Project (IP) processing by outside agencies

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

The CCD stores information about U.S. citizens and legal permanent residents (hereafter "U.S. persons"), as well as foreign nationals (hereafter "non-U.S. persons") such as nonimmigrant and immigrant visa applicants. The PII in CCD includes, but is not limited to:

- Names
- Home/business addresses
- Birthdates
- Biometric data (fingerprints and facial images)
- Phone numbers
- Email address
- Financial information
- Race
- Gender
- Identification numbers (e.g. social security numbers and alien registration numbers)
- Personnel Information
- Nationality
- Passport information
- Medical information (DS-2054, DS-3025, DS-3026, DS-3030)
- Legal information
- Education information
- Family information
- Arrests and convictions
- Social media indicators

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 U.S.C. 552a (Privacy Act of 1974 as amended);
- 8 U.S.C. 1101-1537 (Immigration and Nationality Act of 1952, as amended (INA)), including 8 U.S.C. 1104 (Powers and Duties of the Secretary of State) and 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens); and selected non-INA sections of Title 8 as listed in the Appendix to Bender's Immigration and Nationality Act Pamphlet, 2018 edition);
- Omnibus Consolidated Appropriations Act, 1997, PL 104-208, September 30, 1996
- Illegal Immigration Reform and Immigration Responsibility Act, PL 104-208, Div. C, September 30, 1996

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, PL 107–56, October 26, 2001
- Enhanced Border Security and Visa Entry Reform Act of 2002, PL 107-174, May 14, 2002
- Child Status Protection Act of 2002, PL 107–208, August 6, 2002 (an Act to amend the Immigration and Nationality Act of 1952);
- 18 U.S.C. 911, 1001, 1541–1546 (Citizenship, passport and visa crimes);
- 22 U.S.C. 2651a (Organization of the Department of State);
- 22 U.S.C. 3927 (Chief of Mission);
- 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and providing assistance to other agencies);
- 22 U.S.C. 211a et seq.(U.S. Passports);
- 22 U.S.C. 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number);
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries);
- 22 U.S.C. 2705 (U.S. Passports and Consular Reports of Birth Abroad);
- 22 U.S.C. 2671(b)(2)(A)-(B) and (d) (Evacuation assistance and repatriation loans for destitute U.S. Citizens abroad);
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance);
- 22 U.S.C. 2151n–1 (Assistance to arrested citizens) (Repealed, but applicable to past records);
- 22 U.S.C. 5501–5513 (Aviation disaster and security assistance abroad; mandatory availability of airline passenger's manifest);
- 22 U.S.C. 4195, 4196; (Official notification of death of U.S. citizens in foreign countries; transmission of inventory of effects) (22 U.S.C. 4195, repealed, but applicable to past records);
- 22 U.S.C. 2715b (notification of next of kin of death of U.S. citizens in foreign countries);
- 22 U.S.C. 4197 (Assistance with disposition of estates of U.S. citizens upon death in a foreign country);
- 22 U.S.C. 4193 (Receiving protests or declarations of U.S. citizen passengers, merchants in foreign ports);
- 22 U.S.C. 4194 (Lists and returns of seamen and vessels);
- 22 U.S.C. 4205–4207 (Services to American vessels or seamen, prohibitions);
- 46 U.S.C. 10318 (Wages on discharge of seaman in foreign port);
- 46 U.S.C. 10701-10711 (Responsibility for deceased seamen and their effects);

- 22 U.S.C. 2715a (Responsibility to inform victims and their families regarding crimes against U.S. citizens abroad);
- 22 U.S.C. 4215, 4221 (Administration of oaths, affidavits, and other notarial acts);
- 22 U.S.C. 4802 (Responsibility for security and protective functions of U.S. missions abroad and domestic Department of State offices);
- 26 U.S.C. 6039E (Information concerning resident status);
- 28 U.S.C. 1740, 1741 (Authentication of documents);
- 28 U.S.C. 1781–1783 (Judicial Assistance to U.S. and foreign courts and litigants);
- 42 U.S.C. 1973ff–1973ff–6 (Overseas absentee voting);
- 42 U.S.C. 402 (Social Security benefits payments);
- Sec. 599C of Public Law 101–513, 104 Stat. 1979, as amended (Claims to benefits by virtue of hostage status)(Benefits ended, but applicable to past records);
- 42 U.S.C. 14901–14954; Inter-country Adoption Act of 2000, as amended (Implementing legislation for the Convention on Protection of Children and Co-operation in Respect of Intercountry Adoption, done at The Hague on May 29, 1993);
- 22 U.S.C. 9001-9011, International Child Abduction Remedies Act (implementing legislation for the Convention on the Civil Aspects of International Child Abduction, done at The Hague October 25, 1980; assistance to applicants in the location and return of children wrongfully removed or retained or for securing effective exercise of rights of access);
- 22 U.S.C. 9101, 9111–9114, 9121–9125, 9141, International Child Abduction Prevention and Return (implementing legislation for the Convention on the Civil Aspects of International Child Abduction, done at The Hague October 25, 1980; reporting requirements, prevention measures, and other assistance on international parental child abduction cases);
- 50 U.S.C. App. 453, 454, Presidential Proclamation No. 4771, July 2, 1980 as amended by Presidential Proclamation 7275, February 22, 2000 (Selective Service registration);
- Executive Order 11295, of August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. Passports);22 C.F.R. Part 22 (Schedule of Fees for Consular Services –Department of State and Foreign Service);
- 22 C.F.R. Parts 40-42, and 46 (Visas);
- 22 C.F.R. Parts 50, 51 and 52 (Nationality Procedures and Passports);
- 22 C.F.R. Part 71 (Protection and Welfare of Citizens and Their Property);
- 22 C.F.R. Part 72 (Deaths and Estates);
- 22 C.F.R. Part 92 (Notarial and Related Services);
- 22 C.F.R. Part 93 (Service on Foreign State);
- 22 C.F.R. Parts 96 -99 (Intercountry Adoptions)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
STATE-26, Passport Records, March 24, 2015
STATE-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016
STATE-39, Visa Records; June 15, 2018
STATE -77, Country Clearance Records, October 3, 2011

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
- Schedule number:

A-15-001-01 Consular Services Policy File
Description: Consists of correspondence and reports which document the development and implementation of policies, procedures, agreements, regulations, and legislation pertaining to the provision of consular services. Excludes material regarding routine operational and administrative activities and material concerning matters for which other offices have primary responsibility
Disposition: Permanent. Retire to the RSC when 5 years old. Transfer to the National Archives when 15 years old.
DispAuthNo: NC1-059-77-28, item 1

A-15-001-02 American Citizens Services (ACS) system
Description: The American Citizens Services (ACS) system is an electronic case management application designed to track, monitor, and report on services provided to U.S. citizens traveling or living abroad. ACS supports domestic consular operations and consular activities at overseas Posts. ACS records include case level data on the following types of citizen services: arrest cases; citizenship issues; death notifications; financial assistance cases; loss of nationality cases;

lost and stolen passports; property cases; citizen registrations; and welfare and whereabouts cases. Record level data includes· biographic information, case information, and case activity log.
Disposition Temporary: Cut off when case closed/abandoned. Destroy 3 years after cut off or when no longer needed, whichever is later.
DispAuthNo: N1-059-09-40, item 1

A-15-002-01 General Policy Files (Abduction and Adoption) - Arrange by subject
Description: Memorandums, correspondence, telegrams, court decisions, briefing papers, and other material relating to matters handled by the Office of Children's Affairs.
Disposition Temporary: Permanent. Cut off files when 10 years old and transfer to RSC for transfer to WNRC. Transfer to the National Archives when 25 years old
DispAuthNo: N1-059-97-14, item 1

A-15-002-02 Child Custody/Abduction Case Files
Description: Cases reflect applications filed for the return of children abducted to countries that are party and not party to the Hague Abduction Convention. Included are requests for assistance in locating children taken by the other parent, legal proceedings, information of available courses of action, monitoring the welfare of a child, information on child custody laws and procedures in the host country, and related correspondence.
Disposition: Cases reflect applications filed for the return of children abducted to countries that are party and not party to the Hague Abduction Convention. Included are requests for assistance in locating children taken by the other parent, legal proceedings, information of available courses of action, monitoring the welfare of a child, information on child custody laws and procedures in the host country, and related correspondence.
DispAuthNo: N1-059-97-14, item 2

A-15-002-03 Adoptions Tracking Service (ATS)
Description: ATS records include the following types of information: unique identifier, case status and tracking information, application information, adoptive parent information. child information, Hague Convention documentation, inquiry and complaint information, and adoption agency information.
Disposition: Temporary. Cut off at end of calendar year when adoption case closes. Destroy 75 years after adoption case closed.
Disposition: N1-059-09-09, item 1

A-13-001-16 Passport Lookout Master
Description: This online information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have

been denied passports, or those who are not entitled to the issuance of full validity passport and those whose existing files must be reviewed prior to issuance.
Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)
DispAuthNo: N1-059-04-2, item 16

A-13-001-23 Routine Passport Application Status Check and Expedite Fee Upgrades Email
Description: Email messages regarding the status of passport applications and requests for expedited service.
Disposition Temporary: Destroy/delete when 25 days old
DispAuthNo: N1-059-98-03, item 1

A-13-002-02 Requests for Passports
Description: Copies of documents relating to selected passport requests.
Disposition: Temporary: Cutoff at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty five (25) years old.
DispAuthNo: N1-059-05-11, item 2

A-13-002-03 Tracking/Issuance System
Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition: Permanent: Delete when twenty five (25) years old.
DispAuthNo: N1-059-05-11, item 3

A-14-001-03 thru A-14-001-24 Tracking/Issuance System
Description: Visa records on Aliens.
Disposition/DispAuthNo: Permanent or as depicted by the specific record item disposition authority.

B-09-001-01a thru B-0900-10 Passport and Citizenship Case Files, Correspondence and Citizenship Requests
Description: These records pertain to American citizens abroad who have applied to overseas posts for passports, the renewal, amendment or extension of passports, or for registration and other citizenship services; and files pertaining to American citizens who have applied to territorial governments for passport services. Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition/DispAuthNo: The length of time the record will be kept is dependent on the specific item and the applicable disposition rules in B-09-001-01a -10.

B-09-002-01a Immigrant Visas Issuances (Consular Consolidated Database
Description: Information obtained from issued immigrant visa application forms (DS-23, 260, and related forms) and supporting documentation. Immigrant visa case records potentially include the following types of case level data: unique identifier; applicant personal and biographical data; adjudication data; visa class information; visa clearance and name check data; case summary data; case status data; and notes

Disposition: Temporary. Cutoff at end of calendar year when issued. Destroy 11 years after issuance.
DispAuthNo: N1-084-02-02, item 1a

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public (are U.S. citizens or aliens lawfully admitted for permanent residence)
☐ U.S. Government/Federal employees or Contractor employees
☒ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No

- If yes, under what authorization?

26 USC§ 6039E – Information Concerning Resident Status
Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008

(c) How is the information collected?

All data is voluntarily provided by applicants upon completion of applications from the system in which services are being requested. The data is stored on the respective systems that collect it. Through the CCD replication process, a copy of the data is stored in the CCD from the consular systems domestically, at posts, and from external government agencies. The data collected from domestic and post applications are replicated from the systems' databases to the CCD.

(d) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other
- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

CA's Consular Systems and Technology (CST) teams monitor the databases to ensure replication from post to central is consistent and accurate. The configuration management procedures and extensive monitoring and analysis utilities provide daily updates on the data and related software both within the CCD and the systems at posts.

No data is collected by CCD from applicants. Information accuracy is managed in accordance with the system's procedures where the end user is submitting an application for services.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Data is replicated from post databases to the CCD database approximately every 60 seconds. Requests go directly from the post database server to the Local Traffic Manager server, which sends the request to the CCD database cluster for storage.

Ensuring posts'/federal agency information is current is a process managed in accordance with the system where the end user is submitting an application requesting services.

(g) Does the system use information from commercial sources? Is the information publicly available?

Some information stored in the CCD, such as names, addresses, birth dates, race, social media indicators, and country of origin, submitted by federal agencies may come from commercial databases and/or public records. This data is used by analysts to support national security, U.S. border security, official government business and/or federal law enforcement.

(h) Is notice provided to the individual prior to the collection of his or her information?

Although CCD maintains and processes information with U.S. person data that is subject to the Privacy Act and non-citizen data that is subject to INA 22(f), the CCD system is not a public facing system. The data in CCD is replicated from other systems after the applicant provides documents/information to the Department of State when applying for consular services. Notification is provided by the visa and passport applications that originally collect the information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, **how** do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

CCD information is replicated from other Department of State /Federal agency systems that provide the notice and consent at the information collection point for services requested. Consent is documented in the visa and passport applications and in case information.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII items replicated in the CCD system are the minimum necessary to perform the actions required by this system supporting visa and American citizen services. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the systems to perform the functions for which they are intended.

5. Use of information

(a) What is/are the intended use(s) for the information?

The intended use of the PII in the CCD is to support the Department of State's centralized visa and American citizen services program. The information consists of current and archived data from post databases and other federal agencies to support the transaction process in reviewing and providing consular services.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information is for the management of the Department of State's centralized visa and American citizen services programs. The collection is required to make determinations for granting the various consular services being requested.

(c) Does the system analyze the information stored in it?

☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the information?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Internally: Department of State users, including post users and associated systems.

The following are Department of State interconnected system(s) to CCD;

- Adoption Tracking Service (ATS)
- American Citizen Services (ACS)
- Automatic Biometric Identification System (ABIS)
- Automated Cash Register System (ACRS)
- Consular Electronic Application Center Portal (CEAC)
- Consular Lookout and Support System (CLASS)
- Consular Shared Tables (CST)
- Diversity Immigrant Visa Information System (DVIS)
- Consular Data Information Transfer System (CDITS)
- electronic Document Processing (eDP) Web
- Immigrant Visa Allocation Management System (IVAMS)
- Immigrant Visa information System (IVIS)
- International Parental Child Abduction (IPCA)
- Internet-based Registration Service/Consular Task force (IBRS/CTF)
- Enterprise Visa Application Forms (EVAF)
- Smart Traveler Enrollment Program (STEP)
- Immigrant Visa Overseas (IVO)
- Non-Immigrant Visa (NIV)
- Ten Print Live Scan (TPLS)
- Online Passport Status Service (OPSS)
- Passport Information Electronic Records System (PIERS)
- Passport Lookout Tracking System (PLOTS)
- Passport Records Imaging Systems Management (PRISM)
- Travel Document Issuance System (TDIS)
- Visa Opinion Information System (VOIS)
- Waiver Review System (WRS)

External Federal Agencies:

- Department of Homeland Security (DHS)
- Department of Commerce
- Department of Defense (DoD)
- Department of Justice (DOJ)
- Government Printing Office (GPO)
- Office of Personnel Management (OPM)
- Federal Bureau of Investigation (FBI),
- Other Interagency Partners

Each interagency partner has at least one Certifying Authority who is responsible for managing the users within the organization. Certifying Authorities are government employees who use the CCD to approve account requests and assign CCD roles appropriate for each user's job requirement. CCD roles determine the access to data.

(b) What information will be shared?
The various PII information listed in paragraph 3d is shared internally and externally based on the requirement.

(c) What is the purpose for sharing the information?
Sharing of information is required for the submission, processing, adjudication and approval/denial decisions of consular services.

(d) The information to be shared is transmitted or disclosed by what methods?
Information transmitted internally is via interconnected State Department systems.

Information is transmitted via interagency partners using Department of State approved secure transport layer security methods and interconnections.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal recipients, within the Department of State, must comply with U.S. government requirements for the protection and use of PII. These safeguards include but are not limited to security training and following internal Department policy for the handling and transmission of "Sensitive but Unclassified" information. In addition, all Department users are required to attend annual security awareness training to reinforce safe handling practices of information. Internal sharing requires a connection agreement and OpenNet users with privileged role-based access to manage the connection. Communication is secured using transport level security.

External agencies that share information with CCD interconnect through either the managed Multi-Protocol Label Switching (MPLS) or connection via the Department of State's extranet. CCD is not internet facing. All external agencies that share information with the CCD are required to sign a Memoranda of Understanding (MOU) with the Department of State, which generally defines a set of responsibilities and requirements. Items generally covered in the MOU include, but are not limited to: Trusted Behavior Expectations, User Community, Access Controls, Audit Trail Responsibility, Data Ownership, Security Parameters, Incident Handling and Reporting, Antivirus and Security Training and Awareness.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to unauthorized parties: Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization, and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

b. Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal, or other.

The Department of State mitigates these risks by enforcing rules and requirements using a multifaceted approach to security requirements regarding:

- Frequent security training on information security for all users, including the safe handling and storage of PII, "Sensitive but Unclassified", and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization, and need-to-know.

- System authorization and accreditation process along with continuous monitoring. Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared internally are encrypted as per the Department of State's Security Configuration Guides' security policies and procedures.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

Individuals are unable to access their information in the CCD. CCD does not collect information directly from applicants. CCD data originates from consular affairs visa and passport systems and from interagency partner systems.

Notices to individuals on how to access their information are provided at the point of collection of information for the system where services are being requested. Procedures for notification and redress are also published in the System of Records Notice (SORN) Passport Records – STATE-26, Visa Records-STATE -39, and in rules published within 22 CFR 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

Procedures are provided to individuals at the point of data collection, prior to replication into the CCD. CCD does not collect information directly from applicants. CCD data originates from consular systems and from interagency partners.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Procedures are provided to individuals at the point of data collection, prior to replication into the CCD. The source system where the data originates provides notices on how to correct information.

Guidance is also outlined in SORNS STATE 26 (Passport Records) and STATE 39 (Visa Records) and in rules published at 22 CFR 171, informing the individual how to inquire about the existence of records, how to request access to records, and how to request amendment of a record.

8. Security Controls

(a) How is the information in the system secured?
The CCD system is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous

monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Applications are configured according the Department of State's Security Configuration Guides to optimize security while still providing functionality. This complies with federal regulations and the Federal Information System Management Act (FISMA). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

To access the CCD system, persons must be authorized users of the Department of State's unclassified network, which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Each authorized user must electronically agree to the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the CCD system is role based, and restricted according to job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Information System Security Officers determine the access level needed by a user to ensure it correlates to the user's particular job function and level of clearance.

Data shared with other government agencies is carefully regulated according to an MOU and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The level of access granted to CCD restricts the data that may be viewed and the degree to which data may be modified. Administrative activity is monitored, logged, and audited.

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with Department of State Security Configuration Guides and conduct annual control assessments (ACA) to ensure that all

systems/applications comply and remain compliant with Department of State and federal policies. Additionally, configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor OpenNet-connected systems that host CA's major and minor applications for any changes to security controls.

The execution of privileged functions (e.g., administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with Department of State Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State Security Configuration Guides, auditing is enabled to track events on the host operating systems and back-end database servers.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

Operating system (OS) level auditing is set in accordance with the Department of State Security Configuration Guides. The OS interface allows the system administrator or ISSO to review audit trail information through the Security Log found in the Event Viewer. In addition to the security log, the system log and application log provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, mandatory annual Cyber Security Awareness training, with a privacy component, is required for all authorized users. The Department of State's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users digitally agree to the rules and acknowledge that they must protect PII through appropriate safeguards to ensure security, privacy and integrity. All Department of State users are required to complete the mandatory FSI course, PA 459 Protecting Personally Identifiable Information.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No
If yes, please explain.

To combat the misuse of information by personnel, numerous management, operational, and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists, are in use. System and information integrity auditing are implemented to monitor and record possible attempts of unauthorized access or data manipulation. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?

Organizations or individuals whose PII has been breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss.

Security measures are in place to minimize that risk, and to minimize the risk of harm to Department of State programs or the public interest through an unauthorized release of sensitive information. The security measures listed above were implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

The following personnel have access to the CCD: Post users/OpenNet-based users, Domestic users, CCD Administrators (System, application, database, network, and web) and External Agency Users.

(b) How is access to data in the system determined?

Access is determined and based on individual job functions which are approved by the supervisor and ISSO. Access is role based and the user is granted only the role(s) required to perform officially assigned duties. Interagency account access is granted by the Consular Affairs Visa Office and determined based on their mission and the Department's mission and authorities.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

☒Yes ☐No

Information is documented in the CCD System Security Plan. The plan includes information regarding roles and system access to data.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Users other than administrators will not have access to all data in the system. Separation of duties and least privilege is employed allowing users access to only the data required and approved by the supervisor to perform official duties.

Internal Department of State Users

Post Users/OpenNet-based Users

Post users include U.S. Citizens and local hires from the country where the U.S. embassy or consulate is located. All of these users can view CCD data, but there are restrictions to which data each user has access, based on job responsibility.

Domestic Users/OpenNet-based Users

Domestic users within the United States include both U.S. government employees and contractors. Domestic organizations are made up of groups of people who either work at the same physical location or have related job assignments or both. Each domestic organization has at least one Certifying Authority who is responsible for managing the users within the organization. Certifying Authorities are government employees who use the CCD to approve account requests and assign CCD roles appropriate for each user's job requirement.

Administrators (System, application, database, network and web)

Administrators include both U.S. government employees and contractors. CCD System Administrators are responsible for daily CCD maintenance, including establishing access control lists, backups, managing user accounts, software upgrades, patches, database configurations and establishing, activating, modifying, reviewing, disabling, and removing accounts.

External Agency Users

In addition to the users within Department of State, CCD data is used by numerous external agencies. These agencies are able to access CCD through a web interface (CCDi) via the Department's extranet. Once in CCDi, users are permitted access to the appropriate CCD data marts based on their assigned user role.

Each external agency has at least one Certifying Authority who is responsible for managing the users within the organization.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

-Access control policies and enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role based as required by policy.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Audit logs are reviewed at the Application, Database, and System level,

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN) and activities while logged in can be traced to the person that performed the activity.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DOC SOCIETY et al.,

Plaintiffs,

v.

ANTONY J. BLINKEN, *in his official capacity as Secretary of State*, et al.,

Defendants.

Civil Action No. 19-3632 (TJK)

ORDER

For the reasons set forth in the accompanying Memorandum Opinion, it is hereby **ORDERED** that Defendants' Motion to Dismiss, ECF No. 31, is **GRANTED IN PART** and **DENIED IN PART**. Insofar as the motion seeks dismissal for lack of subject-matter jurisdiction, it is **DENIED**. Insofar as the motion seeks dismissal for failure to state a claim, it is **GRANTED**. It is further **ORDERED** that Plaintiffs' Complaint, ECF No. 1, is **DISMISSED WITH PREJUDICE**. This is a final, appealable Order. The Clerk of Court is directed to close the case.

SO ORDERED.

/s/ Timothy J. Kelly
TIMOTHY J. KELLY
United States District Judge

Date: August 11, 2023

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DOC SOCIETY et al.,

Plaintiffs,

v.

ANTONY J. BLINKEN, *in his official capacity as Secretary of State*, et al.,

Defendants.

Civil Action No. 19-3632 (TJK)

MEMORANDUM OPINION

When the President ordered federal agencies to vet entrants to the United States more thoroughly, the State Department responded by telling visa applicants to disclose their social-media activity. Plaintiffs, two organizations that foster and promote documentary films, say that policy violates the First Amendment and the Administrative Procedure Act. But both claims run headlong into the discretion entrusted to Congress and to the President to set immigration policy and to enforce our immigration laws. Thus, Plaintiffs have failed to state a claim, and the Court will grant Defendants' motion to dismiss the case.

I. Background

The social-media-disclosure requirement now forms part of the procedure for requesting a visa to enter the United States. So the Court begins with a brief explanation of the legal framework surrounding that procedure. The facts below are drawn from Plaintiffs' complaint because the Court is resolving a motion to dismiss.

A. Legal Background

Aliens may not be admitted to the United States without a visa. *See* 8 U.S.C. §§ 1181(a), 1182(a)(7). Consular officers may issue visas after a "proper application." *Id.* § 1201(a)(1). The

statutory criteria for a proper application differ slightly between "immigrant" and "nonimmigrant" visas. *See id.* § 1202(a), (c). But both types of applications must include "such additional information necessary to the identification of the applicant . . . and the enforcement of the immigration and nationality laws as may be by regulations prescribed." *Id.*

Many factors can render an alien inadmissible. *See generally* 8 U.S.C. § 1182(a). Statutory grounds for inadmissibility include the alien's health, criminal history, risks to national security, ability to earn income, occupation, immigration history, documentation, and ineligibility for citizenship. *See id.* If a consular officer determines that an alien has any forbidden attribute, she must deny the application. *Id.* For denials based on most statutory grounds, the officer must give the applicant written notice of the denial that "lists the specific provision or provisions of law under which the alien is inadmissible." *Id.* § 1182(b). But no such notice is required if the officer determines that the alien is inadmissible because of his criminal history or for national-security-related reasons. *See id.* § 1182(a)(2)–(3), (b)(3). The State Department maintains an appeals process to review denials applicants wish to contest. ECF No. 31-8 at 12.

Visa applications are submitted via an online form. The forms are substantially similar for immigrant and nonimmigrant applications. *Compare* ECF No. 31-12 *with* ECF No. 31-13. Each form requests detailed information about the applicant's characteristics, life history, and plans for residing in the United States. *See, e.g.*, ECF No. 31-12 at 8–82. All aliens who apply for a visa from abroad complete one of those forms—including aliens who are already permanent residents of the United States, who often apply for new visas or for visa renewals from abroad. ECF No. 1 ("Compl.") ¶ 23.

The government retains the information collected on visa applications, even after it adjudicates the applications. The information is confidential. 8 U.S.C. § 1202(f). But the State

Department stores the information in a database that it shares with several federal agencies, including the Department of Homeland Security ("DHS"). Compl. ¶ 35. It also may share some stored information with other agencies, Congress, and state, local, tribal, and foreign governments. *Id.* ¶¶ 35–37. Part of the reason the government retains the information, it says, is to "enforce immigration and nationality laws, a responsibility that does not end once a visa has been granted." ECF No. 44 at 29; *see also* 8 U.S.C. § 1202(f)(2); ECF No. 31-8 at 10; ECF No. 31-9 at 10.

The Secretary of State ("the Secretary") promulgates regulations that interpret the visa-requirement statutes. *See* 22 C.F.R. § 40.1 *et seq*. Those regulations permit consular officers to request information beyond that requested by the application forms "whenever the . . . officer believes that the information provided in [the application] is inadequate to permit a determination of the alien's eligibility to receive [a visa]." *Id.* §§ 41.103(b)(2), 42.63(c). The regulations also bind consular officers to require applicants to complete the application forms described above. *Id.* §§ 41.103(b)(1), (3), 42.63(b). Insofar as those regulations have the "force of law," *United States v. Mead Corp.*, 533 U.S. 218, 226–27 (2001), they are entitled to deference under *Chevron, U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837 (1984).

B. Factual Background

1. The Agency Action

The challenged agency action began with an executive order. In 2017, President Trump directed the heads of four federal agencies to revamp the procedures for vetting visa applications. *See* Exec. Order No. 13,780 § 5(a), 82 Fed. Reg. 13209, 13215 (Mar. 6, 2017). Broadly, the new program was supposed to increase the government's capacity to verify an applicant's identity, assure his candor, and gauge the likelihood that he would participate in crime or terrorism. *See id.*

In response, the State Department proposed a change to its online visa forms. It sought to collect, among other things, information about the social-media platforms an applicant had used

in the five years before the application.[1] The proposed addition to the forms would also have required applicants to divulge their "identifiers"—that is, the usernames, handles, or other monikers associated with their social-media accounts. 83 Fed. Reg. at 13806–07. That information would allow the State Department to review an applicant's posts, interactions, and associations.

That proposal's notice-and-comment process generated intense interest. Roughly ten-thousand comments raised concerns related to free speech and association, privacy, and efficacy. Compl. ¶ 26. The State Department responded to those comments in sixteen groups for immigrant visas, *see* ECF No. 31-8 at 4–19, and in twenty groups for nonimmigrant visas, ECF No. 31-9 at 5–20. It noted that its proposal would collect only information that an applicant had shared publicly on social media. ECF No. 31-8 at 9. Still, it acknowledged that the collection would nullify the anonymity that some social-media platforms afford their users. *Id.* The State Department explained that it would use a collection method that "best safeguards" the information's transmission to the consular officer and then treat the data as confidential under 8 U.S.C. § 1202(f). *Id.* at 9–10. As for efficacy, it concluded that the proposal would help screen "visa applicants for specific visa ineligibility grounds" and verify their identities. *Id.* at 14.

The State Department implemented a version of its proposal by adding questions to its visa-application forms. Compl. ¶ 27. Visa applicants must now indicate whether they have used any listed social-media platform in the last five years. Compl. ¶¶ 28–30. If they have used a listed platform, they must provide the account's identifier, even if the account is pseudonymous. Compl. ¶¶ 28–31. Applicants may also provide the same information for social-media platforms that are

[1] 60-Day Notice of Proposed Information Collection: Application for Immigrant Visa and Alien Registration, 83 Fed. Reg. 13806, 13806 (Mar. 30, 2018); 60-Day Notice of Proposed Information Collection: Application for Nonimmigrant Visa, 83 Fed. Reg. 13807, 13807 (Mar. 30, 2018).

not listed on the forms. Compl. ¶¶ 28–30. Those requirements apply to almost all visa applicants, including those who already reside in the United States but are applying for a new visa from abroad. Compl. ¶¶ 32–33.

When President Biden took office, he revoked the executive order that prompted the disclosure requirement. Proclamation No. 10141 § 1, 86 Fed. Reg. 7005, 7005 (Jan. 20, 2021). The State Department then began a "policy review" that included reconsideration of the requirement. *See* ECF No. 52 at 1; *see also* ECF No. 54 at 2. More recently, the State Department represented that it decided not to make "imminent changes" to the requirement, although the policy remains "under discussion." ECF No. 58 at 1. Thus, the disclosure requirement remains in place to this day, despite the change in administrations.

2. Plaintiffs

Plaintiffs are two documentary-film organizations that help produce films all over the world. Compl. ¶¶ 40–41. The first, Doc Society, helps fund documentary films, in part by hosting events that connect funders and filmmakers. Compl. ¶ 40. It also promotes such films in hopes of achieving social change. *See id.* The second organization, International Documentary Association ("IDA"), funds and promotes documentary films too, but it also hosts events to help filmmakers with the more practical aspects of their work. *See* Compl. ¶ 41.

Plaintiffs' activities rely on collaboration with many foreign nationals. IDA has members in fifty-three countries. Compl. ¶ 41. Doc Society has no members, Compl. ¶ 40, but it has "partners" in diverse countries, Compl. ¶ 42. By "partners," it means "filmmakers, advocates, activists, and other[s]," whom it invites to events and helps make films. *See* Compl. ¶ 47. Both organizations host in-person events where "non-U.S. members and partners" must "travel to the United States." Compl. ¶ 45. Doc Society also believes that its film-funding efforts depend on the ability of its non-U.S. partners to meet face-to-face with "potential funders or activists." Compl. ¶ 44.

Many of Plaintiffs' foreign members and partners thus plan to visit the United States and require visas to do so. Compl. ¶ 42.

Plaintiffs consider social media "an indispensable research, education, and communication tool." Compl. ¶ 46. Essentially, they use it to identify new potential projects, members, and partners, to promote films and political messages, and to share resources. *See* Compl. ¶¶ 47–48. Their members and partners use it for similar purposes. *See* Compl. ¶¶ 49–50. Some of those members and partners use social media pseudonymously, whether out of concern for their safety or to aid in researching groups whose aims they do not share. *See* Compl. ¶ 51.

Some of Plaintiffs' members and partners who both need visas and use social media do not wish to divulge their online activities to the State Department. They fear two types of potential harm. First, social-media use might disadvantage a user's visa application. *See* Compl. ¶¶ 57–59. For example, a consular officer might misinterpret a user's speech or impute to him the speech of others in his network. *See* Compl. ¶¶ 57–58. And even if those events do not cause an application to be denied, they may still lead to processing delays. Compl. ¶ 59. Second, people other than consular officers—including officials of foreign governments—might learn of a user's posts or associations. Compl. ¶¶ 60–61. That could occur by intentional information sharing, Compl. ¶ 60, or through data breaches, which have happened before, Compl. ¶ 61.

Plaintiffs' members and partners have responded in two ways. Some users have reduced their social-media presence by, for example, avoiding political subjects or by refraining from associating with certain individuals. *See* Compl. ¶¶ 54–55. Others have elected not to apply for a visa or visit the United States. Compl. ¶ 56.

Plaintiffs say both these responses harm them. When their members and partners reduce their social-media use, Plaintiffs have less information from which they can identify new members,

partners, issues, and potential films. *See* Compl. ¶¶ 66–68. When their members and partners refuse to travel to the United States, attendance at Plaintiffs' events declines, and Plaintiffs are able to fund and screen fewer films. *See* Compl. ¶¶ 70–72. Plaintiffs have responded by spending more resources to "find and engage with members and partners . . . [,] to support and promote the work of their members and partners[,] and to recruit new members, partners, and projects" given their reduced ability to connect on social media or persuade foreign nationals to visit the United States. Compl. ¶ 75.

C. Procedural History

Plaintiffs filed suit not long after the disclosure requirement took effect. They bring two claims. First, they allege that the disclosure requirement violates the Administrative Procedure Act ("APA"). Compl. ¶ 77. Second, they contend that the requirement transgresses the First Amendment. Compl. ¶ 78. They ask the Court to hold the disclosure requirement unlawful, enjoin Defendants from enforcing it, and order them to "expunge all information collected" by the social-media questions. Compl. at 34. Defendants move to dismiss. ECF No. 31. They contend that Plaintiffs lack standing to challenge the disclosure requirement, ECF No. 31-1 at 20–38, and that they have failed to state a claim, *id.* at 38–56. Three groups of amici join Plaintiffs in opposing that motion. ECF Nos. 32, 35-1, 37-1, and 39-1.

With that motion pending, the Court stayed the case after President Biden revoked President Trump's executive order and announced a review of the disclosure requirement. Minute Order of Mar. 31, 2021. The Court lifted that stay several months later when Defendants did not withdraw the disclosure requirement. *See* Minute Order of Aug. 18, 2021; Minute Order of Oct. 20, 2021. At this point, no policy change appears forthcoming that would moot the case. *See* ECF No. 58 at 1. Thus, the Court will resolve Defendants' motion.

II. Legal Standards

Defendants' motion relies on Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). Under Rule 12(b)(1), Plaintiffs have the burden to establish standing. *Little v. Fenty*, 689 F. Supp. 2d 163, 166–67 (D.D.C. 2010). That burden "grows heavier at each stage of the litigation." *Osborn v. Visa Inc.*, 797 F.3d 1057, 1063 (D.C. Cir. 2015). To survive a motion to dismiss, Plaintiffs need only allege a qualifying "injury resulting from [Defendants'] conduct." *Id.* (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). The Court must "assume the truth of all material factual allegations in the complaint and . . . grant[Plaintiffs] the benefit of all inferences that can be derived from the facts alleged." *Am. Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (quotation omitted).

Under Rule 12(b)(6), Plaintiffs' complaint must "contain sufficient factual matter . . . to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quotation omitted). A claim is plausible if "it contains factual allegations that, if proved, would allow the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Hurd v. District of Columbia*, 864 F.3d 671, 678 (D.C. Cir. 2017) (quotation omitted). Again, the Court must "accept all the well-pleaded factual allegations of the complaint as true and draw all reasonable inferences from those allegations in the plaintiff's favor." *Id.* (quotation omitted). But it must disregard "a legal conclusion couched as a factual allegation." *Cason v. NFL Players Ass'n*, 538 F. Supp. 3d 100, 109 (D.D.C. 2021) (quotation omitted).

III. Analysis

For the reasons explained below, the Court concludes that (1) under this Circuit's binding precedent, Plaintiffs have shown they have organizational standing to bring suit, but (2) they have failed to state a claim under either the APA or the First Amendment. Thus, for that reason, the Court will grant the motion to dismiss.

A. Plaintiffs Have Organizational Standing Because the Disclosure Requirement Allegedly Impedes Their Activities

As a threshold matter, the Court must ensure Plaintiffs have standing. *See Freedom Watch, Inc. v. McAleenan*, 442 F. Supp. 3d 180, 186 (D.D.C. 2020); *see also Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94 (1998). That is, it must ensure that Plaintiffs have "clearly allege[d] facts demonstrating" they have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant[s], and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016) (alteration adopted). The alleged injury must be particular to Plaintiffs; they may not raise a "generally available grievance." *Lance v. Coffman*, 549 U.S. 437, 439 (2007) (per curiam).

Plaintiffs allege two forms of harm. First, they point to their own injuries. Compl. ¶ 39. Courts term that sort of standing "organizational" and treat the entity as they would "an individual plaintiff." *People for the Ethical Treatment of Animals v. U.S. Dep't of Agric.*, 797 F.3d 1087, 1093 (D.C. Cir. 2015) ("*PETA*"). Second, Plaintiffs assert the injuries to their "members and partners," both abroad and in the United States. Compl. ¶ 39. Courts call that type of standing "associational" and ask whether the entity has identified a particular member who would (1) "have standing to sue in his own right" based on (2) an interest "germane" to the entity's "purpose" and (3) whether the individual's personal participation in the suit is necessary. *Chamber of Commerce of the U.S. v. EPA*, 642 F.3d 192, 199–200 (D.C. Cir. 2011).

The Court concludes that, under this Circuit's precedent, Plaintiffs' allegations of organizational standing are enough to establish subject-matter jurisdiction. Specifically, Plaintiffs alleged a cognizable injury-in-fact because they have been deprived of information on which their regular activities rely. Compl. ¶¶ 66–67. That injury is traceable to Defendants' conduct because the informational vacuum allegedly was caused by the disclosure requirement. Compl. ¶¶ 54–55.

Likewise, an order vacating the requirement would restore the desired information. *See id.* Because that theory of standing can sustain Plaintiffs' challenge at this stage, the Court need not consider Plaintiffs' other theories.

1. Injury-in-Fact

A concrete injury is "foremost" among the standing requirements. *Steel Co.*, 523 U.S. at 103. An organization pleads a concrete injury by alleging facts showing that the challenged action has "perceptibly impaired" its "activities," leading to a "drain on the organization's resources." *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 379 (1982). By contrast, a "setback to the organization's abstract social interests" is not enough. *Id.*

Courts in this Circuit use a two-part test to apply that standard. *Tex. Low Income Hous. Info. Serv. v. Carson*, 427 F. Supp. 3d 43, 52 (D.D.C. 2019). First, they assess the alleged impairment to the organization's activities. *Elec. Privacy Info. Ctr. v. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371, 378 (D.C. Cir. 2017) ("*EPIC I*"). The impediment must frustrate the organization's "daily operations." *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 919 (D.C. Cir. 2015) (quoting *PETA*, 797 F.3d at 1094). And there must be a "direct conflict between the [defendants'] conduct and the organization's mission." *Elec. Privacy Info. Ctr. v. FAA*, 892 F.3d 1249, 1255 (D.C. Cir. 2018) ("*EPIC II*") (quotation and emphasis omitted). Second, courts ensure the organization "used its resources to counteract that harm." *EPIC I*, 878 F.3d at 378 (quoting *PETA*, 797 F.3d at 1094). That effort cannot be a "self-inflicted budgetary choice." *Id.* at 379 (quotation omitted). So litigation costs or extra advocacy efforts do not count. *Food & Water Watch*, 808 F.3d at 919.

Plaintiffs allege that their organizations have suffered an informational injury because the government has deprived them of desired information. *See Found. on Econ. Trends v. Lyng*, 943 F.2d 79, 84–85 (D.C. Cir. 1991) (describing the premises of "informational standing"). They say

they suffer such harm because the disclosure requirement "deters" their members and partners from sharing information on social media, which undermines their use of social media for research. Compl. ¶¶ 66–68.

Recent caselaw in this Circuit suggests that an informational injury is sufficiently concrete if an organization wishes to use a stream of information in a specific, regular way as part of its established activities. For example, a plaintiff had a concrete informational injury where an agency's alleged failure to apply a regulatory requirement meant the agency was not issuing reports that would have aided the plaintiff in preparing its *own* educational materials for the public, which it ordinarily did. *PETA*, 797 F.3d at 1095–96. Another plaintiff suffered a similar injury where an agency did not promulgate regulations that would have obviated informational materials that it prepared, saving the plaintiff time and money. *Am. Anti-Vivisection Soc'y v. U.S. Dep't of Agric.*, 946 F.3d 615, 619 (D.C. Cir. 2020). In both cases, the injury was concrete because the agency action "restrict[ed] the flow of information that [the plaintiffs used] to educate [their] members." *See Food & Water Watch*, 808 F.3d at 921. The sum of those cases is that the inability to use recurrent information for an organization's "services," "daily operations," or "activities" can perceptibly impair those activities. *See Ctr. for Responsible Sci. v. Hahn*, 809 F. App'x 10, 12–13 (D.C. Cir. 2020) (per curiam) (quotations omitted).

The Circuit has, however, consistently rejected allegations of informational injury based solely on an organization's lack of access to discrete, one-off pieces of information. It has sometimes characterized such allegations merely as harm to the organization's generalized advocacy or lobbying efforts. *E.g.*, *Food & Water Watch*, 808 F.3d at 921. So a plaintiff cannot show a concrete informational injury from only a single instance of missing information, even if it wishes to use that information to create educational materials. *See EPIC I*, 878 F.3d at 378–79. In such

cases, the alleged harm "sound[s] in pure issue advocacy." *EPIC II*, 892 F.3d at 1256. Only the interruption of a regular "flow of information" connected to an organization's ongoing activity is sufficient to show that the organization has been injured for standing purposes. *Food & Water Watch*, 808 F.3d at 921.

Moreover, under this Circuit's precedent, organizational plaintiffs' standing to seek recurrent information for specific, established activities does not depend on the organization's legal entitlement to the information.[2] If "information is essential to the injured organization's activities and . . . the lack of the information will render those activities infeasible," all that is needed is "a plausible link between the agency's action, the informational injury, and the organization's activities." *Competitive Enter. Inst. v. Nat'l Highway Traffic Safety Admin.*, 901 F.2d 107, 122 (D.C. Cir. 1990). That rule may well clash with the precept that an injury-in-fact is an invasion of a "legally protected interest." *PETA*, 797 F.3d at 1102–03 (Millett, J., dubitante) (quoting *Lujan*, 504 U.S. at 560). But it is the law of this Circuit, which this Court is bound to follow.

Thus, Plaintiffs have adequately alleged impairment to their activities—the first part of the test for organizational standing—by describing this "plausible link." The regular activity they wish to continue is the use of information posted on social media for research. Compl. ¶¶ 67–68. They explain the many ways they use that tool to provide their services.[3] Plaintiffs have further

[2] That is, a recurrent-information plaintiff need not show that "(1) it has been deprived of information that, on its interpretation, a statute requires the government or a third party to disclose to it, and (2) it suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure." *Friends of Animals v. Jewell*, 828 F.3d 989, 992 (D.C. Cir. 2016); *see also FEC v. Akins*, 524 U.S. 11, 20–25 (1998).

[3] Compl. ¶ 67 ("Doc Society [uses social media] to identify films to honor at its awards ceremonies [and] to research issues to explore in new programs . . . . Doc Society also relies on social media to identify new issues to address in its programs. Through Twitter, Doc Society identified [partners] whom it then connected with documentary filmmakers . . . ."); Compl. ¶ 68 ("IDA . . . follows numerous documentary filmmakers on [social media]. IDA pays close attention

alleged that the disclosure requirement makes its continued reliance on social media infeasible because many individuals whose speech they wish to receive have stopped speaking on relevant topics. Compl. ¶¶ 54–55. That allegation is plausible because Plaintiffs have explained why the disclosure requirement has induced these individuals' silence. Compl. ¶¶ 57–61. And the allegation is not speculative because Plaintiffs have explained that information on which they had been relying has already disappeared. Compl. ¶¶ 54–55.

Plaintiffs have also alleged a "direct conflict" between the disclosure requirement and their "mission[s]." *EPIC II*, 892 F.3d at 1255 (quotation and emphasis omitted). Defendants say Plaintiffs have shown only "indirect[ ]" effects, ECF No. 44 at 18, but that argument ignores relevant caselaw. The Circuit has explained that the direct-conflict requirement "exists because, if the challenged conduct affects an organization's activities, but is neutral with respect to its substantive mission, then it is entirely speculative whether the challenged practice will actually impair the organization's activities." *PETA*, 797 F.3d at 1095 (quotation omitted and alteration adopted). So regardless of whether an agency targeted its action at an organization's mission, a direct conflict exists if the action "hamper[s]" the agency's "stated mission" "in a non-speculative manner." *Id.* That is true here because, like in *PETA*, Plaintiffs have plausibly alleged that the agency action has made their mission harder to accomplish. *See id.* at 1095–96; Compl. ¶¶ 39–41 (explaining that Plaintiffs' missions include enabling the production and dissemination of documentary films). For the reasons already explained, the disclosure requirement directly conflicts with those missions.

Plaintiffs have also satisfied the second part of the organizational-standing test. They

to what filmmakers are saying on Twitter and Facebook to inform its educational and advocacy efforts on their behalf. For example, through social media IDA has discovered a number of cases of filmmaker censorship, which IDA has then investigated in order to assist the censored filmmakers and to alert its membership to the threats they may face in different countries. IDA addresses these and similar issues in [its programming].").

allege they diverted resources to counteract the informational harm. They explain that, because of social media's reduced efficacy, they expend more "time, staff resources, and funding to find and engage with members and partners." Compl. ¶ 75. Defendants point out that Plaintiffs do not "identify any other activities from which they have 'diverted' resources," but that observation is irrelevant. ECF No. 44 at 20. Defendants identify no case that requires Plaintiffs to specify which activities have yielded to their increased efforts to counter the agency action, and the Court can find none. Every organization has finite resources, so any increase in expenditures leaves less available for other purposes, making such a requirement unnecessary. All Plaintiffs must do is allege they have used more resources in a way they otherwise would not have. *See EPIC I*, 878 F.3d at 379.

Nor is Plaintiffs' injury self-inflicted in the relevant sense. True, Plaintiffs voluntarily spend the extra resources, but that fact does not address the relevant question. *See Equal Rts. Ctr. v. Post Props., Inc.*, 633 F.3d 1136, 1140–41 (D.C. Cir. 2011). An injury is not self-inflicted if money is spent "in response to, and to counteract, the effects of the defendants' [conduct]." *Id.* at 1140. Plaintiffs allege that they now need more resources to accomplish the same tasks they performed before the disclosure requirement. Compl. ¶¶ 67–68, 75. And they have drawn a "direct causal link between the [requirement] and [their] expenditures." *EPIC I*, 878 F.3d at 379 n.7; Compl. ¶¶ 55–61. So they have pled an organizational, informational injury-in-fact.

2. Traceability and Redressability

Of course, an injury is not the only standing requirement Plaintiffs must satisfy. Organizations, like other plaintiffs, must also allege facts showing "traceability" and "redressability." *Tex. Low Income Hous.*, 427 F. Supp. 3d at 57. Plaintiffs' allegations establish both elements.

Traceability and redressability are two sides of the same coin. The former element requires that the injury results from "the challenged action of the defendant," not "from the independent

action of some third party not before the court." *Simon v. E. Ky. Welfare Rts. Org.*, 426 U.S. 26, 41–42 (1976). The latter element requires that it is "likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Lujan*, 504 U.S. at 561 (quotations omitted). Those elements are closely linked because vitiating an injury's cause usually at least mitigates the injury. *See Dynalantic Corp. v. Dep't of Def.*, 115 F.3d 1012, 1017–18 (D.C. Cir. 1997). But they are still distinct because the former concerns the relationship between the injury and the defendant's conduct, while the latter concerns the relationship between the injury and the requested relief. *West v. Lynch*, 845 F.3d 1228, 1235–36 (D.C. Cir. 2017).

The difficulty for Plaintiffs is that they are not the subject of Defendants' conduct because they are not visa applicants. Instead, the injury to Plaintiffs materializes through the social-media decisions of third parties, for whom, as Defendants point out, the visa-application requirements of the United States government are "one of many factors" they consider in deciding what to say. ECF No. 44 at 19. Accordingly, Plaintiffs face "a considerably tougher row to hoe." *Tex. Low Income Hous.*, 427 F. Supp. 3d at 58. They must allege facts that allow the Court plausibly to infer how those third parties have acted and will act in response to an order in Plaintiffs' favor. *See Lujan*, 504 U.S. at 562.

Still, the Circuit has recognized that even an injury inflicted by third parties can be traceable to the government and redressable by an order to the government. That is true where the factual allegations present "substantial evidence of a causal relationship between the government policy and the third-party conduct." *Nat'l Wrestling Coaches Ass'n v. Dep't of Educ.*, 366 F.3d 930, 941 (D.C. Cir. 2004), *abrogated on other grounds by Perry Cap. LLC v. Mnuchin*, 864 F.3d 591 (D.C. Cir. 2017). Courts must inquire into the "logic" of the allegations; the allegation of causality itself is not enough. *See Renal Physicians Ass'n v. U.S. Dep't of Health & Human Servs.*, 489 F.3d

1267, 1275–78 (D.C. Cir. 2007). On the redressability element, that assessment means asking whether "the new status quo is held in place by other forces," so that even an order eliminating the original cause of the injury will not now redress it. *Id.* at 1278.

Plaintiffs' allegations show plausible traceability and redressability. They explain, relying on the explanations of some of their members and partners, that many now refrain from relevant speech on social media because they fear the views they share, even pseudonymously, "will be used against them during the visa process." Compl. ¶ 55. But those same people "previously used social media" to contribute to the information streams on which Plaintiffs rely. *Id.* Those allegations are not bare attributions because Plaintiffs explain in detail why their members and partners fear the disclosure requirement's effects. Compl. ¶¶ 57–63. And Plaintiffs seek an order that would eliminate the collection and storage of social-media identifiers and nullify its prior impact. *See* Compl. at 34. The most logical inference from those allegations, accepted as true, is that the order Plaintiffs request would restore the information on which they rely. In other words, their allegations present "substantial evidence of a causal relationship" between the social-media silence and the disclosure requirement, *Nat'l Wrestling*, 366 F.3d at 941, and there is no reason to think the "new status quo is held in place by other forces," *Renal Physicians*, 489 F.3d at 1278.

Plaintiffs' reliance on the explicit reasoning of the relevant third parties distinguishes this case from others in which traceability and redressability were found speculative. For example, the plaintiff in *Texas Low Income Housing* had alleged only that the legal change would "remov[e] an impediment" to the desired behavior of a third party and would make that behavior "far easier." 427 F. Supp. 3d at 59–60 (emphasis omitted). With no concrete reason to believe that the third party *would* behave differently, this Court disregarded those allegations as "conjecture." *Id.* at 60. So too in *National Wrestling*, where the plaintiffs could show no more than that a favorable order

would create "better odds" that their desired result would materialize. 366 F.3d at 939. Here, by contrast, the allegations show strong evidence that the sole "disincentive" to the third parties' otherwise-desired conduct is the agency action. *See Block v. Meese*, 793 F.2d 1303, 1308–09 (D.C. Cir. 1986); *see also Tozzi v. U.S. Dep't of Health and Hum. Servs.*, 271 F.3d 301, 308–09 (D.C. Cir. 2001) (finding that an agency action was a "substantial factor" in third parties' decisions (quotation omitted)).

Thus, at this stage, Plaintiffs have shown organizational standing to challenge the disclosure requirement. That conclusion, of course, relies on the Court's assumption that Plaintiffs' allegations are true and on its drawing of inferences in their favor. *See Osborn*, 797 F.3d at 1063–64. At later stages of litigation, Plaintiffs could "no longer rest on mere allegations, but must set forth by affidavit or other evidence specific facts." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 412 (2013) (quoting *Lujan*, 504 U.S. at 561) (cleaned up). But this Court has jurisdiction to reach the merits, so Defendants' Rule 12(b)(1) motion will be denied.

B. Plaintiffs Have Not Stated an APA Claim Because the Visa-Application Statute Presents a Judicially Unmanageable Standard

Plaintiffs' first claim arises under the APA. They ask this Court to "set aside" the disclosure requirement as "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" or "in excess of statutory . . . authority." Compl. ¶ 77; *see also* 5 U.S.C. § 706(2)(A), (C).[4] Plaintiffs explain that their APA claim has two aspects. First, they say the Secretary lacked the statutory authority to impose the disclosure requirement. ECF No. 32 at 32. Second, they contend that the rulemaking process was arbitrary and capricious. *Id.*

[4] Plaintiffs also bring a claim under 5 U.S.C. § 706(2)(B), which directs courts to set aside agency actions that are "contrary to constitutional right, power, privilege, or immunity." *See* Compl. ¶ 77. But that aspect of their APA claim is coterminous with their second claim under the First Amendment, so the Court will address it later.

Defendants attempt to refute those claims, but they also interpose two threshold obstacles to APA review. First, they argue that Congress committed to the Secretary the discretion to decide what information a proper visa application must contain. ECF No. 31-1 at 28–31. If that is true, the agency action is not reviewable under the APA. 5 U.S.C. § 701(a)(2). Second, they maintain that Plaintiffs fall outside the zone of interests of the Immigration and Nationality Act ("INA") and so cannot sue under its legal requirements. ECF No. 31-1 at 43–44. If either of those obstacles has merit, the Court must dismiss Plaintiffs' APA claim under Rule 12(b)(6). *See Sierra Club v. Jackson*, 648 F.3d 848, 853–55 (D.C. Cir. 2011) (agency discretion); *CSL Plasma Inc. v. U.S. Customs & Border Prot.*, 33 F.4th 584, 588 (D.C. Cir. 2022) (statutory zone of interests). In the end, the first obstacle proves insurmountable, so the claim must be dismissed.

The APA's "presumption of judicial review" is superseded if an "agency action is 'committed to agency discretion by law.'" *Dep't of Commerce v. New York*, 139 S. Ct. 2551, 2567 (2019) (quoting *Abbott Labs. v. Gardner*, 387 U.S. 136, 140 (1967), and 5 U.S.C. § 701(a)(2)). An action is unreviewably committed to agency discretion in "those rare circumstances where the relevant statute is drawn so that a court would have no meaningful standard against which to judge the agency's exercise of discretion." *Weyerhaeuser Co. v. U.S. Fish & Wildlife Serv.*, 139 S. Ct. 361, 370 (2018) (quoting *Lincoln v. Vigil*, 508 U.S. 182, 191 (1993)). That "exception" is "generally" limited to actions in "areas traditionally committed to agency discretion." *Dep't of Commerce*, 139 S. Ct. at 2568.[5] But it also applies if the statutory text "heralds Congress's judgment

[5] Examples include "a decision not to institute enforcement proceedings," *Dep't of Commerce*, 139 S. Ct. at 2568 (citing *Heckler v. Chaney*, 47 U.S. 821, 831–32 (1985)), "a decision by an intelligence agency to terminate an employee in the interest of national security," *id.* (citing *Webster v. Doe*, 486 U.S. 592, 600–01 (1988)), "the allocation of funds from a lump-sum appropriation," *Weyerhaeuser*, 139 S. Ct. at 370 (citing *Lincoln*, 508 U.S. at 191), and "a decision not to reconsider a final action," *id.* (citing *ICC v. Locomotive Eng'rs*, 482 U.S. 270, 282 (1987)).

to commit the decision exclusively to agency discretion." *Make the Road N.Y. v. Wolf*, 962 F.3d 612, 632 (D.C. Cir. 2020) (interpreting a statute that textually gave an agency head "sole and unreviewable discretion" (quoting 8 U.S.C. § 1225(b)(1)(A)(iii)(II))).

Defendants invoke that exception here. They claim that "Congress has given the Secretary of State broad discretion over the visa application process." ECF No. 31-1 at 40. They observe that visa applications lie "at the intersection of foreign policy and national security." *Id.* at 42. And they contend that the relevant statutes lack "any substantive standards against which to measure" the legality of this agency action. *Id.* at 41.

The relevant statutes require visa applications to be made "in such form and manner" "as shall be by regulations prescribed." 8 U.S.C. § 1202(a), (c). Both statutes specifically list, as information that applicants "shall state," an applicant's "full and true name" and his "date and place of . . . birth." *Id.* Applications for immigrant visas must also contain "any other name" an applicant has used "or by which he has been known" and his "age and sex." *Id.* § 1202(a). Those for nonimmigrant visas must also contain an applicant's "nationality, the purpose and length of his intended stay in the United States," and "his marital status." *Id.* § 1202(c). Finally, both statutes require an applicant to state "such additional information necessary to the identification of the applicant" "and the enforcement of the immigration and nationality laws as may be by regulations prescribed." *Id.* § 1202(a), (c).[6] The Secretary pointed to that final clause as authority to enact the disclosure requirement. *See* ECF No. 31-8 at 2; ECF No. 31-9 at 2.

The Circuit confronted a similar question about Section 1202(a) in *Legal Assistance for Vietnamese Asylum Seekers v. Department of State*, 104 F.3d 1349 (D.C. Cir. 1997) ("*LAVAS*").

[6] Section 1202(c) also contains the phrase "necessary to . . . the determination of his eligibility for a nonimmigrant visa."

The dispute in *LAVAS* concerned the place where an applicant could apply for an immigrant visa. *See id.* at 1350. Section 1202(a) allows applications to be made "at such place as shall be by regulations prescribed." That "broad language," the court explained, "grants to the Secretary discretion to prescribe the place at which aliens apply for immigrant visas without providing substantive standards against which the Secretary's determination could be measured." *Id.* at 1353. And the decision where to permit applications is the sort of action that "counsels against [judicial review]" because it requires the "balancing [of] complex concerns involving security and diplomacy." *Id.* So the Circuit held that the venue decision was committed to agency discretion by law. *Id.*

Defendants reason that "*LAVAS* compels dismissal of the Plaintiffs' APA claims." ECF No. 31-1 at 41. The Court disagrees. Deciding what information to require on a visa application is not the sort of decision "traditionally committed to agency discretion." *Dep't of Commerce*, 139 S. Ct. at 2568. And the statute contains a "meaningful standard" that, in the abstract, is capable of judicial application. *Weyerhaeuser*, 139 S. Ct. at 370.

Decisions traditionally committed to agency discretion are those over which Congress lacks or has relinquished shared control. *See Lincoln*, 508 U.S. at 191–92; *Shawnee Tribe v. Mnuchin*, 984 F.3d 94, 99–100 (D.C. Cir. 2021). Although that is often true "[i]n the foreign affairs arena," *Detroit Int'l Bridge Co. v. Canada*, 883 F.3d 895, 903 (D.C. Cir. 2018), a mere connection to a core executive power does not render a decision unreviewable, *see, e.g.*, *Dep't of Homeland Sec. v. Regents of the Univ. of Cal.*, 140 S. Ct. 1891, 1906–07 (2020) (holding that a decision that created a "program for conferring affirmative immigration relief" was reviewable). Even in areas related to foreign affairs and national security, actions may have a "focus for judicial review." *Id.* at 1906 (quoting *Chaney*, 470 U.S. at 832). Such a focus exists where Congress has

asserted control "by putting restrictions in the operative statute[ ]." *Shawnee Tribe*, 984 F.3d at 100 (quoting *Lincoln*, 508 U.S. at 193).

Sections 1202(a) and (c) contain several restrictions that provide a focus for judicial review. For one thing, both statutes require visa applications to contain specific elements. For another, the clauses under which the Secretary claimed authority for this action restrict the "additional information" to that "necessary" for various purposes. 8 U.S.C. § 1202(a), (c). Those attributes distinguish this part of the statute from that in *LAVAS*, where Congress provided only that the decision would be made by regulation, leaving the decision "entirely to the discretion of the Secretary." 104 F.3d at 1353. The presence of those limitations means that the statutes carry "no presumption of non-reviewability." *Shawnee Tribe*, 984 F.3d at 100.

Nor does the Court lack "law to apply." *Shawnee Tribe*, 984 F.3d at 99 (quotations omitted). Defendants point out that the phrase "may be . . . prescribed" in the statute implies that the Secretary has discretion. ECF No. 31-1 at 41–42 (citing *Haig v. Agee*, 453 U.S. 280, 294 n.26 (1981) (noting that "'may' expressly recognizes substantial discretion")). Maybe so, but Defendants do not answer the further question—"Discretion over *what*?" The word "may" modifies only the clause "be by regulations prescribed." That is, the Secretary has discretion over the decision whether to require additional information. 8 U.S.C. § 1202(a), (c). If he does so, the statute requires that the "additional information" be "necessary" to the listed purposes. *Id.* If Congress had intended to place no limitations on what kind of information the Secretary could require, it could have said nothing—as it did in the language analyzed in *LAVAS*. *Id.* § 1202(a) (Applications shall be "in such form and manner and at such place as shall be by regulations prescribed."). Its decision to limit the information—and even to do so in different ways for immigrant and nonimmigrant visas—shows that the word "necessary" limits the Secretary's discretion. *See City of Arlington v.*

FCC, 569 U.S. 290, 296 (2013) ("Congress knows to speak in plain terms when it wishes to circumscribe, and in capacious terms when it wishes to enlarge, agency discretion.").

Still, as Defendants observe, the legal standard must also be "judicially manageable." ECF No. 44 at 25 (quotation omitted); *see also Physicians for Social Resp. v. Wheeler*, 956 F.3d 634, 643 (D.C. Cir. 2020) (quotation omitted). In the usual sense, it is. True, the word "necessary" is fraught with possible interpretations. *See Nat. Res. Def. Council v. Thomas*, 838 F.2d 1224, 1237 (D.C. Cir. 1988) (explaining that the word's meaning "varies with context"). But courts confront and resolve that sort of ambiguity routinely. *See, e.g.*, *Safe Extensions, Inc. v. FAA*, 509 F.3d 593, 601 (D.C. Cir. 2007) (finding judicially manageable the statutory standard "necessary for safety"). Federal courts have long wrestled versions of this precise question. *See, e.g.*, *M'Culloch v. Maryland*, 17 U.S. 316, 413–14 (1819) ("The word 'necessary' . . . has not a fixed character, peculiar to itself. It admits of all degrees of comparison; and is often connected with other words, which increase or diminish the impression the mind receives of the urgency it imports."). Yet they have found answers. *See, e.g.*, *id.* at 421.

But other cases on which Defendants rely, such as *Center for Biological Diversity v. Trump*, 453 F. Supp. 3d 11 (D.D.C. 2020), ultimately persuade the Court to dismiss the claim. As these cases explain, applying some statutory standards "calls for sensitive judgments that Congress plainly intended" another branch of government to make. *Id.* at 38 (quotation omitted). For example, a judgment whether "military construction is 'necessary' . . . crosses the line into military policy." *Id.* And "the federal judiciary is ill-equipped to conduct reviews of the nation's military policy." *Nat'l Fed'n of Fed. Emps. v. United States*, 905 F.2d 400, 406 (D.C. Cir. 1990). The lesson of these cases is that courts must consider the *purpose* for which a statutory subject is to be judged necessary and avoid policy decisions entrusted to other branches of government.

Evaluating Plaintiffs' APA claim would require the Court to intrude on a similar policy decision entrusted to another branch of government. No matter what construction of "necessary" is right, evaluating the claim would involve, for both types of visas, determining what information is necessary to aid "enforcement of the immigration and nationality laws." *See* 8 U.S.C. § 1202(a), (c). But the law-enforcement value of the information at issue, if any, materializes only in the individual decisions whether to admit a particular noncitizen or to revoke a particular noncitizen's visa. That is, whether the information is necessary to enforce the law in a particular situation depends on a decision about how the law *should* be enforced in that situation. And that is precisely the sort of decision that calls for the executive branch to "balance factors peculiarly within its expertise." *Regents of the Univ. of Cal.*, 140 S. Ct. at 1906; *see also Chaney*, 470 U.S. at 831. Notably, the merits of the government's enforcement decisions in this area are judicially unreviewable. *See Saavedra Bruno v. Albright*, 197 F.3d 1153, 1160 (D.C. Cir. 1999). Thus, the Court could not judge the necessity of the information without impermissibly "second guessing the Secretary's assessment of [its law-enforcement] value" to officials in their exercise of judicially unreviewable executive power. *See Center for Biological Diversity*, 453 F. Supp. 3d at 38.

For that reason, at least one statutory purpose that might justify collecting the information presents no "subject[ ] fit for judicial involvement." *District No. 1, Marine Eng'rs' Beneficial Ass'n v. Mar. Admin.*, 215 F.3d 37, 42 (D.C. Cir. 2000). The Court cannot determine whether the statutory standard for necessity is satisfied without weighing "the Executive's . . . judgments on questions of foreign policy[,] national interest," and enforcement discretion. *See id.* So it must dismiss Plaintiffs' APA claim under Rule 12(b)(6). *Sierra Club*, 648 F.3d at 853–55.

C. Plaintiffs Have Not Stated a First Amendment Claim Because the Disclosure Requirement is Rationally Connected to Legitimate Government Interests

Plaintiffs' second claim is that the disclosure requirement violates the First Amendment.

Compl. ¶ 78. They explain that the requirement implicates the rights "to speak anonymously, to associate privately, and to receive information and ideas." ECF No. 32 at 44. They assert that the requirement further offends the Constitution by its overbreadth. *Id.* To evaluate Defendants' motion to dismiss that constitutional claim, the Court must decide first what tier of judicial scrutiny applies.[7] That is a "purely legal question" and so is appropriate for resolution on a motion to dismiss. *See Marshall Cnty. Health Care Auth. v. Shalala*, 988 F.2d 1221, 1226 (D.C. Cir. 1993).

Defendants say the Court's review here must be "limited given that the policy concerns a condition of entry into the United States by a foreign national." ECF No. 31-1 at 50. They therefore argue that the Court should apply a "deferential standard" of review. *Id.* Under that standard, they contend, the requirement passes muster because it "advance[s] the Government's legitimate national-security interest in sufficiently screening and vetting foreign nationals before they are allowed to enter the country." *Id.* at 56.

The Court agrees with Defendants that it must tread carefully. That is because the "admission and exclusion of foreign nationals is a 'fundamental sovereign attribute exercised by the Government's political departments largely immune from judicial control.'" *Trump v. Hawaii*, 138 S. Ct. 2392, 2418 (2018) (quoting *Fiallo v. Bell*, 430 U.S. 787, 792 (1977)). But even when that principle applies, courts must "engage[ ] in a circumscribed judicial inquiry" if the action "burdens

[7] *See, e.g.*, *Sanchez v. Off. of State Superintendent of Educ.*, 45 F.4th 388, 395–96 (D.C. Cir. 2022), *cert. denied*, 143 S. Ct. 579 (2023) (explaining that, "[a]t the motion-to-dismiss stage" on rational-basis review, "the plaintiff must plausibly allege facts showing that no reasonably conceivable state of facts could provide a rational basis for the challenged policy"); *Brown v. District of Columbia*, 390 F. Supp. 3d 114, 123–24 (D.D.C. 2019) (explaining that, where the application of a higher tier of scrutiny might depend on factual questions, "courts typically do not reach the merits of a First Amendment challenge at the motion-to-dismiss stage" (emphasis omitted)); *BEG Invs., LLC v. Alberti*, 85 F. Supp. 3d 13, 36–38 (D.D.C. 2015) (dismissing a First Amendment claim under Rule 12(b)(6) after concluding that the plaintiff had not plead facts "that must be analyzed with strict scrutiny").

the constitutional rights of a U.S. citizen." *Id.* at 2419; *see also Kleindienst v. Mandel*, 408 U.S. 753, 765–70 (1972) (asking only whether the immigration decision was facially based on "a legitimate and bona fide reason"). It follows that courts must also evaluate the burdens on the constitutional rights of foreign nationals, if those exist.[8] The Court thus begins by defining the scope of the constitutional rights at issue.

1. Constitutional Rights at Issue

Plaintiffs describe three ways in which they say the disclosure requirement burdens some individuals' constitutional rights. First, Plaintiffs argue that the chilling effect of the requirement—that is, its disincentive to speech and association—deprives U.S. citizens of the rights to hear the speech of would-be visa applicants and to associate with them. ECF No. 32 at 51–52. Second, they contend that the government has impermissibly conditioned eligibility for a benefit on the registration of visa applicants' speech and associations. *Id.* at 50–51. Third, they say the requirement unlawfully erases visa applicants' protected anonymity in their online speech and associations. *Id.* at 48–49.

Plaintiffs' first theory—which relies on the purported generalized right of U.S. citizens to *hear* the unidentified speech of unidentified persons—is flawed. Although the Supreme Court has recognized the "right to receive information and ideas," *Mandel*, 408 U.S. at 762 (quotation omitted), and the right to "associate for expressive purposes," *Roberts v. U.S. Jaycees*, 468 U.S. 609,

[8] The Supreme Court has never held that burdens on the constitutional rights of foreign nationals trigger even a circumscribed judicial inquiry in this area because, as reflected in *Trump v. Hawaii*, *Mandel*, and other such cases, the relevant foreign nationals had no such rights. *See Trump v. Hawaii*, 138 S. Ct. at 2419; *Mandel*, 408 U.S. at 762; *Kerry v. Din*, 576 U.S. 86, 88 (2015) (plurality opinion). But to the extent foreign nationals are protected by the U.S. Constitution, *see generally Nat'l Council of Resistance of Iran v. Dep't of State*, 251 F.3d 192, 200–03 (D.C. Cir. 2001), the Court sees no reason to treat burdens on their rights differently than those on the rights of citizens. The content of those rights is, after all, the same no matter who possesses them. *See id.* at 203–209 (applying the ordinary due-process standards to foreign organizations).

622–23 (1984), it has done so only in the context of specific speech and specific associations. In *Mandel*, for instance, the Court recognized that U.S. citizens were entitled to "hear, speak, and debate with" a particular noncitizen who had been denied entry into the country. 408 U.S. at 762. Similarly, in *Lamont v. Postmaster General*, the government refused to deliver specific mail considered "communist political propaganda" unless a recipient affirmed he wished to receive it. 381 U.S. 301, 303–04 (1965). The Court held that requirement was an "unconstitutional abridgement of the addressee's First Amendment rights." *Id.* at 307. Plaintiffs cite no case supporting the idea that U.S. citizens can claim a generalized right to hear more speech from or to form more associations with unidentified persons.

Put another way, Plaintiffs' theory conflicts with the precept that "freedom of speech presupposes a willing speaker." *Competitive Enter. Inst. v. U.S. Dep't of Transp.*, 856 F.2d 1563, 1566 (D.C. Cir. 1988) (alteration adopted) (quoting *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748, 756 (1976)). The Supreme Court has described speakers' rights and listeners' rights as "reciprocal." *Va. Citizens*, 425 U.S. at 757. For that reason, some courts have concluded that a listener's right is "derivative of the First Amendment rights of the speaker." *See Martin v. EPA*, 271 F. Supp. 2d 38, 47 (D.D.C. 2002). That is not always the case—the speakers in *Mandel* and *Lamont* lacked First Amendment rights—but that framing still captures the idea that rights to free speech and association exist only vis-à-vis specific expressive activity. *See also Cato Inst. v. SEC*, 438 F. Supp. 3d 44, 53–54 (D.D.C. 2020); *Hardy v. Hamburg*, 69 F. Supp. 3d 1, 19–20 (D.D.C. 2014). Thus, to rely on listeners' rights, Plaintiffs must "identify a willing speaker" who "would provide the information" some would-be listener or associate "would like to receive." *Competitive Enter. Inst.*, 856 F.2d at 1566.

Plaintiffs' complaint does not approach that specificity. Instead, Plaintiffs allege that the

disclosure requirement "deprives [U.S. citizens] of opportunities to hear from and engage with [noncitizens]" and that citizens "no longer enjoy" online interactions "to the same extent they previously did." Compl. ¶ 69. And they fear that their in-person events will suffer from reduced attendance, diluting their associational benefits. Compl. ¶ 73. These allegations fail to identify a particular instance of speech that any person wishes to—but cannot—hear. And that aspect of these allegations takes them far afield from the relevant caselaw. The general desire to interact more online is quite different than the desire to "hear, speak, and debate with" a particular noncitizen who, despite wishing to speak in a specific instance, has been prevented from doing so. *See, e.g., Mandel*, 408 U.S. at 762. In the end, Plaintiffs cite no case in which any court has recognized such a nebulous First Amendment theory. Thus, it does not support a First Amendment claim.

That leaves Plaintiffs' second and third burden theories. Unlike their first, these theories rely on the First Amendment rights of *noncitizens* interested in applying for a relevant visa. So a quick detour is necessary to determine the extent to which any such rights exist in the first place. Plaintiffs argue that noncitizens "enjoy full First Amendment protection" if they have "substantial connections to the United States." ECF No. 32 at 22, 46. The caselaw, however, does not see it that way.

The "substantial connections" language comes from *United States v. Verdugo-Urquidez*, 494 U.S. 259, 271 (1990). There, the Court used that phrase to reject a criminal defendant's argument that the Fourth Amendment protected him against the search of his two homes in Mexico. *Id.* at 262, 270–71. The defendant was present in the United States when his homes were searched, but he was brought here by law-enforcement officers and held against his will. *Id.* at 271. The Court rejected the view that his physical presence here was enough to confer constitutional rights, requiring instead that an alien both "come within the territory of the United States *and* develop[ ]

substantial connections with this country." *Id.* (emphasis added).

The Supreme Court recently reaffirmed that both conditions are necessary. In rejecting the view that "the First Amendment could extend to foreign organizations operating abroad," the Court described as "long settled" the principle that "foreign citizens outside U.S. territory do not possess rights under the U.S. Constitution." *Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 140 S. Ct. 2082, 2086 (2020) (citing, among other cases, *Verdugo-Urquidez*, 494 U.S. at 265–75). The Court acknowledged that "foreign citizens *in the United States* may enjoy certain constitutional rights," but it emphasized the territorial limitations of that rule. *See id.*

Plaintiffs' position about First Amendment protections, then, mistakes a necessary condition for a sufficient one. A foreign citizen who both is present in and has "substantial connections" to the United States has First Amendment rights. *Nat'l Council of Resistance*, 251 F.3d at 203. But once she leaves the country or areas under its territorial control, those personal constitutional rights vanish. *See Agency for Int'l Dev.*, 140 S. Ct. at 2086.[9]

Plaintiffs have alleged that many noncitizens affected by the disclosure requirement have "substantial connections to the United States." Compl. ¶ 43. The facts supporting that conclusion include the existence of noncitizens who live here, have family here, and work and attend school

[9] Of course, that is not to say that a foreign citizen abroad lacks rights relating to property that remains in the United States. A foreigner who "acquires or holds property in this country may invoke the protections of the Constitution when that property is placed in jeopardy by government intervention." *Nat'l Council of Resistance*, 251 F.3d at 204. The D.C. Circuit has long recognized that "a foreign national residing outside the United States" may retain a "substantial connection" to the country and so retain constitutional protection vis-à-vis her property holdings. *Rahimov v. Gacki*, No. 19-2554 (JEB), 2020 WL 1911561, at *4–5 (D.D.C. Apr. 20, 2020) (collecting cases).

Nor does the Court here express any view about the constitutional rights of noncitizens in United States custody, a question the Circuit recently declined to decide categorically. *See Al-Hela v. Biden*, 66 F.4th 217, 226–28 (D.C. Cir. 2023) (en banc); *id.* at 249–60 (Rao, J., concurring in the judgment in part and dissenting in part) (arguing that "constitutional rights do not extend to aliens without property or presence in the sovereign territory of the United States").

here. *Id.* Accepting those allegations as true, the disclosure requirement ultimately will affect U.S. residents who have "accepted some societal obligations" here and thus have a substantial connection to the country. *See Verdugo-Urquidez*, 494 U.S. at 273.

Still, the requirement applies only to visa applications "from abroad." Compl. ¶ 23. Even if it is "common," as Plaintiffs allege, for U.S. residents to leave the country and so submit visa applications "from abroad," *id.*, the requirement definitionally applies only to "foreign citizens outside of U.S. territory," *Agency for Int'l Dev.*, 140 S. Ct. at 2086. No applicant, then, has First Amendment rights when she submits the application.

Returning to Plaintiffs' theories, their second theory of constitutional burden is that the government may not require "individuals to register their speech or associations with the government as a condition of" their admissibility to the country. ECF No. 32 at 50. It relies on cases such as *Shelton v. Tucker*, where a state had required every public schoolteacher or professor "to file annually an affidavit listing without limitation every organization to which he has belonged or regularly contributed within the preceding five years." 364 U.S. 479, 480 (1960). That requirement, the Supreme Court held, was an unconstitutional "interference with personal freedom" in part because the teachers served "at the absolute will of those to whom the disclosure must be made." *Id.* at 486. But even assuming consular officers exercise comparable authority over visa applications, those cases are inapposite because, as explained above, the applicants have no constitutional "right of free association" to protect. *Id.* For this reason, Plaintiffs' second theory does not support a claim under the First Amendment either.

That leaves Plaintiffs' third theory. That theory—the idea that the disclosure requirement erases *future* visa applicants' online anonymity and thereby discourages their speech and associations, ECF No. 32 at 48–49—is much broader in scope than the second. Plaintiffs allege that these

noncitizens forgo speech and associations *before* they need to apply for a visa. *See* Compl. ¶ 55. In other words, those who know they will someday need a visa renewed—including those who now live in the United States and have substantial connections here—"have deleted past posts, altered or limited their speech, or entirely dropped out of certain groups on social media." *Id.* Because the accompanying harms occur while the noncitizens are still in the United States, this aspect of the disclosure requirement *does* bear on their First Amendment rights.

The rights to speak and associate of these noncitizens include, typically, the rights to do so anonymously, even where a person has already revealed aspects of his identity. *Buckley v. Am. Const. L. Found., Inc.*, 525 U.S. 182, 198–200 (1999). For that reason, "compelled disclosure, in itself, can seriously infringe on privacy of association and belief." *Buckley v. Valeo*, 424 U.S. 1, 64 (1976). The Supreme Court has thus held unconstitutional, for example, a requirement that petition circulators wear name badges, *Am. Const. L. Found.*, 525 U.S. at 197–200, a requirement that literature related to political campaigning contains the name and address of the author, *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 348–53 (1995), a requirement that door-to-door canvassers get municipal permits, *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 536 U.S. 150, 165–69 (2002), and a requirement that all handbills contain the name of the writer and the name and address of the sponsor, *Talley v. California*, 362 U.S. 60, 64–65 (1960). Plaintiffs compare the noncitizens affected by the disclosure requirement to the plaintiffs in these cases. *See* ECF No. 32 at 48–49.

But these cases are all distinguishable for the same reason: they all involved direct restrictions on speech, not abstract disincentives to speech. That is, the disclosure requirement in those cases was a precondition of speech, not a consequence of a later decision to apply for a benefit. *See Am. Const. L. Found.*, 525 U.S. at 188–89; *McIntyre*, 514 U.S. at 338 & n.3;

Watchtower Bible, 536 U.S. at 154–57; *Talley*, 362 U.S. at 60–61. Plaintiffs have not alleged that they must divulge their social-media identifiers before they can speak or associate on those platforms. And the Supreme Court has explained that a disclosure requirement's timing is significant and that a speaker's "interest in anonymity is greatest" when she speaks. *Am. Const. L. Found.*, 525 U.S. at 199. Thus, the Court noted that "*McIntyre* left room" for some requirements that take effect after speech occurs. *Id.* at 200.

Still, that room is limited. Even a subsequent disclosure requirement may trigger heightened scrutiny, *Doe v. Reed*, 561 U.S. 186, 195–96 (2010), particularly where challengers show "a reasonable probability that the compelled disclosure of personal information will subject them to threats, harassment, or reprisals from either Government officials or private parties," *id.* at 200 (quoting *Buckley*, 424 U.S. at 74). Although such a requirement is a "more subtle [form of] governmental interference" with speech, the fact that disclosure may risk harm to speakers means that the "rights of free speech and free association . . . need breathing space to survive." *Gibson v. Fla. Legis. Investigation Comm.*, 372 U.S. 539, 544 (1963) (quotations omitted).

The most prominent case in which the Supreme Court applied those principles is *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958). There, Alabama sought to enforce against the NAACP a requirement "to qualify before doing business" in the state. *Id.* at 451. During the enforcement proceeding, Alabama demanded the "names and addresses" of all NAACP "'members' and 'agents'" in the state, which plaintiffs argued burdened their associational rights after the fact. *Id.* at 453. The Court held that compelled disclosure of the membership lists would "abridge the rights of its rank-and-file members to engage in lawful association." *Id.* at 460. It recognized "that compelled disclosure of affiliation with groups engaged in advocacy" could be "as effective a restraint on freedom of association" as "direct action to restrict the right." *Id.* at 461–62 (citations

omitted). Because of the members' justified fears that disclosure would lead to reprisals, the Court found the disclosure "likely to affect adversely" their associational rights. *Id.* at 462–63.

More recently, the Supreme Court reaffirmed that a subsequent disclosure requirement "burden[s] . . . associational rights" if it creates a "risk of a chilling effect on association." *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2389 (2021). The risk itself, or the "'*possible* deterrent effect' of disclosure" is enough. *Id.* at 2388 (quoting *NAACP*, 357 U.S. at 461). That is true even where the disclosed information is not publicly available, where the government assures those affected that the data will be treated as confidential, and where not all associates share the desire for anonymity. *Id.*

Plaintiffs' complaint satisfies the standard reflected in these cases for a First Amendment claim. They allege more than a mere risk that the disclosure requirement will chill online speech and association—they say it is already happening. Compl. ¶ 55. They plausibly attribute that phenomenon to the same concerns accepted by the Court in *NAACP* and *Americans for Prosperity*—fears that they will suffer reprisals because of their speech or associations, whether from the United States or from foreign governments. Compl. ¶¶ 57–61. And that chilling effect materializes, in some cases, long before a noncitizen must apply for a visa, including while he lives in the United States and remains protected by the Constitution. *See* Compl. ¶ 55.

Thus, "the protections of the First Amendment are triggered" by Plaintiffs' allegations. *Ams. for Prosperity*, 141 S. Ct. at 2389. So the Court proceeds to determine the level of scrutiny it must apply to evaluate whether they state a valid First Amendment claim.

2. The Degree of Judicial Scrutiny

Ordinarily, the Court's conclusion that the disclosure requirement burdens First Amendment rights would compel "exacting scrutiny" of the rule. *See Ams. for Prosperity*, 141 S. Ct. at

2382–83 (plurality opinion) (rejecting an argument that strict scrutiny should apply instead).[10] Under exacting scrutiny, the government has the onus to show the burden's lawfulness. *Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984). So if exacting scrutiny applied, the Court would likely deny Defendants' motion to dismiss because it challenges only the legal sufficiency of Plaintiffs' complaint. *See, e.g.*, *Brown*, 390 F. Supp. 3d at 126–27.

But Defendants point to a countervailing principle: This case, they say, concerns "a condition of entry into the United States by a foreign national." ECF No. 31-1 at 50. For that reason, they advocate a much more deferential standard of review. *Id.* at 50–53. Plaintiffs reply that the rule "imposes [only] a procedural requirement" and so does not implicate the rationale for courts' deferring to the other branches of government. ECF No. 32 at 45–47.

The Court agrees with Defendants. Two cases are especially relevant to this question: *Mandel* and *Trump v. Hawaii*.

In *Mandel*, the Supreme Court observed that "ancient principles of the international law of nation-states," reflected in a long line of its cases, establish that "the political branches of government" have exclusive control over the admission and exclusion of aliens. 408 U.S. at 765–66 (quotation omitted). So where Congress has given the executive branch discretion to make immigration decisions, and the executive has provided "a facially legitimate and bona fide" explanation, "courts will neither look behind the exercise of that discretion, nor test it by balancing its justification against the First Amendment interests of those who" challenge that decision. *Id.* at 770. Later, the Court explained that *Mandel*'s rationale does not depend on "the nature of the policy

[10] *See also Republican Nat'l Comm. v. Pelosi*, 602 F. Supp. 3d 1, 34–35 (D.D.C. 2022) (explaining that surviving exacting scrutiny requires the strength of the government's interest to reflect the seriousness of the burden the action imposes and that the action is narrowly tailored to further the government's interest without substantial overbreadth), *vacated as moot*, 2022 WL 4349778 (D.C. Cir. Sept. 16, 2022).

choice at issue," such as national security. *Fiallo*, 430 U.S. at 795–96. Instead, it applies to all cases "in the area of immigration and naturalization" because "[t]he conditions of entry for every alien, the particular classes of aliens that shall be denied entry altogether, the basis for determining such classification, the right to terminate hospitality to aliens, [and] the grounds on which such determination shall be based" are outside courts' "power . . . to control." *Id.* (quotations omitted). Judicial inquiry under that standard, limited though it is, is often called "*Mandel* review." *See, e.g.*, *Udugampola v. Jacobs*, 70 F. Supp. 3d 33, 42–45 (D.D.C. 2014).

The Supreme Court most recently discussed *Mandel* review in *Trump v. Hawaii*. There, it appeared to affirm that the standard applies when courts are asked to "'probe and test the justifications' of immigration policies." 138 S. Ct. at 2419 (quoting *Fiallo*, 430 U.S. at 799). It even offered an expansive "upshot" of the *Mandel* line of cases: that judicial "inquiry into matters of entry and national security is highly constrained." *Id.* at 2419–20. But it did not actually *apply* *Mandel* review. *See id.* at 2420. Instead, the Court "assume[d]" that rational-basis review applied and—because the contested policy satisfied that higher tier of scrutiny—did not settle the issue of which methodology to use. *See id.* at 2420–23. That resolution did not "purport to alter *Mandel*." *Yafai v. Pompeo*, 924 F.3d 969, 973–74 (7th Cir. 2019) (opinion of Barrett, J.). The Court simply assumed that rational-basis review applied "at the request of the government." *Id.* at 973; *see also* *Trump v. Hawaii*, 138 S. Ct. at 2420.

Defendants here request a similar assumption. Although they mainly argue that the Court should apply *Mandel* review, ECF No. 31-1 at 51–52, they rely on *Trump v. Hawaii* to suggest that the Court might also assume that rational-basis review applies, *id.* at 52.

Plaintiffs try to distinguish those cases on two grounds. First, they point out that *Mandel* and *Trump v. Hawaii* "focused principally on foreigners outside the United States who . . . lacked

their own First Amendment rights." ECF No. 32 at 46. This case is different, they explain, because it concerns "the First Amendment rights of [organizations and people] who currently reside in the United States." *Id.* Second, they observe that those cases concerned what they call "substantive admissibility decisions"—that is, decisions about whether aliens may enter the United States. *Id.* at 46–47 (emphasis omitted). The disclosure requirement, they claim, is "a procedural requirement on all visa applicants[that] makes no substantive [admissibility] determination." *Id.* at 47.

Plaintiffs' first argument misconstrues the Supreme Court's decisions. The premise of judicial review in *Mandel* and *Trump v. Hawaii* was that the challenged actions burdened the constitutional rights of U.S. citizens. *See Mandel*, 408 U.S. at 762–65; *Trump v. Hawaii*, 138 S. Ct. at 2419. The same was true in other cases in which the Court applied *Mandel* review.[11] If Plaintiffs mean to assert that a special situation is present where the rightsholder is the same person whose entry into the United States may be affected, they cite no case for that novel proposition. And the Court sees no reason to treat some First Amendment rightsholders as more equal than others. Besides, the rationale for applying *Mandel* review is categorical; it depends on the type of "decision[ ] made by the Congress or the President," not the identity of the person asserting the right or the severity of the asserted burden. *See Fiallo*, 430 U.S. at 796 (quotation omitted).

Plaintiffs' second argument is also unpersuasive. For starters, even if the Court were to accept Plaintiffs' substance-procedure distinction, it is not clear that the disclosure requirement "makes no substantive determination as to the admissibility of any applicant," as they say. ECF

[11] *See, e.g.*, *Fiallo*, 430 U.S. at 794–95 (rejecting the argument that the Court should apply greater scrutiny because the challenged action "infringed upon the due process rights of citizens and legal permanent residents"); *Din*, 576 U.S. at 101–06 (Kennedy, J., concurring in the judgment) (applying *Mandel* review to conclude that any right to due process held by a U.S. citizen was satisfied); *Cardenas v. United States*, 826 F.3d 1164, 1167 (9th Cir. 2016) (holding that Justice Kennedy's opinion in *Din* is "controlling").

No. 32 at 47. Plaintiffs took great pains to explain that a visa applicant must divulge the requested information to complete her application. *See* Compl. ¶¶ 28–33 (explaining that the requirement applies to "nearly all applicants," that it is "mandatory and makes no exception," and that it "applies nearly universally"). Violating the rule thus makes an applicant inadmissible. *See* 8 U.S.C. § 1201(a)(1) (conditioning both types of visas on a "proper application"). In other words, the rule states a "condition[ ] of entry," which the Supreme Court has explicitly recognized as a type of action subject to *Mandel* review. *Fiallo*, 430 U.S. at 796 (quotation omitted).[12]

That said, there is no reason to think Plaintiffs' substance-procedure distinction matters. As Defendants point out, ECF No. 44 at 32, the Supreme Court has justified *Mandel* review on the grounds that "[*a*]*ny policy* toward aliens is vitally and intricately interwoven with

[12] Reference to the substance-procedure distinction in choice-of-law analysis crystalizes the conclusion that the disclosure requirement is more accurately characterized as substantive. Although the Supreme Court long ago tried neatly to divide truly substantive rules from truly procedural ones, *see Guaranty Tr. Co. v. York*, 326 U.S. 99, 109 (1945), it has since explained that "every procedural variation" can, under the right circumstances, control the outcome of a process, *see Hanna v. Plumer*, 380 U.S. 460, 468–69 (1965). So courts must consider whether the rule at issue is so significantly related to the resolution of the dispute that its application is likely to influence a party's *ex ante* choice of forum. *See Hanna*, 380 U.S. at 469; *Burke v. Air Serv. Int'l, Inc.*, 685 F.3d 1102, 1109 (D.C. Cir. 2012). Put another way, a rule is substantive if it is "bound up with the definition of the rights and obligations of the parties," not "merely a form and mode of enforcing" existing rights and obligations. *See Byrd v. Blue Ridge Rural Elec. Co-op, Inc.*, 356 U.S. 525, 536 (1958).

Applied here, the question is whether the information provided in the disclosure section of the application is likely to make a "material difference" in a consular officer's eventual admission decision. *Cf. Kohlrautz v. Oilmen Participation Corp.*, 441 F.3d 827, 831 (9th Cir. 2006). And framed that way, even Plaintiffs must concede that the disclosure requirement is a substantive part of the visa-application process. Their interest in challenging the requirement stems, after all, from their fears, and those of their members and partners, that the information collected under the requirement will be used by consular officers to delay, deny, or revoke visas. *See* Compl. ¶¶ 57–59. Indeed, they have alleged that the disclosure requirement now forms such an important part of the visa-application process that some of their "members and partners are no longer applying for U.S. visas—and are foregoing personal, educational, and professional opportunities" to avoid it. Compl. ¶ 56. Their selective attempts to diminish the disclosure requirement as mere procedural red tape cannot withstand scrutiny.

contemporaneous policies in regard to the conduct of foreign relations and the war power." *Trump v. Hawaii*, 138 S. Ct. at 2418 (quotation omitted and alteration adopted). And Justice Kennedy's controlling concurrence in *Din* applied *Mandel* review to the question of "how much information the Government is obliged to disclose about a . . . denial of a visa." *See* 576 U.S. at 106. The amount and type of information an applicant receives after a denial cannot possibly be more substantive than the amount and type of information an applicant must provide to be considered for admission.

So although there is no reason to think that *Mandel* review has been displaced, this Court will follow the Supreme Court's lead in *Trump v. Hawaii* and assume that rational-basis review applies. That is for two reasons. First, like in *Trump v. Hawaii*, the government has invited the Court to do so. *See* 138 S. Ct. at 2420; ECF No. 31-1 at 52; ECF No. 44 at 32–33. Second, that assumption does not affect the outcome. A policy that survives rational-basis review will of course survive *Mandel* review and, as the Court will explain, the disclosure requirement breezes through rational-basis review.

3. Rational-Basis Review

Rational-basis review begins with "a strong presumption" that the challenged action is valid. *FCC v. Beach Commc'ns, Inc.*, 508 U.S. 307, 314 (1993). Plaintiffs have the burden to negate "every conceivable basis" that might support the requirement. *Id.* at 315 (quotation omitted). Under that standard, courts "hardly ever" hold a policy unconstitutional. *Trump v. Hawaii*, 138 S. Ct. at 2420. The Court would need to conclude that the law's only purpose is the "bare desire to harm a politically unpopular group," *id.* (quoting *Dep't of Agric. v. Moreno*, 413 U.S. 528, 534 (1973)), or that it is "inexplicable by anything but animus," *id.* (quoting *Romer v. Evans*, 517 U.S. 620, 632 (1996)).

At the pleading stage, the Plaintiff "must plausibly allege facts showing that no reasonably conceivable state of facts could provide a rational basis for the challenged policy." *Sanchez.*, 45 F.4th at 396. Even the possibility that the government relied on "rational speculation unsupported by evidence or empirical data" is enough to defeat a complaint. *Id.* at 398 (quoting *Beach*, 508 U.S. at 315). If a "conceivably rational justification" for the policy is "readily apparent," the Court must dismiss the claim. *Id.*

The disclosure requirement is far from inexplicable. Plaintiffs do not contest that the proffered interests of "confirming visa applicants' identities [and] determining their visa eligibility" are "important government interests." ECF No. 32 at 53. Instead, they claim the government "cited no evidence" that the disclosure requirement will advance those interests. *Id.* (quotation omitted). But as the Court has just explained, the government does not have to do so. *See Sanchez*, 45 F.4th at 396. And given the amount of personal information that can be gleaned from many social-media users' accounts, the disclosure requirement is "is self-evidently (and rationally) connected" to those ends. *Id.* at 398.

Plaintiffs also find fault with the requirement's breadth, noting that it applies to all applicants absent "individualized suspicion." ECF No. 32 at 54. Defendants think that argument "puts the cart before the horse" because, in many cases, the government does not know which applicants may warrant further scrutiny until it reviews their social-media activity. ECF No. 31-1 at 56. The Court agrees with Defendants. It is at least conceivable that some visa applicants' claims appear true until they are compared with a more objective record of their biographical details and associations. And in one way, the requirement's universality counts in its *favor* under rational-basis review. If the requirement applies to nearly all applicants, it would be hard to conclude that the motivation behind it was an "irrational prejudice" against applicants from any particular subgroup.

Cf. Trump v. Hawaii, 138 S. Ct. at 2420 (quotation omitted).

Nor is it irrational to retain the information past the disposition of an application, as Plaintiffs suggest. ECF No. 32 at 55. The government explains that it retains the information to help enforce immigration and national-security laws prospectively, such as by monitoring visa holders for "grounds for deportability" or the denial of future benefits. ECF No. 31-1 at 54–55. Again, that rationale is self-evidently connected to inarguably legitimate government interests. *Cf. Pinho v. INS*, 249 F.3d 183, 190 (3d Cir. 2001) (describing "foreign relations, national security policy, and compliance with on-going government programs" as "legitimate government interests").

At bottom, Plaintiffs do not seriously engage with the rational-basis standard. Their argument rests mainly on their contention the Court has rejected—that heightened scrutiny applies, shifting the burden to the government. *See* ECF No. 32 at 52–56 (contending that Defendants cannot carry their burden "even under intermediate scrutiny"). Under rational-basis review, their position amounts to a challenge based on the "effectiveness and wisdom" of the disclosure requirement. *See Trump v. Hawaii*, 138 S. Ct. at 2421. Even if they are right when they call the requirement unwise and ineffective, that is no basis for the Court to "substitute [its] assessment" for that of the executive branch. *Id.* The disclosure requirement is rationally connected to legitimate government interests. Thus, Plaintiffs have not stated a First Amendment claim.

* * *

Finally, Plaintiffs ask for leave to amend their complaint given the Court's conclusion that they have not stated a claim. *See* ECF No. 32 at 57. Yet ultimately, the main deficiency in their complaint stems not from inadequate detail or correctable mistakes, but from the nature of the

government action they challenge.[13] For that reason, the Court finds that further allegations consistent with those already pled could not cure the deficiency and so will dismiss the complaint with prejudice. *See Firestone v. Firestone*, 76 F.3d 1205, 1209 (D.C. Cir. 1996) (per curiam).

IV. Conclusion

For all the above reasons, the Court will grant Defendants' motion to dismiss insofar as it seeks dismissal for failure to state a claim. A separate order will issue.

/s/ Timothy J. Kelly
TIMOTHY J. KELLY
United States District Judge

Date: August 11, 2023

[13] As explained above, the sole area in which the Court found Plaintiff's complaint lacking in specificity was in its failure to allege any particular U.S. citizen who wanted to hear the particular speech of any particular noncitizen whom the disclosure requirement dissuaded from speaking. But the Court cannot fathom—and Plaintiffs have not proposed—how under these circumstances the complaint could be amended to address these deficiencies in a way that would make a difference under rational-basis review.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

DOC SOCIETY and INTERNATIONAL DOCUMENTARY ASSOCIATION

Plaintiffs,

v.

ANTONY J. BLINKEN, in his official capacity as Secretary of State, and ALEJANDRO N. MAYORKAS, in his official capacity as Secretary of Homeland Security,

Defendants.

Civil Action No. 19-cv-3632 (TJK)

NOTICE OF APPEAL

Notice is hereby given this 10th day of October, 2023, that Plaintiffs Doc Society and International Documentary Association hereby appeal to the United States Court of Appeals for the District of Columbia Circuit from the Memorandum Opinion and Order of this Court entered on August 11, 2023 (ECF Nos. 66, 67), dismissing Plaintiffs' Complaint (ECF No. 1) with prejudice and granting in part and denying in part Defendants' Motion to Dismiss (ECF No. 31).

October 10, 2023

Respectfully submitted,

/s/ *Faiza Patel*
Faiza Patel*
Emile Ayoub*
Brennan Center for Justice
at NYU School of Law
120 Broadway, Suite 1750
New York, NY 10271
patelf@brennan.law.nyu.edu
(646) 292-8310

/s/ *Carrie DeCell*
Carrie DeCell (D.C. Bar No. 1015491)
Jameel Jaffer (D.C. Bar No. MI0067)
Katie Fallow*
Anna Diakun*
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302–304
New York, NY 10115
carrie.decell@knightcolumbia.org
(646) 745-8500

/s/ *Rachel Levinson-Waldman*
Rachel Levinson-Waldman*
Brennan Center for Justice
at NYU School of Law
1140 Connecticut Avenue, NW
11th Floor, Suite 1150
Washington, D.C. 20036
levinsonr@brennan.law.nyu.edu
(202) 249-7190

/s/ *Joshua Polster*
Joshua Polster*
Evan Gilbert*
Simpson Thacher & Bartlett LLP
425 Lexington Avenue
New York, NY 10017
joshua.polster@stblaw.com
(212) 455-2000

*admitted *pro hac vice*

Counsel for Plaintiffs