PAGE WITHHELD PURSUANT TO

(b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO

(b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO

(b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO

(b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

PAGE WITHHELD PURSUANT TO

(b)(5)

PAGE WITHHELD PURSUANT TO

(b)(5)

PAGE WITHHELD PURSUANT TO (b)(5)

Horn, Dawn D

From: Neufeld, Donald W
Sent: Wednesday, May 24, 2017 7:31 AM
To: Thomas, Ronnie D; Padilla, April Y; Hutchings, Pamela G
Cc: Thompson, Kirt
Subject: FW: Urgent Request RE: JANUS Cases

Sharing just for visibility. This initial work is all done by FOD, but of course the results may end up on our plate if we have to review any already adjudicated SCOPS cases for rescission/revocation.

From: Farnam, Julie E
Sent: Wednesday, May 24, 2017 8:12 AM
To: Valverde, Michael; McCament, James W; Renaud, Daniel M; Neufeld, Donald W; Symons, Craig M; Miles, John D
Cc: Renaud, Tracy L; Emrich, Matthew D; Davidson, Andrew J
Subject: RE: Urgent Request RE: JANUS Cases

According to Al Davis, as of 5/16, 607,398 historical fingerprint records have been uploaded into IDENT. This includes the HFE I, II, and III (HFE III also known as "Waldo") records. These records yielded 22,295 SGNS—about a 3.7% hit rate. There are about 2.5M total records that need to be ingested, so only about a quarter have been ingested so far.

I don't have the breakdown of how many of those cases are post-adjudication, but am working with Al to get this number. The SGNs that fire on pending cases can be addressed during the adjudication process. The SGNs that fire on adjudicated cases are the ones that will need the review to potentially revoke/rescind the benefit. But if we just take the raw numbers of 22,295 cases right now—and this would be an overestimate of resources needed because not all are post-adjudication and I would think that naturalization cases take longer to review than other cases—and using the number of people who reviewed the Janus cases for the OIG report (15 people) and the length of time it took to review the OIG's cases (approximately 2,000 cases over about 3 ½ months), you could either have 165 people review all those cases and be done with them in about 3-4 months or reduce the number of people reviewing and increase the amount of time it will take to review proportionally.

One other point—the number of people to review the cases noted above does not include OCC resources.

Julie Farnam
Senior Advisor
Field Operations Directorate
U.S. Citizenship and Immigration Services

[redacted] (b)(6)

From: Valverde, Michael
Sent: Tuesday, May 23, 2017 8:35 PM
To: McCament, James W; Renaud, Daniel M; Neufeld, Donald W; Symons, Craig M; Miles, John D; Farnam, Julie E
Cc: Renaud, Tracy L
Subject: RE: Urgent Request RE: JANUS Cases

Adding Julie F for this background and fuller ask. Thanks.

Michael Valverde
DHS USCIS
Field Operations Directorate, Deputy Associate Director

[redacted]

(b)(6)

From: McCament, James W
Sent: Tuesday, May 23, 2017 8:25:41 PM
To: Renaud, Daniel M; Neufeld, Donald W; Valverde, Michael; Symons, Craig M; Miles, John D
Cc: Renaud, Tracy L
Subject: RE: Urgent Request RE: JANUS Cases

Adding John Miles as well.

James W. McCament
Director (Acting) | Deputy Director
U.S. Citizenship and Immigration Services
Department of Homeland Security

[redacted]

(b)(6)

From: McCament, James W
Sent: Tuesday, May 23, 2017 8:25:13 PM
To: Renaud, Daniel M; Neufeld, Donald W; Valverde, Michael; Symons, Craig M
Cc: Renaud, Tracy L
Subject: RE: Urgent Request RE: JANUS Cases

Thanks Dan for that good point and caution. I shared that I would get back to them tomorrow afternoon with what preliminary estates we might be able to calculate. For further back ground, we've been asked for an estimate of how long it would take to clear the backlog at current funding levels, and how quickly it could be cleared if funding were significantly increased, as well as how much it would cost to do so.

Thanks again all,

James

James W. McCament
Director (Acting) | Deputy Director

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

(b)(6)

[redacted]

This email (including any attachments) is intended solely for the use of the addressee(s) and may contain information that is sensitive or otherwise protected by applicable law. If you are not the intended recipient, please notify USCIS immediately by replying to this message and destroy all copies of this message and any attachments. Thank you.

From: Renaud, Daniel M
Sent: Tuesday, May 23, 2017 5:50:48 PM
To: McCament, James W; Neufeld, Donald W; Valverde, Michael; Symons, Craig M
Cc: Renaud, Tracy L
Subject: RE: Urgent Request RE: JANUS Cases

A deadline tomorrow would be better, but we need to keep in mind that the HFE work being done by the ICE contractor at the NRC will not be complete for at least another month or so. As a result, hard estimates will be difficult. Then we have HFE 3...4...5. Nonetheless, we should be able to provide an estimate tomorrow based on what we know from the HFE 1 workload.

Daniel M. Renaud
Associate Director, Field Operations
U.S. Citizenship and Immigration Services

From: McCament, James W
Sent: Tuesday, May 23, 2017 5:43:19 PM
To: Neufeld, Donald W; Renaud, Daniel M; Valverde, Michael; Symons, Craig M
Cc: Renaud, Tracy L
Subject: RE: Urgent Request RE: JANUS Cases

Right, Ill let them know we need a bit of time to pull more information.

James W. McCament
Acting Director
Deputy Director
U.S. Citizenship and Immigration Services
Department of Homeland Security
Washington, DC 20529-2150

(b)(6)

[redacted]

This email (including any attachments) is intended solely for the use of the addressee(s) and may contain information that is sensitive or otherwise protected by applicable law. If you are not the intended recipient, your disclosure, copying, distribution or other use of (or reliance upon) the information contained in this email is strictly prohibited. If you are not the intended recipient, please notify the sender immediately and delete or destroy all copies. Thank You.

From: Neufeld, Donald W
Sent: Tuesday, May 23, 2017 5:40:46 PM
To: McCament, James W; Renaud, Daniel M; Valverde, Michael; Symons, Craig M
Cc: Renaud, Tracy L
Subject: RE: Urgent Request RE: JANUS Cases

We will need to coordinate on this tomorrow.

From: McCament, James W
Sent: Tuesday, May 23, 2017 5:36:30 PM
To: Renaud, Daniel M; Valverde, Michael; Neufeld, Donald W; Symons, Craig M
Cc: Renaud, Tracy L
Subject: Urgent Request RE: JANUS Cases

Guys, please see the below request from WH DPC. Did you arrive at any firm statistics on the total number of JANUS cases as well as the resource estimates for resolution? Im including Don for SCOPS and Craig for OCC regarding resources.

Id like to provide a getback timeline soonest to DPC but would like your best estimates before doing so.

Thanks!

James

James W. McCament
Acting Director
Deputy Director
U.S. Citizenship and Immigration Services
Department of Homeland Security
Washington, DC 20529-2150
(b)(6)
[redacted]

From: Wetmore, David H. EOP/WHO
Sent: Tuesday, May 23, 2017 5:23:54 PM
To: McCament, James W
Cc: Dougherty, Michael
Subject: RE: James, connecting you...

Thanks, Mike.

James: DPC is looking for an estimate from USCIS on the amount of time and resources required to review the backlog of potential Janus cases in the shortest amount of time. Do you know who can provide that information

to DPC. Once we have that information, we can explore funding possibilities and begin working with USAOs and DOJ OIL on a process to handle the expected influx of denaturalization criminal and civil denaturalization cases. We are already starting to plan for the 2019 budget, so time is of the essence.

Dave

DAVID H. WETMORE
Immigration Advisor
Domestic Policy Council
Executive Office of the President

[redacted] (b)(6)

From: Dougherty, Michael [mailto:michael.dougherty@hq.dhs.gov]
Sent: Tuesday, May 23, 2017 5:18 PM
To: McCament, James W <James.W.McCament@uscis.dhs.gov>; Wetmore, David H. EOP/WHO <David.H.Wetmore@who.eop.gov>
Subject: James, connecting you...

And Dave Wetmore. We're working Operation Janus and Dave wants to ensure from DPC that we have correct USCIS folks involved.

Everything You Ever Wanted to Know About Denaturalization but Were Afraid to Ask

An Interactive Discussion with
Tom Baxley, Janette Martinez, and Mark Martinez

U.S. Citizenship and Immigration Services

Revocation of Naturalization

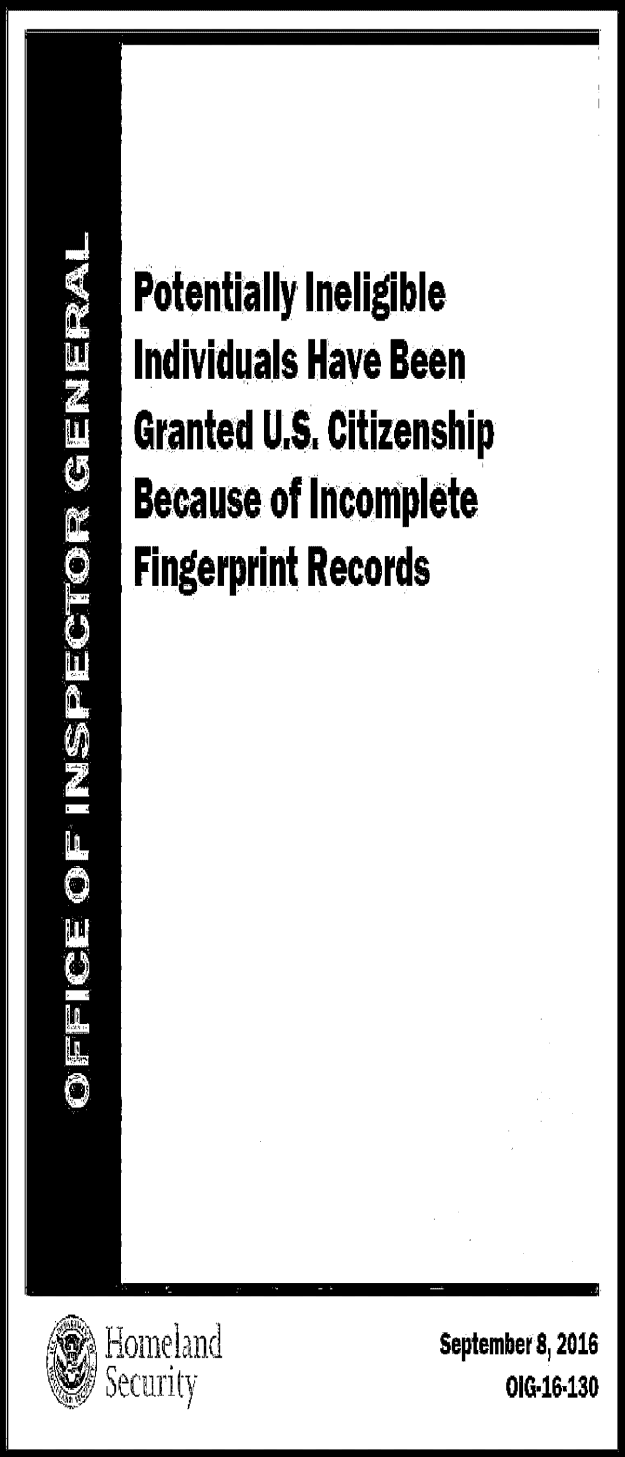
(b)(5)

U.S. Citizenship and Immigration Services

(b)(5)

PAGE WITHHELD PURSUANT TO

"The Report"



U.S. Citizenship and Immigration Services

(b)(5)

U.S. Citizenship and Immigration Services

(b)(5)

U.S. Citizenship and Immigration Services

(b)(5)

U.S. Citizenship and Immigration Services

(b)(5)

U.S. Citizenship and Immigration Services

(b)(5)

U.S. Citizenship and Immigration Services

(b)(5)

U.S. Citizenship and Immigration Services

10

(b)(5)

U.S. Citizenship and Immigration Services

(b)(5)

U.S. Citizenship and Immigration Services

INTERMISSION

U.S. Citizenship and Immigration Services

PRACTICUM

(b)(5)

U.S. Citizenship and Immigration Services

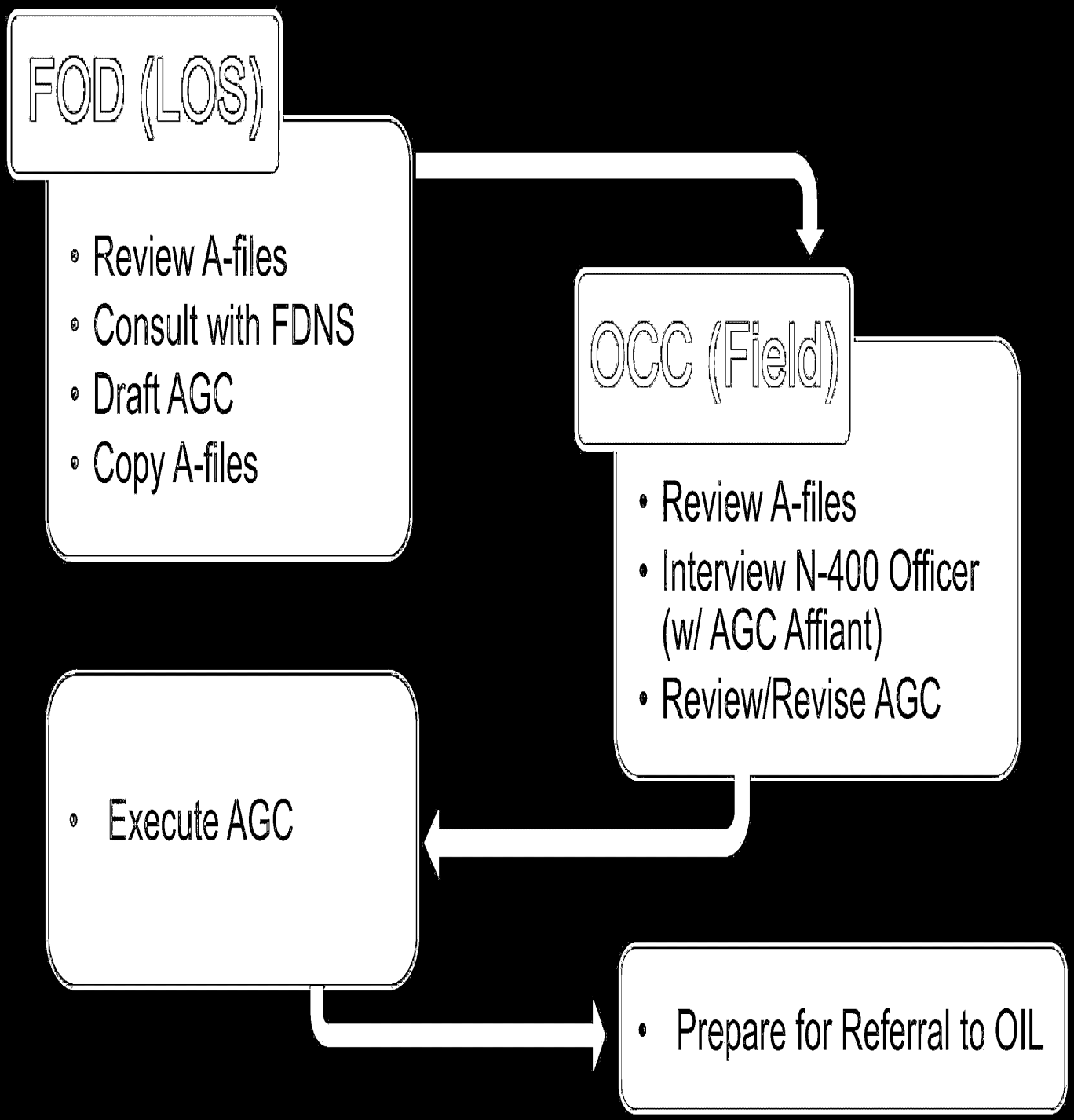
(b)(5)

U.S. Citizenship and Immigration Services

16

(b)(5)

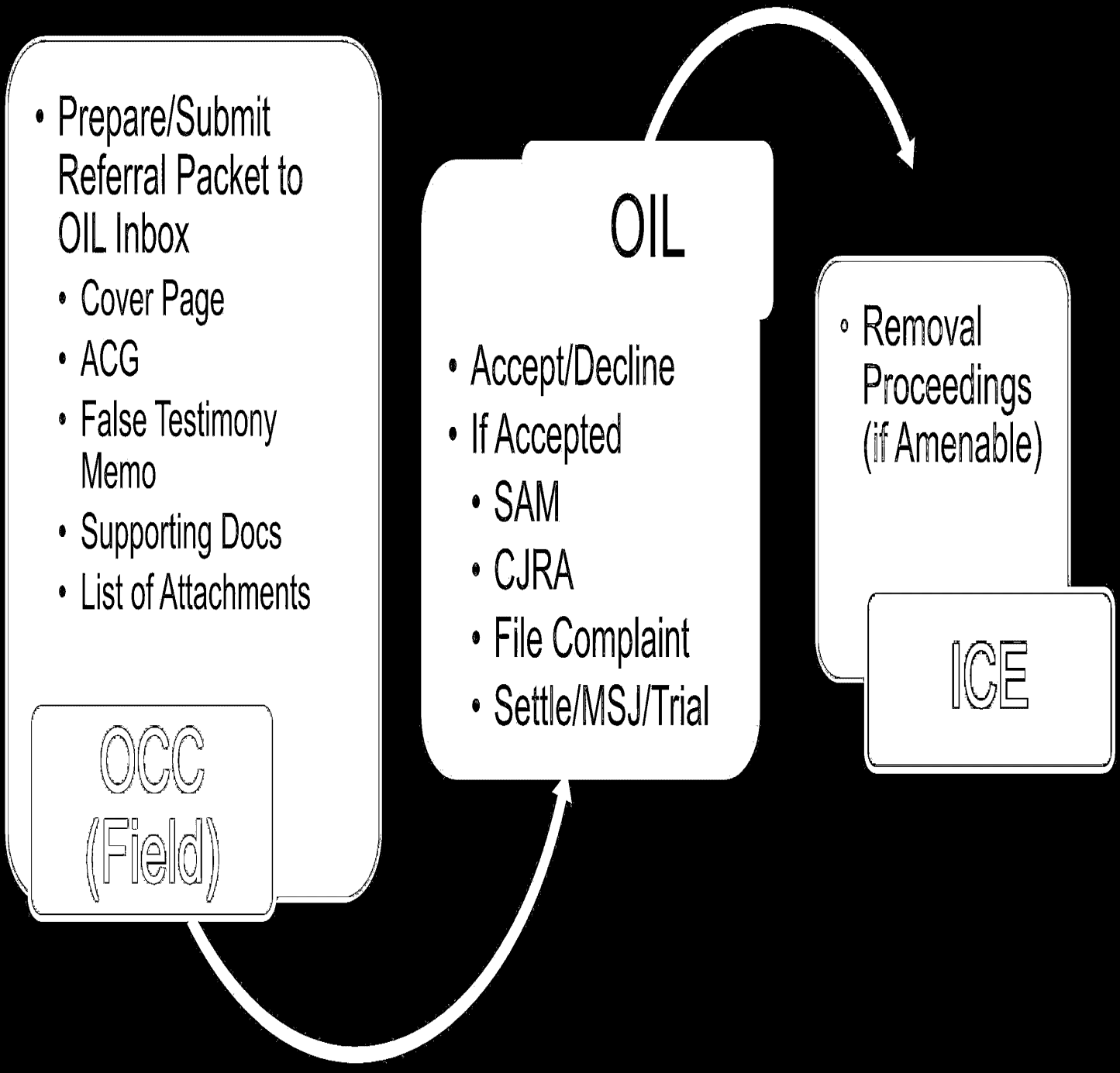
OIG Project – Case Preparation



U.S. Citizenship and Immigration Services

18

OIG Project – Case Referral



U.S. Citizenship and Immigration Services

19

(b)(5)

(b)(5)

U.S. Citizenship and Immigration Services

WLD Steps for HFE Denatz cases

As you are assigned an HFE matter, please take the following steps to ensure consistent handling of HFE matters within WLD:

Step 1: Update PMT

a. Change PMT Service Item Owner for case
    i. Go to WLD Dashboard
    ii. Click on report titled HFE (OIG) Denaturalization Cases
    iii. Look for your case-should be currently assigned to Kayla
    iv. Click on detail view
    v. Next to service item owner there is a place to click "change"

b. If no Field Office is listed, update the Field Office for the Service Item to indicate the Field Office that will provide the operational support (this is the office that has jurisdiction over the subject's place of residence, not necessarily the office that the assigned attorney sits in)

Step 2: Perform initial review of the AGC, A-File, and Preliminary Case Review sheet.

a. If you are not in D23, the A-file will be the electronic A-file uploaded on the ECN. You should review that A-file (left and right hand side).
b. As part of your review, please go to the OCC ECN HFE Denatz. http://ecn.uscis.dhs.gov/team/occ/SitePages/Denaturalization.aspx
c. There you will find the latest approved AGC template, samples AGCs being filed, and other useful materials.
d. You should also consult the WLD ECN Resource Library for additional guidance, template, etc. http://ecn.uscis.dhs.gov/team/occ/field/western/Resource%20Library/Forms/AllItems.aspx

Step 3: E-mail the HFE assigned officer (HFE ISO) as this will be the primary officer assigned to your case.

a. The HFE assigned officer is listed in the HFE email assigning the case to you.
b. If you need further assistance, you can contact the Branch Chief of the HFE Project, also listed on the email.
c. For FDNS assistance, reach out to the HFE FDNS officer (HFE FDNS IO) assigned on the email.
d. You may also inform the local Field Office management that you have received an HFE Denaturalization case and may need some basic operational support but you should not be using local field office resources if your issues can be resolved through your HFE ISO, HFE FDNS IO, or the HFE Branch Chief

Step 4: Determine location and status of witnesses

a. Reach out to local FOD where witnesses currently work to give a heads up that you may be contacting witnesses in their office.
b. Ask operational POC for assistance getting contact info for retired/separated employees

Step 5: Conduct in-depth A-file review and update AGC accordingly

a. Review AGC in detail for factual inaccuracies and confirmed facts with A-file.
b. Check that statutory/regulatory citations are correct
    i. Corrections common to cases

- Citation of 245(a) when adjustment was under 209 (refugee/asylee) or 245(i)

c. Review legal sufficiency of claims
    i. Check HFE ECN page for outstanding legal questions and note on AGC which claims are subject to an outstanding question

Step 6: Schedule interview with N-400 adjudicator(s) and HFE ISO to discuss adjudicator's standard practices for N-400 interviews

a. Sample questions available on ECN
b. If witness is no longer employee, best option is to have the witness come to a USCIS office to review documents. If this is not possible, discuss with your supervisor other options for providing records to the former employee

Step 7: Conduct interview/discussion with N-400 adjudicator(s)

a. Best practice is for attorney to take lead on questioning and allow HFE ISO to ask follow-up questions
b. If questions related to the witness's personal circumstances that would affect ability to be a witness need to be discussed, have that discussion on a separate call with the witness, without the HFE ISO

Optional Step 7A: Complete false testimony (Optional)

c. Sample memo on ECN
d. Options for memo
    i. Attorney completes
    ii. LOS ISO completes
    iii. Employee who is interviewed completes

Step 8: Respond to HFE ISO with edited AGC and reconcile any comments/edits with HFE ISO

Optional Step 8A: Compete memo detailing any discovery issues if applicable (b)(6)

a. Sample on HFE ECN page

Step 9: Complete Referral Cover Sheet

a. "Submitted by" will be John D. Miles [redacted] Deputy Chief Counsel for Field Mgt.
b. Sheet will be dated when the final packet is e-mailed to Denatz box

Step 10: Create attachments for the AGC and draft table of contents

Step 11: Forward AGC (in Word format), attachments (in single PDF document), draft table of contents, and referral cover sheet for supervisory review

b. Refer case initially to first line supervisor
c. After first line review, case should be referred to Janette, Theresa, and/or John for additional comments before AGC is finalized, copy your supervisor
d. Once supervisory edits are received, make changes to AGC and have AGC signed by LOS ISO

Step 12: Submit finalized packet to HFE Denatz e-mail box

a. Complete referral packet with attachments and page numbers for table of contents
b. Referral sheet should be dated with the date the packet is e-mailed to the HFE Denatz box
c. Respond to the initial e-mail that you received notifying you that the case had been assigned to you
d. Copy your supervisor

Step 13: Update PMT to record hours worked

a. Cheat sheet on HFE ECN page
b. Only 1 activity is entered to record total hours worked
c. Include time your first line supervisor spent reviewing your case
d. Kayla will perform other updates to PMT to indicate that the case has been referred to OIL and the name of the OIL attorney assigned
e. Kayla will notify you once OIL has received the case and an OIL attorney has been assigned

Step 14: Complete paragraph to be included in Denatz monthly report and send e-mail to Janette with paragraph

a. Sample language:

On ___ __, 2017, USCIS referred the case of _____, A__-___-___, aka _____, A__-___-___, to OIL for civil denaturalization. [Ms./Mr.]_____ initially entered the United States without inspection, and when encountered by INS gave a false name and claimed to be a U.S. citizen. She eventually admitted that she was not a U.S. citizen, but then gave INS a second false name. She was criminally prosecuted and convicted under 18 U.S.C. 911, False Claim to Citizenship. Following her conviction, she was placed in deportation proceedings under the second false name, and after failing to appear for a scheduled hearing was ordered deported in absentia. Subsequently, using the name Carmen Rosario, she became a permanent resident based on her marriage to a lawful permanent resident. She did not reveal her criminal conviction, her previous identity, or her immigration history. She ultimately naturalized under the Carmen Rosario identity. The USCIS OCC field attorney assigned to this case is _____(phone number).

Step 15: OIL Attorney will reach out with next steps

a. If OIL attorney requests that we provide the fingerprint comparison, inform the attorney that USCIS has provided information to Tim Belson regarding the process to obtain a fingerprint comparison/witness. The OIL attorney should follow up with their chain if they have further questions about the agreement that was made, but in short, the fingerprint comparison/witness will not be provided only when the case is going to be filed in federal court.

Table of Contents

A. A File Requests

B. A File Certification

C. AGC

D. Litigation Hold

E. CJR Letter

F. Complaint

G. Current Address

VIII. Post Denaturalization -- Reserved

- Appendix A – Sample HFE Email Assigning the Case with POC Information
- Appendix B – Sample CISOCCDENATZ email to OIL referring denaturalization case

OCC Guidance for HFE Denatz cases

The guidance below is based on the last available information as of the "LAST UPDATED" date contained in the header. This document aims to provide procedural guidance and best practices specific to a certain subset of denaturalization cases. To the extent that USCIS is standing up a denaturalization project for the first time since the creation of the agency, the procedural guidance and best practices will necessarily remain fluid as the agency develops additional expertise in this area. If you identify matters not covered in this document that should be covered, or if items in this document are different from what you are experiencing in your cases, you may access an editable version of this document on the OCC ECN where you may provide comments or make recommended changes.

Background

On September 8, 2016, the DHS Office of Inspector General issued a report entitled "Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records." Based on those findings, USCIS established a unit within the LOS District Office – known as the HFE[1] FOD Unit --to review potential denaturalization cases.

The officers assigned to the HFE FOD Unit initially review potential denaturalization cases and draft the statutorily required Affidavit of Good Cause (AGC) in appropriate cases. Because the A files are physically located in LOS and will initially remain in LOS (unless they are already digitized in EMDS), the HFE FOD Unit will scan the files and upload them to the HFE FOD Unit ECN. Once the HFE FOD Unit has finalized its initial review and completed the draft AGC, the case is referred to OCC for review and further action as necessary.

OCC has established a centralized inbox (CISOCCDENATZ) to receive all cases from the HFE FOD Unit. The incoming email from the HFE FOD Unit will list the ISO and IO assigned to the case and will also contain links to the A files and draft AGC located in the HFE FOD Unit ECN. A sample email is contained in Appendix A. The CISOCCDENATZ box will then forward the case to the appropriate OCC managers, based on jurisdiction, for assignment to a specific OCC attorney. Once OCC has cleared the case for referral, CISOCCDENATZ will refer the case to OIL. A sample email is contained in Appendix B.

In addition to the HFE FOD Unit ECN, where the A Files and case specific documents are accessed, attorneys may also access the OCC ECN, which contains the latest background documents, training materials, templates, and samples.

[1] The cases identified as part of the OIG report are referred to as HFE cases because the ICE-led project to upload old paper fingerprint cards into IDENT, called the Historical Fingerprint Enrollment (HFE), is what resulted in the identification of cases where individuals with multiple identities received immigration benefits. While the OIG report identified a discrete group of HFE cases based on old fingerprints that had been uploaded into IDENT as of a certain date, additional fingerprint cards continue to be uploaded to IDENT. Any potential denaturalization cases identified as part of HFE will be handled the same way, regardless of whether they were initially part of the OIG report or were identified later.

General Order of Events

While the steps you take in any particular case may differ, the general lifecycle of an HFE Denaturalization Case will be as follows (and each point is described more fully in the remainder of the document):

1. Upon receipt of the case, contact the HFE FOD Unit to advise that you have been assigned a case.

2. Review the A file and draft AGC provided by the HFE FOD Unit.

3. Work with the HFE FOD Unit to ensure legal bases for denaturalization contained in draft AGC are legally sufficient.

4. If any basis for denaturalization requires information from an officer who adjudicated an immigration benefit, coordinate with the HFE FOD Unit to contact those potential witnesses.

5. If potential witnesses are interviewed, work with the HFE FOD Unit to memorialize the conversation as appropriate.

6. Finalize the AGC in coordination with the HFE FOD Unit.

7. Submit the AGC to the OCC supervisor who is responsible for reviewing the denaturalization case, as established by your Division, for review and concurrence.

8. Prepare Referral Packet and Referral Cover Sheet.

9. Once the AGC is executed, finalize referral packet, including list of attachments and the Referral Cover Sheet.

10. If possible, create one PDF of all documents so long as the PDF size does not exceed 18MB. If the PDF exceeds 18MB, create multiple PDFs as necessary.

11. Email PDF(s) to the CISOCCDENATZ mailbox, encrypted as necessary.

12. Update PMT throughout the process as necessary.

13. Once the case has been referred to OIL, update the monthly report with a summary of the denaturalization case.

14. RESERVED – additional steps addressing coordination with OIL, including settlement discussions, discovery, and litigation holds will be added later. Additionally, post denaturalization action items will also be added later.

Guidance

I. PMT

A. In General

1. OCC is using PMT to, among other things, track cases referred to OCC from the HFE FOD Unit, track OCC hours devoted to specific cases, track cases referred to OIL once the case has been cleared by OCC, and run various reports. Accordingly, entering information into PMT for these cases is crucial.

B. Specific PMT guidance for HFE Cases

1. Service Item Owner

a. Please ensure the Service Item Owner is completed according to your Division's guidance. In some Divisions, the Service Item Owner is the attorney handling the case, in others it's a paralegal or legal assistant.

b. To change the Service Item owner, follow these steps:

- Look for your case – it will generally be assigned to Kayla Kostelac
- Click on detail view
- Next to service item owner there is a place to click "change" and enter the correct owner

2. Location of Case: Client Office, Field Office, and Division

a. These fields should already be updated in PMT when you are assigned a case. For purposes of these cases, PMT is being updated as follows:

- The Client Office and Field Office fields should indicate the office that adjudicated the naturalization application, not necessarily the office that is providing litigation support.
- The Division data field should indicate the OCC Division that is responsible for handling the denaturalization matter, regardless of where the naturalization adjudication occurred. Accordingly, the Client Office and Field Office may not match the Division in these cases.

3. Hours

a. Update the number of hours spent by **any** OCC personnel on these cases. Step-by-step instructions to report hours for the HFE cases can be found here.

b. The hours should be reported as one cumulative number. The update may be done by anyone, so long as there is one responsible party per case ensuring that the hours are appropriately updated. Accordingly, if the practice within your Division is for attorneys to update the hours, please ensure the attorneys are also accounting for work done by supervisors, legal assistants, paralegals, support staff, etc. Similarly, if the practice in within your Division is for a paralegal or legal assistant to update the hours, please ensure they are accounting for work done by others.

4. Reports

a. Various reports have already been developed in PMT to track cases. You may access the reports under the "Reports" tab. The reports are contained within the JANUS folder.

b. While you may access any of the reports, please do not change any of the report data fields unless you first save the report to your own folder.

II. HFE FOD Unit

A. The HFE FOD Unit is responsible for all operational aspects of the HFE denaturalization cases. The Unit takes the place of the local field office for most operational matters, except as otherwise specifically noted. The POCs from the HFE FOD Unit should be updated regarding matters in these cases the same way you would update your local office.

B. Upon receipt of the case, email the HFE ISO alerting him/her that you will serve as the OCC POC for the case.

C. The assigned HFE ISO is listed in the HFE email assigning the case to you. See Appendix A. The HFE ISO will serve as your primary operational contact for the case; however, if you cannot reach the HFE ISO or have general questions regarding operational matters, you may also send an email to the HFE FOD Inbox which is monitored daily. Please note that OCC has a standing call with the HFE FOD Unit every two weeks and process issues affecting more than your individual case should be raised to the CISOCCDENATZ inbox for general discussion with the HFE FOD Unit.

D. For FDNS assistance, reach out to the HFE FDNS officer (HFE FDNS IO), who is also listed in the email assigning the case to you.

E. You may inform management from the appropriate Field Office that you have received an HFE Denaturalization case but you should not be using local field office resources if your issues can be resolved through your HFE ISO, HFE FDNS IO, or the HFE FOD Unit, **unless** you are advised by the HFE FOD Unit to specifically coordinate locally.

III. OCC Denatz ECN

A. The OCC ECN contains 5 main libraries: Referral Documents, Samples, HFE/Denatz Pending Questions, Reports, and Training/Background Documents. Each is described further below.

B. Referral Documents -- This library contains the latest version of the template AGC, the Referral Cover Sheet, and outline of the AGC grounds, as well as a synopsis of recent updates to the AGC.

1. Referral Cover Sheet

a. The Referral Cover Sheet was developed in coordination with OIL to quickly highlight the type of denaturalization case that is being referred to OIL. It must be completed in every case.

b. The cover sheet also contains a "notes" section. Any issues or concerns regarding a case should be highlighted for OIL in that section. For example, if false testimony is not included in a specific case, the "notes" section would highlight that false testimony was considered but excluded from the AGC. It is not necessary that this section contain a detailed explanation of the issues; it is meant to highlight the matter for further discussion with OIL at a later time.

c. The "Submitted by" section at the bottom of the Referral Cover Sheet is already prepopulated with John Miles's information. You only need to enter the correct date in that section.

2. AGC

a. The OCC ECN contains two template AGCs –one entitled "AGC Comprehensive Template – Redline" and the other entitled "AGC Comprehensive Template – Clean."

b. Both versions should be the same. The redline version simply exists to highlight what edits have been made to the "clean" version recently. Generally, the redlines will remain for at least a month to ensure that all attorneys have had a chance to review any recent changes to the template.

c. Attorneys assigned to work on HFE cases should review the AGC template with some frequency to determine whether any updates have been included.

3. Outline of AGC Grounds

a. This document is simply an outline of the order in which the AGC grounds appear within the template

4. Recent Updates to AGC

a. This document is simply a list of recent changes that have been made to the AGC.

C. Samples

1. This section of the ECN contains various sample documents:

a. Complaints

b. Lit Holds

c. Memos

d. Referral Packets

2. Attorneys are encouraged to upload samples to the ECN that present new issues than the samples already available.

D. Reports

1. This section of the ECN contains a monthly report summarizing the cases referred that month.

2. The current month's report will appear as a Word document. Once a case has been referred to OIL, the attorney should update the Word document with a summary of the case.

3. The summary should roughly follow the example below:

- On ___ __, 2017, USCIS referred the case of _____, A__-___-___, aka _____, A__-___-___, to OIL for civil denaturalization. [Ms./Mr.][NAME] initially entered the United States without inspection, and when encountered by INS gave a false name and claimed to be a U.S. citizen. She eventually admitted that she was not a U.S. citizen, but then gave INS a second false name. She was criminally prosecuted and convicted under 18 U.S.C. 911, False Claim to Citizenship. Following her conviction, she was placed in deportation proceedings under the second false name, and after failing to appear for a scheduled hearing was ordered deported in absentia. Subsequently, using the name [NAME], she became a permanent resident based on her marriage to a lawful permanent resident. She did not reveal her criminal conviction, her previous identity, or her immigration history. She ultimately naturalized under the [NAME] identity. The USCIS OCC field attorney assigned to this case is _____(phone number).

4. Reports from previous months are also contained in this library as PDF documents.

E. HFE/Denatz Pending Questions

1. This section of the ECN is under development. It will contain options papers addressing the various pending legal questions related to the HFE cases for leadership consideration.

F. Training/Background Documents

1. This section of the ECN contains general background and training documents, including notes from the Denaturalization Brown Bag meetings.

IV. Reviewing the Denaturalization Case

A. Once you have received a denaturalization case, review the draft AGC, A-File, and Preliminary Case Review sheet. All these items will be found on the HFE FOD Unit ECN and links to them will also be included in the email assigning the case to you.

B. A files

1. If you are not physically in LOS, you will not have access to the paper A file. The A-file(s) you will review will be the scanned copies of A files uploaded to the HFE FOD Unit ECN, unless the file has already been digitized in EDMS, in which case you will review the digitized A file.

2. Other A files.

a. Currently, the HFE FOD Unit is not routinely requesting related files in advance of drafting the AGC.

b. If after your review of the case you determine that additional files may be relevant to the legal sufficiency determination, you may discuss the need for additional files with the HFE ISO. At this time, there is no standardized practice for having the HFE FOD Unit receive related files for scanning and posting on the HFE FOD Unit ECN. Accordingly, decisions on who should request the file and where it should be received will necessarily be handled on a case by case basis. Generally, the local office in which the OCC attorney is located may be amenable to facilitating the request and storage of these related files. If so, you should coordinate with the appropriate POC in your office. If you believe additional files are necessary for your review of the case, and the HFE FOD Unit and your local office raise objections to requesting the additional files, please advise your supervisor.

C. AGC Review

1. Review the AGC in detail to confirm all facts and citations, ensure the legal accuracy of all grounds contained in AGC, and determine whether additional grounds may be applicable. OCC review necessarily includes a determination about whether a case is legally sufficient, such as consideration of specific circuit precedent where the case will be filed that may affect one or more grounds included in the AGC. Additionally, evidentiary issues that may affect the legal viability of the case should also be considered and addressed with the HFE FOD Unit. If OCC believes a case is not legally sufficient, but the HFE FOD Unit disagrees with the OCC determination, please raise the matter to your supervisor.

2. The latest AGC template can be obtained on the OCC ECN.

3. Be mindful of unresolved legal issues (which will be listed in the OCC ECN) that should not be included in AGC unless cleared by a supervisor.

4. Common mistakes in AGCs:

a. Citing 245(a) when the adjustment occurred under 209 or 245(i).

b. Citing the current version of 212(a)(6), when the earlier version of the inadmissibility ground was applicable.

c. Citing to adjustment when the person was admitted on an immigrant visa.

D. EOIR ROPs

1. It may be necessary to obtain an EOIR ROP or to listen to a recorded hearing. To date, we do not have a centralized request system with EOIR. If information from EOIR is necessary, please work with your local ICE counterpart. Raise any issues in receiving the information you need to your supervisor.

E. Witness Interviews

1. Depending on the grounds contained in the AGC, it may be necessary to interview an officer who adjudicated the N-400 or an officer who adjudicated another application in the A file.

2. If it is determined that such an interview is necessary, work with the HFE FOD Unit POC to identify the officer and schedule an appropriate time to discuss the case with the officer.

3. When interviewing the officer, the HFE ISO should also participate in the interview. Both OCC and the ISO may ask questions of the officer, but OCC may lead the interview.

4. If concerns arise regarding the witness's personal circumstances that would affect his or her ability to be a witness, have that discussion on a separate call with the witness, without the HFE ISO.

5. If the officer is still employed with the government, the relevant applications may be sent by email, encrypted as necessary, if the officer is not co-located with either the OCC POC or the HFE FOD Unit POC.

6. If the officer is no longer employed with the government, and it is not possible to interview that former officer in person, please consult with your supervisor before sending documents from the A file to a non-governmental email account.

7. The OCC ECN contains a list of sample questions that may be asked during such an interview. The questions are simply a sample and the questions in the interview in your case may differ.

8. The interview with the officer may be memorialized in short memo prepared by the HFE FOD Unit POC. Memorializing the conversation is not required.

9. **IMPORTANTLY**: OCC must assess whether the officer's testimony supports the particular ground of denaturalization for which that officer's testimony is sought. If there are concerns about an officer's testimony, the case may be referred without inclusion of that particular denaturalization ground, assuming other grounds of denaturalization exist. If it is referred without this ground, please include that information in the "notes" section of the referral cover sheet.

10. Unavailability of Officer:

a. Deceased -- If the officer is deceased, another officer, generally one who was in a supervisory position over that officer at the time of the adjudication, may be interviewed to establish the deceased officer's pattern and practice.

b. Retired -- if the officer is retired and cannot be located, another officer, generally one who was in a supervisory position over that officer at the time of the adjudication, may be interviewed to establish the retired officer's pattern and practice.

c. Retired and unwilling to participate – if the officer is retired and unwilling to assist the government, OCC should assess the need for the particular denaturalization ground and whether the case should be referred without including any allegations that require the officer's testimony.

F. Union Issues

1. In consultation with CALD, it has been determined that these officer interviews, which are being conducted solely to determine whether a legal basis exists to allege a particular ground of denaturalization, are not the types of engagements for which union representation would be appropriate.

2. HQ FOD sent out an email to the DDs, FODs, the NBC, and Service Center Directors advising them of this determination; accordingly, an officer should not request union representation in these cases. However, should an officer insist on union representation in these cases, please ensure the HFE FOD Unit POC is aware of the request, and also advise your supervisor.

3. **Do not** conduct an officer interview for purposes of denaturalization if the officer insists on union representation. Instead, raise the matter to your supervisor.

4. After consultation with your supervisor, a denaturalization case may be referred without a particular ground for denaturalization if that ground is dependent upon an officer's testimony and there are concerns or issues with that officer's testimony. In such cases, please include a brief description of the issue on the Referral Cover Sheet.

G. Fingerprint Comparisons for Litigation

1. The HFE FOD Unit will be obtaining fingerprint comparisons from the ICE Forensic Lab in advance of referring a case to OIL for cases referred after November 2017.

2. If you are ready to refer a case to OIL, inform the HFE FOD Unit POC so they may request the fingerprint comparison. For any cases referred before November 2017, OIL will request the fingerprint comparison. Any issues regarding fingerprints should be raised to your supervisor.

H. Finalizing the Denaturalization Case

1. Once you have finalized your review of the denaturalization case, refer the case to the supervisor who is responsible for reviewing the denaturalization case, as established by your Division.

2. After the case is approved by the supervisor, prepare the case for referral to OIL.

3. To refer the case to OIL the following items must be completed:

a. Referral Cover Sheet

b. Index/List of Attachments

c. Executed AGC

- The original AGC remains with the A file. A scanned copy of the AGC is what is referred to OIL.

d. Attachments that support the allegations in the AGC

- For cases referred after December 2017, the attachments should include a fingerprint comparison from the ICE Forensic Lab.

4. If possible, all these documents should be scanned into 1 PDF, so long as the PDF size does not exceed 18MB. If the PDF exceeds 18MB, create multiple PDFs as necessary. The PDF(s) will then be emailed, encrypted as necessary, to the CISOCCDENATZ inbox.

a. Any documents with full social security numbers must be encrypted when sent by email, even when the email is being sent internally. As many forms (including most N-400s) have full social security numbers listed, it is important these forms not be sent by email without encryption.

b. Please review the Office of Privacy Connect Page for guidance on how to handle PII and SPII. Some relevant links to documents dealing with PII and SPII are included below:

- USCIS Management Directive Handling Sensitive and Non-Sensitive PII.
- Privacy Newsletter 4 and 1 Issue Final (See page 4)
- Office of Privacy webpage – Q&A
- Privacy Newsletter – Combined 2nd and 3rd Quarter

c. As established by the Office of Privacy, documents containing SPII may be sent using PKI, the information may be attached in an encrypted file, or the information may be redacted. Please ensure any one of the appropriate methods is used when sending SPII.

5. The CISOCCDENATZ inbox will notify you once the case has been referred to OIL and again when the OIL POC is assigned.

6. The CISOCCDENATZ inbox will notify the HFE FOD Unit once the case has been referred to OIL.

7. The CISOCCDENATZ inbox will also notify the ICE DENATZ INBOX that the case has been referred to OIL.

V. Post Referral to OIL

A. A File Requests

1. The OIL attorney will request a copy of the subject's A-files by email. Until a decision is made on other procedures for file sharing, an uncertified, encrypted copy of the A file may be transmitted to OIL by email in cases where there is no classified information in the A file.

B. A File Certification:

1. USCIS will not certify A files upon initial referral to OIL. There are ongoing discussions regarding the timing of the certification of the A file. Any requests to certify the A file in advance of a complaint being filed should be referred to the CISOCCDENATZ mailbox.

C. AGC

1. The OIL attorney may want to discuss aspects of the AGC and the case in general, including why certain allegations were included or omitted; issues implicating unresolved USCIS legal positions should be elevated through your supervisor within USCIS OCC.

2. If an additional ground of denaturalization is added, or a ground is deleted, in advance of filing the complaint, OIL will ask that the AGC be amended and executed again. It is OIL's preference that the AGC and Complaint contain the same grounds of denaturalization at the time the Complaint is filed.

3. In cases where the subjects address changes in advance of filing of the complaint, OIL will ask that the AGC be executed again.

D. Litigation Hold

1. OIL attorney will send litigation hold memo to USCIS, ICE, CBP. OCC is currently working with OIL regarding the litigation hold notices. Until further notice, proceed with litigation holds in these cases as you would normally proceed with any litigation hold in a non-denaturalization case.

E. CJR Letter

1. In advance of filing a complaint, and absent extenuating circumstances, DOJ must attempt to engage in pre-filing settlement discussions with the putative defendant and/or his or her attorney. Accordingly, in advance of filing the complaint, OIL must send out a Civil Justice Reform (CJR) letter to the putative defendant.

2. The OIL attorney should provide the draft CJR letter to assigned USCIS attorney for review and comment. The CJR letter is sent to subject to advise him/her of the government's intent to initiate denaturalization proceedings in federal court and to provide him/her an opportunity to settle the matter before the complaint is filed. In every case, the one non-negotiable term of settlement is that the subject will not retain U.S. citizenship. OCC should review the CJR for factual and legal accuracy and for any unresolved issues which may have project-wide implications. If significant substantive revisions are proposed, elevate within chain of command for concurrence.

F. Complaint

1. The OIL attorney should provide draft Complaint to assigned USCIS attorney for review and comment. The Complaint will generally track the AGC, but this is not a legal requirement. Assertions in the AGC may not have been included in the Complaint, and the Complaint may contain assertions not made in the AGC. The OCC field attorney should review for factual and legal accuracy and for any unresolved issues which may have HFE project-wide implications. If significant substantive revisions are proposed, elevate within chain of command for concurrence.

G. Current Address

1. Once the CJR letter and complaint have been finalized, but before the CJR letter is sent, OIL will request confirmation that the subject's physical address remains as listed in the AGC.

2. OCC should work with the HFE FOD Unit POC to confirm the subject's current address through available means. Absent other indicators that the subject is not residing at the address contained in the AGC, confirmation via public record and other electronic sources is sufficient.

3. If there are indicators within USCIS records (e.g. FOIA request post-dating AGC, petition filed post-AGC) that the subject's address may have changed, the HFE FOD FDNS POC may need to enlist the assistance of local FDNS to confirm current address through means other than public record.

VI. Post Denaturalization – Reserved

Appendix A

Sample incoming email from HFE FOD Unit when denaturalization case is ready for OCC review.

From: Kwan, Russell S
Sent: Wednesday, November 29, 2017 6:36 PM
To: CISOCCDENATZ
Cc: Miles, John D; Martinez, Janette M; Campagnolo, Donna P; Chau, Anna K; Gearhart, Mark A; D'Angelo, Caroline M; Andrade, Daniel W; Salidzik, Christina E (Christy)
Subject: FW: HFE Denatz - Massachusetts - Massachusetts District Court

OCC Denatz:

The following case for Denatz has been loaded to the ECN:

Primary Last Name:	[redacted]
Primary A Number (N400):	[redacted]
USCIS District:	District 1
State:	Massachusetts
District Court:	Massachusetts District Court
ECN Link to District Library:	(Click Here)
ECN Link to HFE Home page:	(Click Here)

The HFE ISO assigned to the case is:

Caroline D'Angelo

(b)(6) [redacted]

Appendix B

Sample email from CISOCCDENATZ to OIL referring a denaturalization case.

-----Original Message-----
From: Kostelac, Kayla A
Sent: Friday, October 13, 2017 11:49 AM
To: 'usdojgov, denaturalization (CIV)'
Cc: Shin, Sandra H; Rojes, Kathleen M; Roy, David V
Subject: FW: AGC Packet [redacted] 603

Good Morning OIL,

In addition to the 2 emails I sent containing 3 attachments for the AGC referral packet on [redacted], as well as the email containing the password, I am sending this email with the following copied, so you have their contact information:

POC: Sandra Shin
Deputy Chief: Kathleen Rojes
Chief of the Western Law Division: David Roy

Please also note that the HFE subject has filed a mandamus regarding an I-130 filed on behalf of her daughter, so there is time sensitivity to this matter.

Thank you,

Kayla Kostelac
Legal Assistant
(b)(6) Office of the Chief Counsel
U.S. Citizenship and Immigration Services U.S. Department of Homeland Security
Office: [redacted]

-----Original Message-----
From: Kayla Kostelac [ma[redacted]
Sent: Friday, October 13, 2017 11:45 AM
To[redacted]
Subject: AGC Packet [redacted] 603

Good Morning OIL,

Attached please find parts 1 and 2 of the AGC referral packet for [redacted] Associate Counsel Sandra Shin is the OCC POC on this case and I will forward her contact information to you. However, in addition to contacting Sandra Shin regarding this case, you may also contact Kathleen Rojes, Deputy Chief, or David Roy, Chief of the Western Law Division. I will forward their contact information on as well. I will be sending one more email containing part 3 of the AGC referral packet, and I will also email you the password for the AGC attachments. If you could please confirm receipt of this email, and send the contact information for an OIL POC, I would appreciate it. Please let me know if you have any questions.

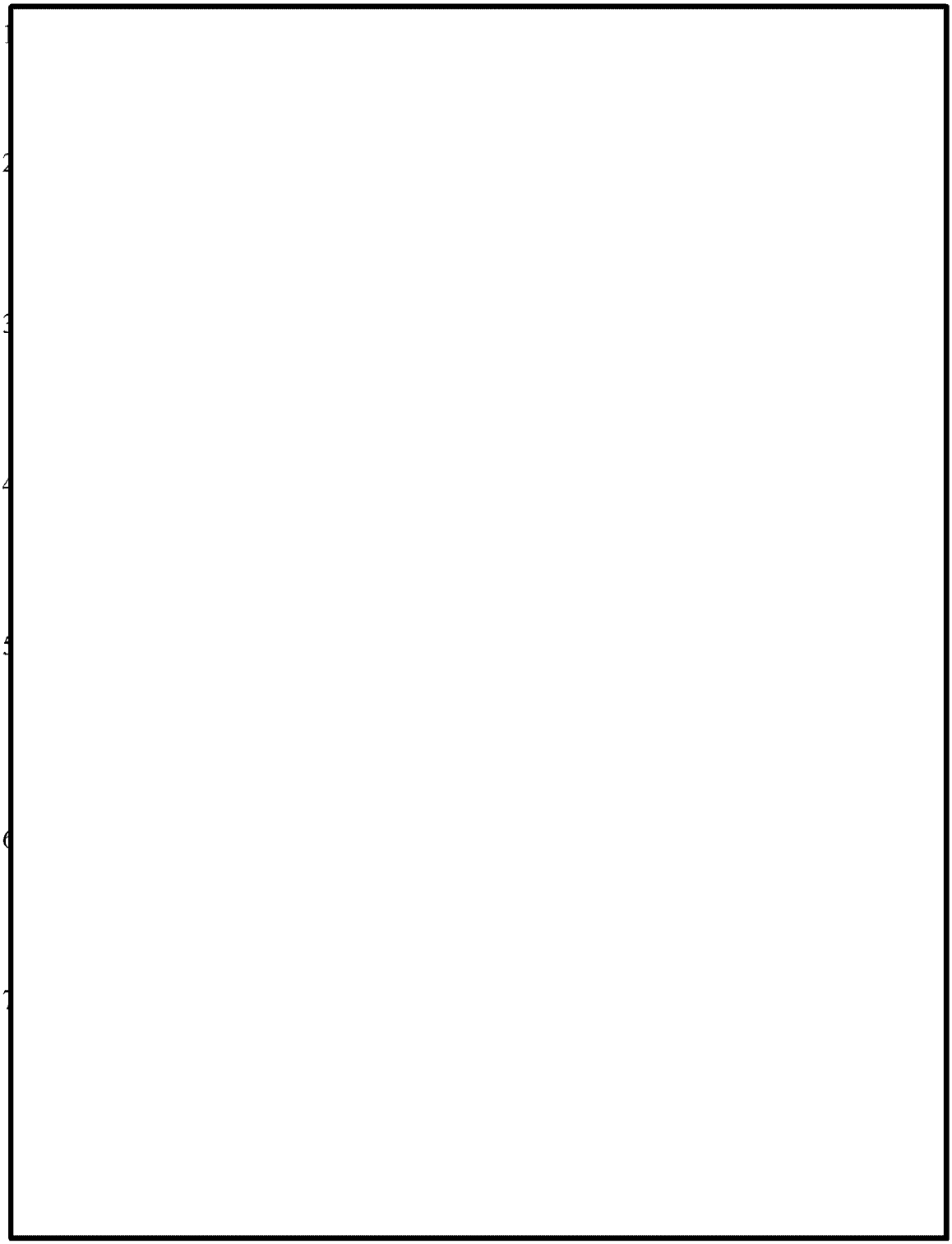
Thank you,

Kayla Kostelac
(b)(6) Legal Assistant
Office of the Chief Counsel
U.S. Citizenship and Immigration Services U.S. Department of Homeland Security
Office: [redacted]
ref:_00DG0hO5S._500t0761F0:ref

ATTORNEY-CLIENT NOTES - DO NOT RELEASE

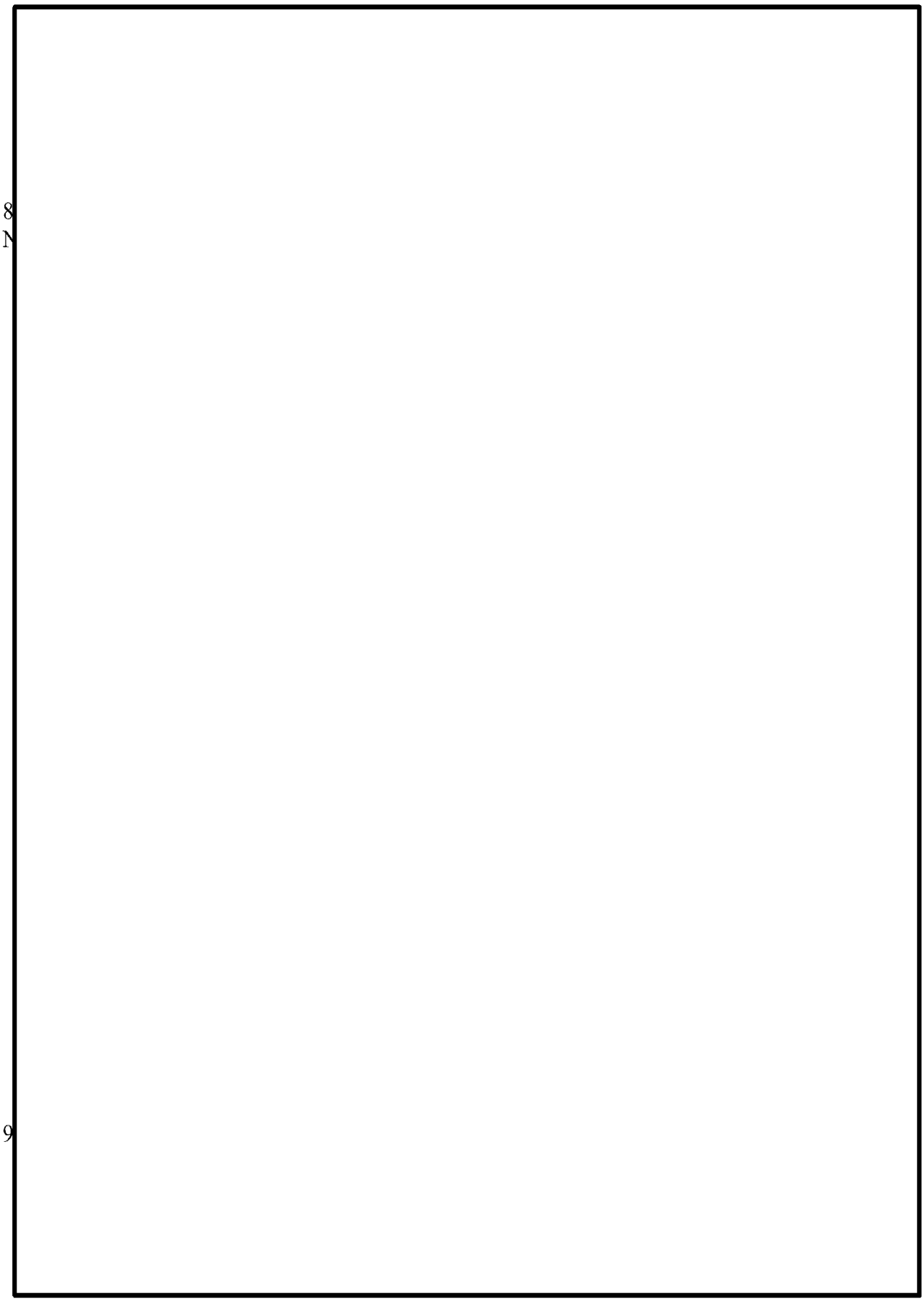
These notes provide sample questions that will be used in contemplation of litigation. They are privileged and are not releasable.

(b)(5)



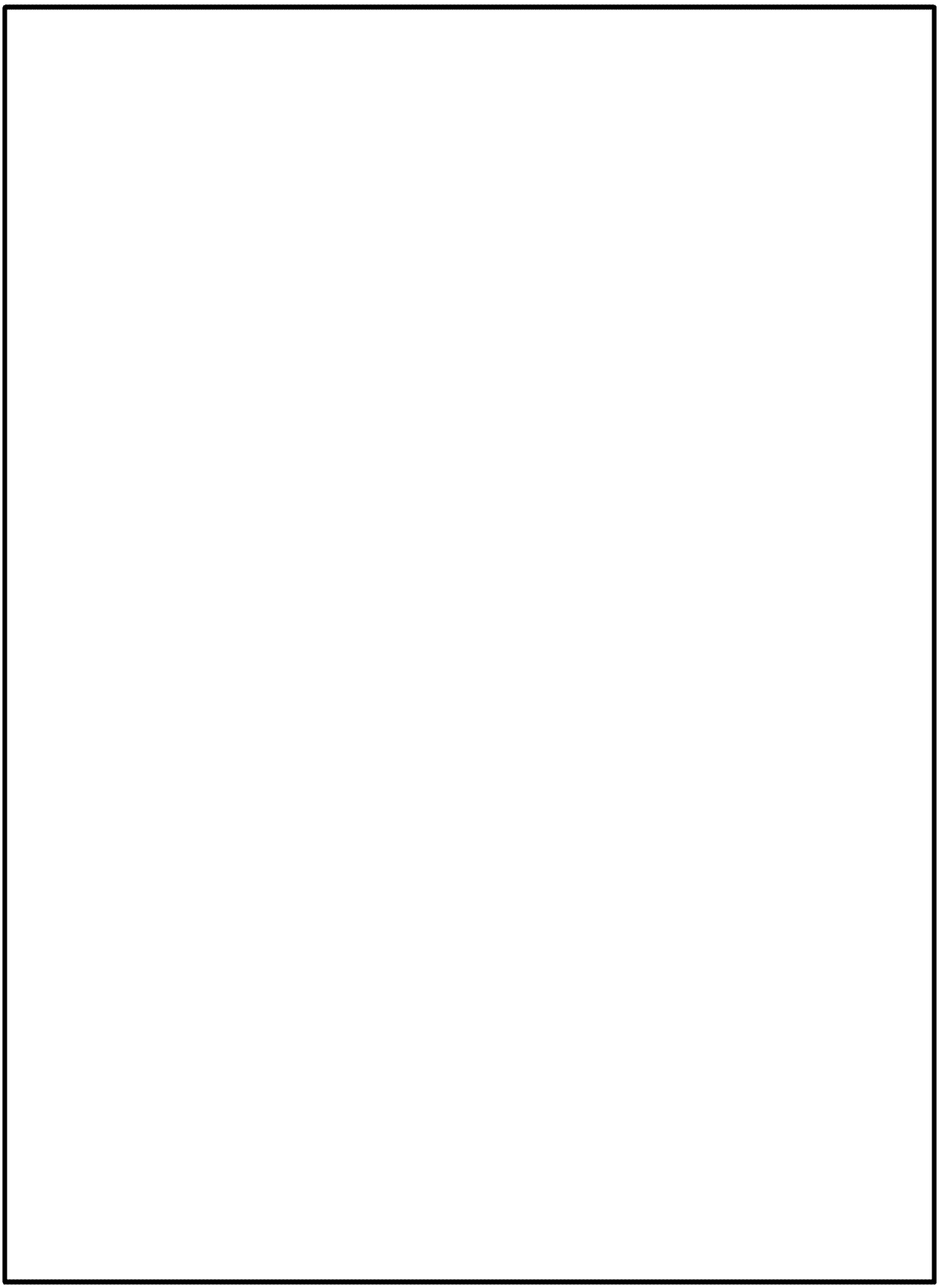
ATTORNEY-CLIENT NOTES - DO NOT RELEASE
ATTORNEY-CLIENT NOTES - DO NOT RELEASE

(b)(5)



ATTORNEY-CLIENT NOTES - DO NOT RELEASE

(b)(5)



(b)(5)

Steps to Creating Referral Packet

(1) Obtain a list of the required documents, preferably in the order the attorney wants them to appear in the packet.

(2) Create a new PDF where you will put the extracted pages from the A-file along with any other documents the attorney provides to be inserted into the packet
   (a) Finalized referral packet will be in this order:
      (i) coversheet first,
      (ii) list of packet attachments (table of contents),
      (iii) AGC
      (iv) Fingerprint comparison,
      (v) then other documents specified in the list of attachments.

   Prior to supervisory review, the AGC, and list of attachments should remain in word format due to changes that may be made before final submission

(3) Extract pages from the A-files (see tip sheet)

(4) Adding Bookmarks to the PDF will be helpful as you add pages to the packet (see tip sheet)

(5) Save the document as "[Name] Referral Packet"

(6) Provide draft packet to attorney in order to submit to supervisor for review along with the word document AGC

(7) Once you receive notice from the attorney that supervisory review is complete and all documents are finalized and ready for submission, create the finalized packet by inserting the signed AGC and any other missing documents.

(8) To finish the packet, add Bates numbering starting with the AGC as page 1. (see tip sheet).

(9) Complete the list of attachments/table of contents with corresponding page numbers and insert into the referral packet after the coversheet.

(10) Insert a date into the coversheet (date packet will be submitted by attorney to the Denatz box)

(11) Save packet as a reduced size pdf (see tip sheet)

(12) E-mail (encrypted unless SSN is redacted) completed referral packet back to attorney for final submission.

Tasks for HFE Denatz cases

1. **Update PMT**
    a. Change PMT Service Item Owner for case
        i. Go to SELD Dashboard
        ii. Click on report titled HFE (OIG) Denaturalization Cases
        iii. Look for your case-should be currently assigned to Kayla
        iv. Click on detail view
        v. Next to service item owner there is a place to click "change"

    b. If no Field Office is listed, update the Field Office for the Service Item to indicate the Field Office and District where the subject naturalized, the division should still say SELD regardless of where the naturalization occurred.

2. **Perform initial review of the AGC**, A-File, and Preliminary Case Review sheet
    a. To gain access to client's ECN page e-mail cisoccdenatz@uscis.dhs.gov
    b. Depending on the circumstances, you may want to locate and review family members' A-files. When case is referred to OIL, the OIL attorney typically asks for the immigration status of spouses/children/parents of the subject.

3. **Determine location and status of witnesses**.
    a. Reach out to local FOD and OCC attorneys where witnesses currently work to give a heads up that you may be contacting witnesses in their office
    b. Ask operational POC for assistance getting contact info for retired/separated employees

5. **Conduct in-depth A-file review and update AGC** accordingly
    a. Review AGC in detail for factual inaccuracies
    b. Compare draft AGC to newest template to ensure AGC has been updated correctly to reflect the language in the newest template
    c. Check that statutory/regulatory citations are correct
    d. Review legal sufficiency of claims
        i. Check HFE ECN page for outstanding legal questions and note on AGC which claims are subject to an outstanding question

6. **Schedule interview with N-400 adjudicator**(s) and LOS ISO to discuss adjudicator's standard practices for N-400 interviews
    a. Sample questions available on ECN  ISO interview questions sample.doc  examiner questions updated.docx
    b. If witness is no longer employee, best option is to have the witness come to a USCIS office to review documents. If this is not possible, discuss with your supervisor other options for providing records to the former employee

7. **Conduct interview/discussion with N-400 adjudicator**(s)
    a. Best practice is for attorney to take lead on questioning and allow ISO to ask follow-up questions

b. If you need to ask questions related to the witness's personal circumstances that would affect ability to be a witness, have that discussion on a separate call with the witness, without the LOS ISO

8. **Complete false testimony memo** (Optional)
   a. Sample memo on ECN

Dhanoa False Testimony Memo to Fi

9. **Respond to LOS ISO with edited AGC** and reconcile any comments/edits with LOS ISO

10. **Compete memo detailing any discovery issues** if applicable
    a. Sample on HFE ECN page

(b)(6)

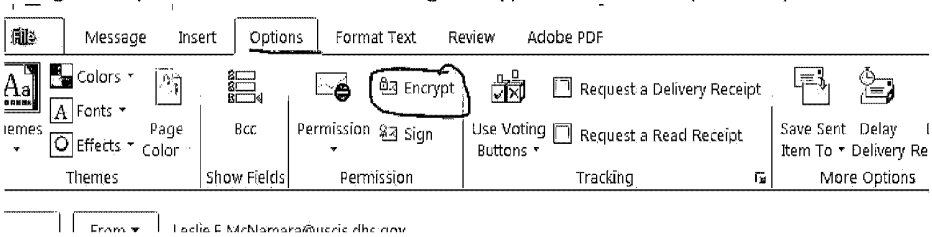
11. **Complete Referral Cover Sheet**
    a. "Submitted by" will be John D. Miles, [redacted] Deputy Chief Counsel for Field Mgt.
    b. Sheet will be dated with the date the final packet is e-mailed to Denatz box

12. **Create attachments for the AGC and draft table of contents**
    a. Contact Leslie if you would like to have the paralegals extract documents from the A-files and assemble the packet.
    b. The attorney should identify the list of documents needed by name of document and A-number if necessary. Paralegals will create a PDF with the attachments from the A-file in the order specified. The paralegal will then forward the PDF containing the attachments to the attorney.
    c. 

Example list of attachments.docx

    d. Steps to create the packet are listed on the SELD ECN Documents library

13. **Forward AGC (in Word format), attachments (in single PDF document), draft table of contents, and referral cover sheet to first line supervisor**
    a. Encrypt all e-mails that contain SSNs in attachments either by encrypting the e-mail by using the Options menu and checking encrypt or with winzip and a password



14. **Once supervisory edits are received, make changes to AGC and have AGC signed** by LOS ISO
    a. ISOs who have left the HFE project and returned to their prior position within USCIS may still sign the AGC

15. **Request Fingerprint Comparison** from the HFE Unit and wait to complete packet until the comparison is received.
    a. Normally takes a few days

16. **Compete Referral packet**
    a. Add AGC and fingerprint comparison to the packet, add page numbering and complete table of contents by adding the corresponding page numbers to the list of attachments for the documents listed. Contact Leslie if you would like paralegal assistance to create the packet.
    b. Referral sheet should be dated with the date the packet is e-mailed to the HFE Denatz box.
    c. Referral cover sheet should briefly note what claims were intentionally left out of AGC due to outstanding legal questions, witness issues, etc. This will give OIL a heads up regarding our view of the claims if they are considering adding claims to the complaint.
    d. Save the packet as a reduced size pdf. If the file is greater than 18 MB, you may have to break it down into two parts for submission to OIL due to PMT/e-mail size limits

17. **Submit finalized packet** to HFE Denatz e-mail box
    a. Encrypt the packet (Winzip with password) if the packet contains SSNs
    b. Copy your supervisor

18. **Update PMT** to record hours worked
    a. Cheat sheet on HFE ECN page

Instructions for
Entering Denatz Time

    b. Only 1 activity is entered to record total hours worked
    c. Track time using "JANUS" as the subject of the activity and then your total time, such as "JANUS 24.5"
    d. Include time your first line supervisor spent reviewing your case
    e. Kayla will perform other updates to PMT to indicate that the case has been referred to OIL and the name of the OIL attorney assigned

19. Kayla will notify you once OIL has received the case and an OIL attorney has been assigned

20. **Complete paragraph to be included in Denatz monthly report** and add paragraph to report
    a. Report is located on HFE ECN page on the right under the Reports Section. Chose the report for the month your case was sent to OIL and add your paragraph directly to the report.
    b. Use the date you sent the final packet to the box as the date you referred. You don't have to wait until you get notification that OIL received the case.
    c. Sample language:

    On ___ __, 2017, USCIS referred the case of _____, A__-___-___, aka _____, A__-___-___, to OIL for civil denaturalization. [Ms./Mr.]_____ initially entered the United States without inspection, and when encountered by INS gave a false name and claimed to be a U.S. citizen. She eventually admitted that she

was not a U.S. citizen, but then gave INS a second false name. She was criminally prosecuted and convicted under 18 U.S.C. 911, False Claim to Citizenship. Following her conviction, she was placed in deportation proceedings under the second false name, and after failing to appear for a scheduled hearing was ordered deported in absentia. Subsequently, using the name Carmen Rosario, she became a permanent resident based on her marriage to a lawful permanent resident. She did not reveal her criminal conviction, her previous identity, or her immigration history. She ultimately naturalized under the Carmen Rosario identity. The USCIS OCC field attorney assigned to this case is _____(phone number).

21. **Provide Litigation Support** to OIL Attorney

a. **A-file Copies**: OCC is working with OIL so that we can jointly use a file sharing system to facilitate sharing the entire A-files but that system is not in place yet. In order to e-mail the A-file copies:
   i. Open A-file PDFs in Adobe Pro, then "save as" and reduced size PDF
   ii. Encrypt the document using Winzip with a password
   iii. Send one PDF at a time if necessary
   iv. Send final e-mail with Winzip password

b. **HSI/AUSA interest in case** as criminal denatz instead of civil: generally defer to DOJ regarding how to bring the case
   i. Add PMT note that the case is in criminal Denatz

c. **Litigation Holds**
   i. Once you receive notification from OIL/USAO email the ISO at the HFE Project in LOS who drafted the Affidavit of Good Cause in your case and have them acknowledge receipt of the hold and demonstrate that they understand their obligations under the litigation hold (implement, conduct search, & preserve relevant documents)

d. **Certified Copies** of records
   i. Submit the request below to the HFE ISO. Separate requests for each document are needed unless you are requesting the entire file.
   ii. 
   Formal Request for Certification of True C

e. **Discovery Issues**
   i. Asserting privileges for 3rd Agency documents
      - CBP: has a rotating duty attorney who can be reached at [redacted]
      - ICE: refer to local ICE OPLA attorneys who handle denaturalization
        Orlando = Pamela Dieguez and Alexandra Rivas
        NC/SC [redacted]

(b)(6)

      - FBI:

- DOS: [redacted] this is the e-mail address used to obtain use authorization for DOS documents

f. **Settlement Issues**
   i. Consent Judgments vs. Settlement Agreements: OIL sees consent judgments as something that the client does not have to approve, but settlement offers that bind the agency to take an action or refrain from taking a certain action have to be approved by the client.
   ii. Family Members: OIL's reading of INA 340(d) is that if the subject is denaturalized based upon illegal procurement, the citizenship status of any spouse or child is not automatically affected, but the government could pursue denaturalization in a separate action if those family members obtained naturalization through the subject. If the denaturalization is due to concealment of a material fact or willful misrepresentation, then the citizenship of any spouse or child that obtained naturalization through the subject will automatically be terminated.
   iii. OIL's strategy is to not address which identity is the true identity so that getting a travel document or renewed LPR card is not complicated by the subject admitting that the naturalized identity is not in fact the true identity.
   iv. I-90s: What happens when the subject admits that the naturalization identity is the wrong identity and then files an I-90 to get replacement green card that contains the admitted to false identity?

       John and Janette working on this issue, no resolution right now
       Ultimately what we will do to provide these people status is not clear yet.

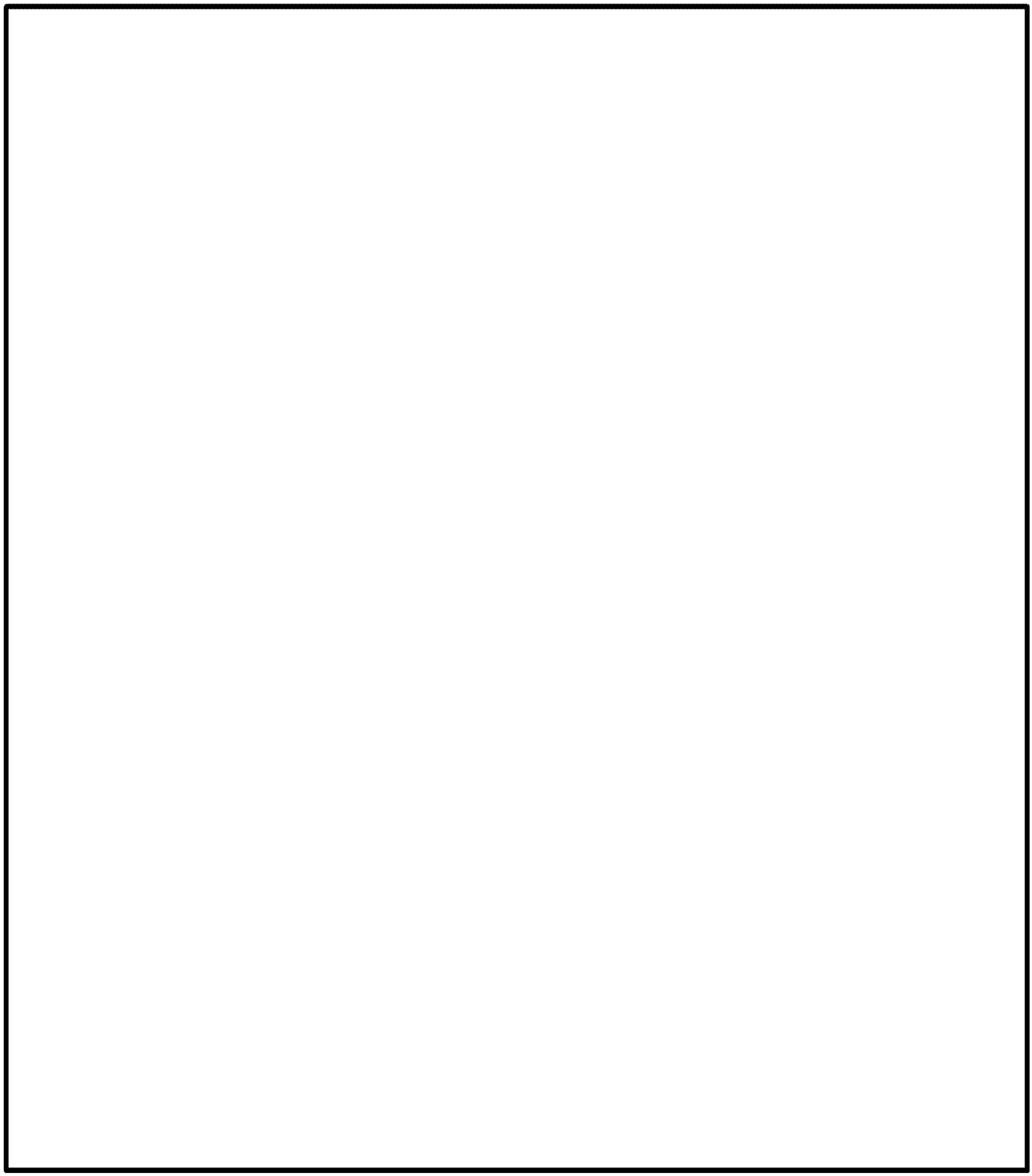
g. **Cancellation/Destruction of the Naturalization Certificate**
   i. Addressed in the CHAP; the RPM and the OSI Handbook
   ii. "VOID" should be written across the naturalization certificate, and the court order and naturalization certificate should be placed in the A-file. ICE or CIS can Void the document.
   iii. Send a copy of the court order and voided naturalization certificate by e-mail to COW RECORDS and CIS HQ Records will update the necessary systems to reflect the denaturalization.
   iv. The original naturalization certificate must be destroyed per OSI Secure Forms Procedures. CIS Records in the Local Office should complete this
   v. A copy of the voided certificate will remain in the A-file.

22. **Continue to update PMT**
   a. with hours spent on case
   b. when complaint is filed in District Court, forward complaint to fed lit mailbox so that Andrea or Jenny can update necessary fields

ATTORNEY-CLIENT NOTES - DO NOT RELEASE

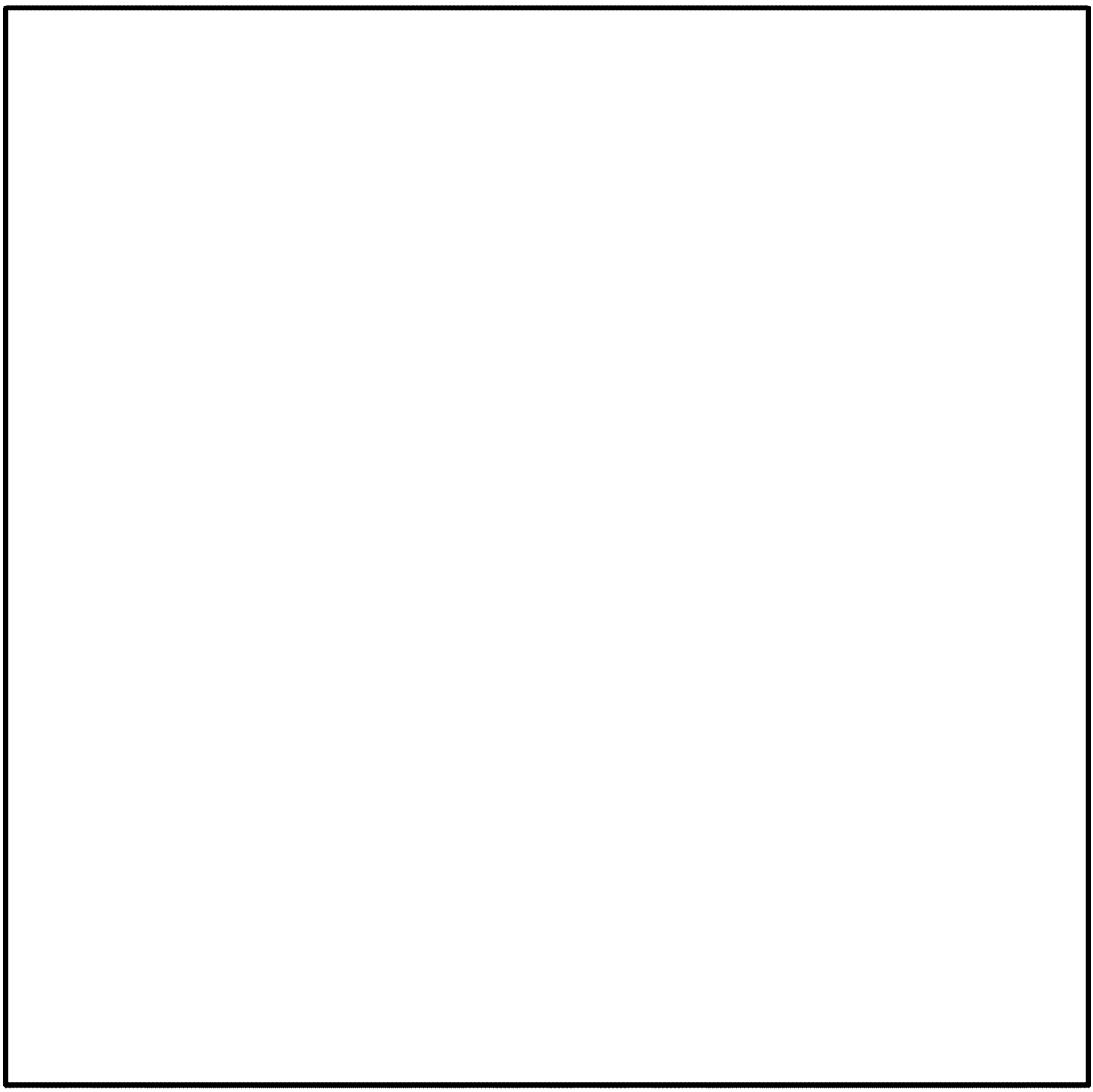
Discussion with _____ Date:_____

(b)(5)



ATTORNEY-CLIENT NOTES - DO NOT RELEASE
ATTORNEY-CLIENT NOTES - DO NOT RELEASE

(b)(5)



ATTORNEY-CLIENT NOTES - DO NOT RELEASE

(b)(5)

(b)(5)

Operation Janus

Talking Points

Top Line Messages

- Fighting fraud and ensuring the integrity of our immigration system are major priorities for USCIS. Operation Janus seeks to protect the integrity of the system against current and prior fraud.
- USCIS identifies and refers to the Department of Justice those individuals believed to have committed criminal fraud. The Justice Department prosecutes cases where criminal fraud is evident.
- Revocation of naturalization occurs in federal court and is a complex legal process that the Department of Justice commences with notification to the citizen that the United States intends to remove his or her citizenship.
- In these cases, the individuals sought to defraud the system by obtaining an immigration benefit under a different identity and were ordered removed.
- Prior to today's Biometric capability, USCIS relied on paper-based finger print scans. Biometrics in place today are intended to verify and validate identity. This technology capability has only existed for the past ten years.

Talking Points

- Operation Janus identified 315, 000 cases with some fingerprint data missing. Among those cases, USCIS identified about 1,600 cases for referral to the U.S. Department of Justice (DOJ).
- These investigations began during the previous administration, as reflected in the DHS-OIG report of September of 2016, and the cases are the result of an ongoing collaboration between USCIS and DOJ to investigate and seek denaturalization proceedings against those who obtained citizenship unlawfully.
- As part of its mission to provide immigration benefits to eligible applicants, USCIS strives to combat fraud that poses a systemic risk to the integrity of our nation's immigration system.
- USCIS has dedicated resources, staff and the Fraud Detection and National Security Directorate which specifically serve to ensure that immigration benefits are given to those who are eligible under law.
- Due to the nature of our anti-fraud investigations, USCIS cannot provide additional details on the techniques and processes for how we handle these types of cases or the length of our investigations.
- Among those identified cases, some may have sought to circumvent criminal record and other background checks in the naturalization process.

1

Quote:

- L. Francis Cissna: "This case, and those to follow, send a loud message that attempting to fraudulently obtain U.S. citizenship will not be tolerated. Our nation's citizens deserve nothing less."

Joint News Release

Tues., Jan. 9, 2017

USCIS partners with Justice Department and Secures First Denaturalization As a Result of Operation Janus

On January 5, Judge Stanley R. Chesler of the U.S. District Court for the District of New Jersey entered an order revoking the naturalized U.S. citizenship of Baljinder Singh aka Davinder Singh, and canceling his Certificate of Naturalization, following a U.S. Citizenship and Immigration Services referral to the Justice Department.

After Judge Chesler's order, Singh's immigration status reverted from naturalized citizen to lawful permanent resident, rendering him potentially subject to removal proceedings at the Department of Homeland Security's discretion.

Singh's denaturalization is the first arising out of a growing body of cases referred to the Department of Justice by United States Citizenship and Immigration Services (USCIS) as part of Operation Janus. The action against Singh was filed contemporaneously with two other Operation Janus cases, as announced by the Justice Department on Sept. 19, 2017.

A Department of Homeland Security initiative, Operation Janus, identified about 315,000 cases where some fingerprint data was missing from the centralized digital fingerprint repository. Among those cases, some may have sought to circumvent criminal record and other background checks in the naturalization process. These cases are the result of an ongoing collaboration between the two departments to investigate and seek denaturalization proceedings against those who obtained citizenship unlawfully.

USCIS dedicated a team to review these Operation Janus cases, and the agency has stated its intention to refer approximately an additional 1,600 for prosecution.

"We appreciate the dedication of our Justice Department partners as we work together to ensure the integrity of our nation's legal immigration system," said USCIS Director L. Francis Cissna. "I hope this case, and those to follow, send a loud message that attempting to fraudulently obtain U.S. citizenship will not be tolerated. Our nation's citizens deserve nothing less."

"The defendant exploited our immigration system and unlawfully secured the ultimate immigration benefit of naturalization, which undermines both the nation's security and our lawful immigration system," said Acting Assistant Attorney General Chad Readler of the Justice Department's Civil Division. "The Justice Department will continue to use every tool to protect the integrity of our nation's immigration system, including the use of civil denaturalization."

2

Baljinder Singh aka Davinder Singh, 43, a native of India, arrived at San Francisco International Airport on Sept. 25, 1991, without any travel documents or proof of identity. He claimed his name was Davinder Singh. He was placed in exclusion proceedings, but failed to appear for his immigration court hearing and was ordered excluded and deported on Jan. 7, 1992. Four weeks later, on Feb. 6, 1992, he filed an asylum application under the name Baljinder Singh. He claimed to be an Indian who entered the United States without inspection. Singh abandoned that application after he married a U.S. citizen, who filed a visa petition on his behalf. Singh naturalized under the name Baljinder Singh on July 28, 2006. Singh has been residing in Carteret, New Jersey.

This case was investigated by USCIS and the Civil Division's Office of Immigration Litigation, District Court Section (OIL-DCS). The case was prosecuted by Counsel for National Security Aaron Petty of OIL-DCS's National Security and Affirmative Litigation Unit, with support from USCIS' Office of the Chief Counsel and USCIS' Field Operations Directorate.

Background:

Statement from July 2017

"Similar to other government agencies, the Department of Homeland Security (DHS) is working to address the challenges posed by the existence of legacy, paper-based files and records. The issues identified in the Office of Inspector General's (OIG) report are a consequence of old, paper-based fingerprint records. Today, all DHS fingerprints are digitally uploaded into IDENT, a data system accessible across all DHS components and interoperable with other federal agencies.

As noted in the OIG report, ICE identified a number of decades-old fingerprints—in legacy Immigration and Naturalization Service (INS) paper files—that were not digitized. The vast majority of these fingerprints date back to the 1990s. DHS currently digitizes all fingerprints and the number of remaining paper records will decrease as DHS continues to digitize old fingerprints.

To address instances in which potentially ineligible individuals may have been naturalized, and to further reduce the risk of any such cases in the future, the OIG made two recommendations, which the Department is currently, and in large part already had been, implementing.

First, ICE will continue digitizing all available paper-based fingerprint records for the files identified in the OIG report. Before the report was issued, ICE had already digitized the majority of the 315,000 records which it had previously identified as having potentially missing paper fingerprint records. Due to a lack of funding, that effort did not complete the digitization process. The remaining number will now be reviewed and digitized.

Second, the Department has established a USCIS-led review team, which is working closely with ICE and DHS headquarters personnel to review every file identified in the OIG report as being a case of possible fraud and where digital fingerprint records were not or may not have been available at the time of the naturalization adjudication. This team has begun its review of the 858 identified cases to determine whether naturalization was fraudulently or otherwise improperly

3

obtained. In addition, the Department is also reviewing the 953 cases that the OIG identified, but was unable to verify, as lacking digitized fingerprint records at the time of the naturalization adjudication. This review builds on the prior and ongoing collaboration between DHS and DOJ to seek denaturalization when citizenship has been obtained unlawfully. As the OIG report notes, the Department had already identified and prioritized for potential criminal prosecution approximately 120 naturalized citizens who appear to have committed fraud and who avoided detection because their fingerprint records were not digitally available at the time of naturalization.

It is important to note that the fact that fingerprint records in these cases may have been incomplete at the time of the naturalization interview does not necessarily mean that the applicant was in fact granted naturalization, or that the applicant obtained naturalization fraudulently. Preliminary results from the file reviews show that in a significant number of these cases naturalization had been denied and that, in some, naturalization was not improperly granted. Other cases are subject to ongoing criminal investigation or to denaturalization proceedings that are pending or completed. Where the DHS review process finds that naturalization was obtained fraudulently, DHS will appropriately refer the case to the Department of Justice (DOJ) for civil or criminal proceedings, including for denaturalization.

Questions and Answers July 2017:

How can someone still be eligible to adjust status or have some sort of legal status in the United States if they've been deported or have claimed another identity?

Yes, it is possible that someone who has been removed (deported) or may have committed fraud or misrepresented information to be eligible to adjust. The immigration law makes waivers available in certain, limited circumstances to waive inadmissibilities related to fraud or willful misrepresentation, provided the applicant can show that removal from the United States would result in extreme hardship to a qualifying relative. An individual who has been removed (deported) from the United States may apply for permission to return to the United States, although this permission is not granted frequently. Additionally, under the law most removals do not result in a lifetime bar to returning to the United States; therefore, someone may return to the United States lawfully after removal if he/she has remained outside the United States for the requisite period of time.

Why doesn't the system catch this?

The Automated Biometric Identification System (IDENT) is a DHS-wide system for storing and processing biometric data. All IDENT users are federal, state, local, tribal, foreign, or international governmental agencies that have entered into written information sharing access agreements. IDENT performs certain quality checks and seeks to ensure that the data meets a minimum level of quality and completeness. However, it is ultimately the responsibility of the original data owner, whether an organization external or internal to DHS, to ensure the accuracy,

completeness, and quality of the data. Similar to other government agencies, the Department of Homeland Security (DHS) is working to address the challenges posed by the existence of legacy, paper-based files and records. The issues identified in the Office of Inspector General's (OIG) report are a consequence of old, paper-based fingerprint records. Today, all DHS fingerprints are digitally uploaded into IDENT, a data system accessible across all DHS components and interoperable with other federal agencies. As noted in the OIG report, ICE identified a number of decades-old fingerprints—in legacy Immigration and Naturalization Service (INS) paper files—that were not digitized. The vast majority of these fingerprints date back to the 1990s. DHS currently digitizes all fingerprints and the number of remaining paper records will decrease as DHS continues to digitize old fingerprints.

What happens once an application is approved, but someone has multiple identities through fingerprint data? Do they get their permanent resident card, work permit, etc revoked?

As stated in the report, if USCIS determines that an immigration benefits was obtained unlawfully, USCIS will review the case and take appropriate action, which may including rescinding, revoking, or terminating an immigration benefit, and/or initiating removal proceedings; or referring the case to the appropriate enforcement authority (i.e., ICE or DOJ).

What is being done in the fingerprint system to prevent this from continuing to happen?

Immigration and law enforcement officials now generally collect biometric information, including fingerprints, electronically and are no longer reliant on paper fingerprint cards. This will reduce the instances where paper fingerprint records are not available in digital systems.

[Defer to ICE to discuss ongoing efforts to digitize historical paper fingerprint contained in immigration files.]

OFFICE OF INSPECTOR GENERAL

Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records

Homeland Security

September 8, 2016

OIG-16-130

DHS OIG HIGHLIGHTS

Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records

September 8, 2016

Why We Did This Inspection

When aliens apply for U.S. citizenship, U.S. Citizenship and Immigration Services (USCIS) obtains information about their immigration history through fingerprint records. Our objective was to determine whether USCIS uses these records effectively during the naturalization process.

What We Recommend

We are recommending that ICE finish uploading into the digital repository the fingerprints it identified and that DHS resolve these cases of naturalized citizens who may have been ineligible.

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

USCIS granted U.S. citizenship to at least 858 individuals ordered deported or removed under another identity when, during the naturalization process, their digital fingerprint records were not available. The digital records were not available because although USCIS procedures require checking applicants' fingerprints against both the Department of Homeland Security's and the Federal Bureau of Investigation's (FBI) digital fingerprint repositories, neither contains all old fingerprint records. Not all old records were included in the DHS repository when it was being developed. Further, U.S. Immigration and Customs Enforcement (ICE) has identified, about 148,000 older fingerprint records that have not been digitized of aliens with final deportation orders or who are criminals or fugitives. The FBI repository is also missing records because, in the past, not all records taken during immigration encounters were forwarded to the FBI. As long as the older fingerprint records have not been digitized and included in the repositories, USCIS risks making naturalization decisions without complete information and, as a result, naturalizing additional individuals who may be ineligible for citizenship or who may be trying to obtain U.S. citizenship fraudulently.

As naturalized citizens, these individuals retain many of the rights and privileges of U.S. citizenship, including serving in law enforcement, obtaining a security clearance, and sponsoring other aliens' entry into the United States. ICE has investigated few of these naturalized citizens to determine whether they should be denaturalized, but is now taking steps to increase the number of cases to be investigated, particularly those who hold positions of public trust and who have security clearances.

Response

DHS concurred with both recommendations and has begun implementing corrective actions.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 8, 2016

MEMORANDUM FOR: The Honorable León Rodriguez
Director
U.S. Citizenship and Immigration Services

The Honorable Sarah R. Saldaña
Director
U.S. Immigration and Customs Enforcement

Richard Chavez
Director
Office of Operations Coordination

FROM: John Roth
Inspector General

SUBJECT: *Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records*

For your action is our final report, *Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records.* We incorporated the formal comments provided by your offices.

The report contains two recommendations aimed at improving the Department's ability to identify and investigate individuals who have obtained or may attempt to obtain naturalization through fraud or misrepresentation. Your offices concurred with both recommendations. Based on information provided in your response to the draft report, we consider both recommendations open and resolved. Once the Department has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions. Please send your updates to the status of recommendations 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 the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Anne L. Richards, Assistant Inspector General for Inspections and Evaluations, at (202) 254-4100.

Attachment

Table of Contents

Appendixes

Abbreviations

CBP	U.S. Customs and Border Protection
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FDNS	Fraud Detection and National Security Directorate
HFE	Historical Fingerprint Enrollment
IAFIS	Integrated Automated Fingerprint Identification System
ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System
INA	Immigration and Nationality Act of 1952
INS	U.S. Immigration and Naturalization Service
NGI	Next Generation Identification
OIG	Office of Inspector General
OPS	Office of Operations Coordination
TSA	Transportation Security Administration
USAO	Offices of the United States Attorneys
USCIS	U.S. Citizenship and Immigration Services
USC	U.S. Code

Background

In 2008, a U.S. Customs and Border Protection (CBP) employee identified 206 aliens who had received final deportation orders[1] and subsequently used a different biographic identity, such as a name and date of birth, to obtain an immigration benefit (e.g., legal permanent resident status or citizenship). These aliens came from two special interest countries and two other countries that shared borders with a special interest country.[2] After further research, in 2009, CBP provided the results of Operation Targeting Groups of Inadmissible Subjects, now referred to as Operation Janus, to DHS. In response, the DHS Counterterrorism Working Group coordinated with multiple DHS components to form a working group to address the problem of aliens from special interest countries receiving immigration benefits after changing their identities and concealing their final deportation orders. In 2010, DHS' Office of Operations Coordination (OPS) began coordinating the Operation Janus working group.

In July 2014,[3] OPS provided the Office of Inspector General (OIG) with the names of individuals it had identified as coming from special interest countries or neighboring countries with high rates of immigration fraud, had final deportation orders under another identity, and had become naturalized U.S. citizens. OIG's review of the list of names revealed some were duplicates, which resulted in a final number of 1,029 individuals. Of the 1,029 individuals reported, 858 did not have a digital fingerprint record available in the DHS fingerprint repository at the time U.S. Citizenship and Immigration Services (USCIS) was reviewing and adjudicating their applications for U.S. citizenship.

USCIS Review of Naturalization Applicants

People from other countries (aliens) may apply to become naturalized U.S. citizens and may be granted citizenship, provided they meet the eligibility requirements established by Congress in the *Immigration and Nationality Act of 1952* (INA).[4] USCIS adjudicates applications for naturalization, as well as other immigration benefits, such as asylum and lawful permanent resident status. Naturalization eligibility requirements in the INA include lawful admission for

[1] When an immigration judge orders an alien to be deported the judge issues an order of removal. In this report, we refer to orders of removal as deportation orders.
[2] Special interest countries are generally defined as countries that are of concern to the national security of the United States, based on several U.S. Government reports.
[3] As of November 2015, OPS had identified 953 more individuals who had final deportation orders under another identity and had been naturalized; some of these individuals were from special interest countries or neighboring countries with high rates of fraud. OPS did not capture the dates these 953 individuals' fingerprint records were digitized, so we could not determine the number whose records were available in the DHS digital fingerprint repository when their applications were being reviewed and adjudicated.
[4] 8 U.S. Code (USC) 1101 et seq.

permanent residence, continuous residence and physical presence in the United States, and good moral character. During the naturalization process, USCIS may determine that aliens who lie under oath about their identity or immigration history do not meet the good moral character requirement. Aliens with final deportation orders may not meet the INA's admissibility requirement, unless other circumstances make them admissible.

On naturalization applications and in interviews, aliens are required to reveal any other identities they have used and whether they have been in deportation proceedings. They must also submit their fingerprints. USCIS checks applicants' fingerprint records throughout the naturalization process. By searching the DHS digital fingerprint repository, the Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation (FBI) digital fingerprint repository, the Next Generation Identification (NGI) system,[5] USCIS can gather information about an applicant's other identities (if any), criminal arrests and convictions, immigration violations and deportations, and links to terrorism. When there is a matching record, USCIS researches the circumstances underlying the record to determine whether the applicant is still eligible for naturalized citizenship.

If USCIS confirms that an applicant received a final deportation order under a different identity, and there are no other circumstances to provide eligibility, USCIS policy requires denial of naturalization. Also, USCIS may refer the applicant's case to U.S. Immigration and Customs Enforcement (ICE) for investigation. Likewise, if a naturalized citizen is discovered to have been ineligible for citizenship, ICE may investigate the circumstances and refer the case to the Department of Justice for revocation of citizenship.

Results of Inspection

USCIS granted U.S. citizenship to at least 858 individuals ordered deported or removed under another identity when, during the naturalization process, their digital fingerprint records were not in the DHS digital fingerprint repository, IDENT. Although USCIS procedures require checking applicants' fingerprints against both IDENT and NGI, neither repository has all the old fingerprint records available. IDENT is missing records because when they were developing it, neither DHS nor the U.S. Immigration and Naturalization Service (INS), one of its predecessor agencies, digitized and uploaded all old fingerprint records into the repository. Later, ICE identified missing fingerprint records for about 315,000 aliens who had final deportation orders or who were criminals or

[5] Until September 2014, when the FBI announced it had replaced its old system with NGI, fingerprints were vetted against the Integrated Automated Fingerprint Identification System.

fugitives, but it has not yet reviewed about 148,000 aliens' files to try to retrieve and digitize the old fingerprint cards.

NGI is also missing records because, in the past, neither INS nor ICE always forwarded fingerprint records to the FBI. As long as the older fingerprint records have not been digitized and included in the repositories, USCIS risks making naturalization decisions without complete information and, as a result, naturalizing more individuals who may be ineligible for citizenship or who may be trying to obtain U.S. citizenship fraudulently. As naturalized citizens, these individuals retain many of the rights and privileges of U.S. citizenship, including serving in law enforcement, obtaining a security clearance, and sponsoring other aliens' family members' entry into the United States. ICE has investigated few of these naturalized citizens to determine whether they should be denaturalized, but within the last year has taken steps to identify additional cases for investigation.

Missing Digital Fingerprint Records Hinder USCIS' Ability to Fully Review Naturalization Applications

To determine whether there is any evidence that may make an alien ineligible for an immigration benefit, such as naturalization, USCIS has established procedures to check fingerprints against other sources of information. In addition, applicants are required to reveal all other identities and past immigration or criminal proceedings on their applications. However, even with fingerprint checks, unless fingerprint records are available or applicants reveal their immigration history, USCIS adjudicators will not know about all identities used by applicants, as well as any prior criminal or immigration issues or charges; therefore, they cannot fully review an application. Without this knowledge, adjudicators may grant citizenship to otherwise ineligible individuals.

The DHS Digital Fingerprint Repository Is Incomplete

During immigration enforcement encounters with aliens, CBP and ICE take fingerprint records. These components and their predecessor, INS, used to collect aliens' fingerprints on two paper cards. One card was supposed to be sent to the FBI to be stored in its repository. The other fingerprint card was to be placed in the alien's file with all other immigration-related documents.

In 2007, DHS established IDENT as the centralized, department-wide digital fingerprint repository. IDENT was built from a digital fingerprint repository

originally deployed by INS in 1994 (used primarily by the Border Patrol).[6] In 2008, according to officials we interviewed, ICE management directed its employees to send all fingerprints collected during immigration enforcement encounters to both IDENT and the FBI repository (at the time, the Integrated Automated Fingerprint Identification System or IAFIS, now NGI). At the same time, USCIS also began gathering fingerprints digitally and storing them in IDENT; since that time, the fingerprints of individuals who apply for immigration benefits requiring fingerprints are stored in IDENT.

Although fingerprints are now taken digitally and stored in IDENT, the repository is missing digitized fingerprint records of some aliens with final deportation orders, criminal convictions, or fugitive status whose fingerprints were taken on paper cards. The records are missing because when INS initially developed and deployed IDENT in 1994, it did not digitize and upload the fingerprint records it had collected on paper cards. Further, ICE investigators only began consistently uploading fingerprints taken from aliens during law enforcement encounters into the repository around 2010.

ICE has led an effort to digitize old fingerprint records that were taken on cards and upload them into IDENT. In 2011, ICE searched a DHS database for aliens who were fugitives, convicted criminals, or had final deportation orders dating back to 1990. ICE identified about 315,000 such aliens whose fingerprint records were not in IDENT. Because fingerprints are no longer taken on paper cards, this number will not grow. In 2012, DHS received $5 million from Congress to pull its paper fingerprint cards from aliens' files and digitize and upload them into IDENT, through an ICE-led project called the Historical Fingerprint Enrollment (HFE). Through HFE, ICE began digitizing the old fingerprint cards of the 315,000 aliens with final deportation orders, criminal convictions, or fugitive status and uploading them into IDENT. The process was labor intensive, requiring staff to manually pull the fingerprint cards from aliens' files. ICE reviewed 167,000 aliens' files and uploaded fingerprint records into IDENT before HFE funding was depleted. Some fingerprint cards were missing or unclear and could not be digitized. Since that time, ICE has not received further funding for HFE; efforts to digitize and upload the records have been sporadic, and the process has not been completed.

[6] In 2004, DHS copied the digital repository deployed by INS in 1994 and made it and other DHS information repositories available to the United States Visitor and Immigrant Status Indicator Technology Program. That program tracked aliens entering and exiting the United States by capturing their biographic information and digital fingerprints when they traveled. This version of IDENT ran in conjunction with the INS-developed digital repository the Border Patrol used until 2007 when the two repositories were merged to form the unified IDENT for all fingerprints collected by DHS.

The FBI Digital Fingerprint Repository Is Incomplete

The FBI has maintained a fingerprint repository since the 1920s, collecting and including in the repository fingerprints from state, local, and Federal agencies. INS and, later, ICE were supposed to provide copies of fingerprints collected during encounters with aliens to the FBI for its repository. In 1999, the FBI established a digital fingerprint repository, IAFIS, which facilitated electronic searches for fingerprint matches. In 2008, IAFIS and IDENT became capable of exchanging information with each other. In 2014, the FBI replaced IAFIS with a new digital fingerprint repository, NGI, which also exchanges information with IDENT.

When identifying aliens who were granted naturalized citizenship even though they had multiple identities and final deportation orders, Operation Janus checked NGI for matching FBI fingerprint records. These checks revealed that NGI does not contain all digital fingerprints from previous INS and ICE actions. ICE officials told us that, in the past, neither INS nor ICE always sent the FBI copies of paper fingerprint cards associated with immigration enforcement encounters. Also according to an official, ICE officers did not always update the information associated with fingerprint records to reflect issuance of final deportation orders. According to the FBI, it has digitized and uploaded into NGI all fingerprint records it received from DHS components and their predecessors, including all records related to immigration enforcement. NGI and IDENT are connected, so IDENT records can be accessed from NGI and NGI records can be accessed from IDENT.

USCIS Naturalized Individuals Who Had a Final Deportation Order Under a Different Identity

With neither a fingerprint record in IDENT, nor an admission by the applicant to alert adjudicators to an individual's immigration history, USCIS granted naturalization to individuals with final deportation orders who may not be eligible for citizenship. According to USCIS officials, merely having used multiple identities or having a previous final deportation order does not automatically render an individual ineligible for naturalization. Each applicant's specific circumstances must be thoroughly reviewed before a determination on eligibility can be made.

In these cases, however, USCIS adjudicators did not always have all the information necessary for a thorough review. Of the 1,029 individuals OPS identified who had final deportation orders under another identity and were naturalized, only 170 had fingerprint records in IDENT at the time of naturalization. The other 858 records were subsequently loaded into IDENT, but were not in the repository at the time of naturalization. If applicants had

revealed the facts of their immigration history, as required, on their applications and in interviews, USCIS adjudicators could have obtained the information. However, our review of 216 of these aliens' files showed that none of the applicants admitted to having another identity and final deportation orders on the naturalization application, and only 4 admitted to another identity and final deportation orders when USCIS adjudicators questioned them.

Because USCIS initially vetted applicants' fingerprints against NGI, adjudicators might also have obtained information about immigration histories from the FBI repository, but it is also missing records. Of the 1,029 naturalized citizens OPS identified as having multiple identities and final deportation orders, 40 had fingerprint records at the FBI. It is not clear whether these fingerprints were in the repository when the individuals were naturalized or whether the fingerprints were related to immigration offenses or other crimes.

Few of These Naturalized U.S. Citizens Have Been Investigated

Although their fingerprint records may not have been available in either the DHS or FBI digital repositories before these individuals were naturalized, all of their digital records are now available and their immigration histories are known. Some of these naturalized citizens may have attempted to defraud the U.S. Government. Yet, having been naturalized, they have many of the rights and privileges of U.S. citizens, including the right to petition for others to come to the United States and the right to work in law enforcement. For example, one U.S. citizen whom Operation Janus identified is now a law enforcement official. Naturalized U.S. citizens may also obtain security clearances or work in sensitive positions. Until they were identified and had their credentials revoked, three of these naturalized citizens obtained licenses to conduct security-sensitive work. One had obtained a Transportation Worker Identification Credential, which allows unescorted access to secure areas of maritime facilities and vessels. Two others received Aviation Workers' credentials, which allow access to secure areas of commercial airports.

Under the INA, a Federal court may revoke naturalization (denaturalize) through a civil or criminal proceeding if the citizenship was obtained through fraud or misrepresentation.[7] However, few of these individuals have been investigated and subsequently denaturalized. As it identified these 1,029 individuals, OPS referred the cases to ICE for investigation. As of March 2015, ICE had closed 90 investigations of these individuals and had 32 open investigations. The Offices of the United States Attorneys (USAO) accepted 2 cases for criminal prosecution, which could lead to denaturalization; the USAO

[7] 8 USC 1451(a), 8 USC 1451(e), and 18 USC 1425

declined 26 cases. ICE transferred two additional cases with fingerprint records linked to terrorism to the FBI's Joint Terrorism Task Force. ICE was scrutinizing another two cases for civil denaturalization.

According to ICE, it previously did not pursue investigation and subsequent revocation of citizenship for most of these individuals because the USAO generally did not accept immigration benefit fraud cases for criminal prosecution. ICE staff told us they needed to focus their resources on investigating cases the USAO will prosecute. In late 2015, however, ICE officials told us they discussed with the Department of Justice Office of Immigration Litigation the need to prosecute these types of cases, and that office agreed to prosecute individuals with Transportation Security Administration (TSA) credentials, security clearances, positions of public trust, or criminal histories. To date, and with assistance from OPS and USCIS, ICE has identified and prioritized 120 individuals to refer to the Department of Justice for potential criminal prosecution and denaturalization.

Recent Actions

In 2016, OPS eliminated Operation Janus and disbanded its staff, which raises concerns about the future ability of ICE and USCIS to continue identifying and prioritizing individuals for investigation. Since 2010 and until recently, Operation Janus identified these individuals, created watchlist entries to ensure law enforcement and immigration officials were aware of them, and coordinated DHS and other agencies' activities related to these individuals. Two DHS employees outside of OPS said that without Operation Janus, it would be difficult to coordinate these cases and combat immigration fraud perpetrated by individuals using multiple identities. We received this information late in our review and cannot assess the future impact of this change.

Conclusion

Given the risk of naturalizing aliens who may be ineligible for this immigration benefit and the difficulty of revoking citizenship, USCIS needs access to all information related to naturalization applicants. Because IDENT does not include 148,000 digitized fingerprint records of aliens with final deportation orders or who are criminals or fugitives, USCIS adjudicators may continue in the future to review and grant applications without full knowledge of applicants' immigration and criminal histories. ICE should review the remaining 148,000 aliens' files and digitize and upload all available fingerprint cards. By making these fingerprint records available in IDENT, USCIS would be better able to identify those aliens should they apply for naturalization or other immigration benefits and ensure a full review of their applications. This, in turn, would help prevent the naturalization of aliens who may be ineligible. In

addition, the digital fingerprint records could reveal others who have received immigration benefits to which they may not be entitled and should be investigated.

Recommendations

Recommendation 1. We recommend that the ICE Deputy Assistant Director for Law Enforcement Systems and Analysis complete the review of the 148,000 alien files for fingerprint records of aliens with final deportation orders or criminal histories or who are fugitives, and digitize and upload into IDENT all available fingerprint records.

Recommendation 2. We recommend that the Directors of USCIS, ICE, and OPS establish a plan for evaluating the eligibility of each naturalized citizen whose fingerprint records reveal deportation orders under a different identity. The plan should include a review of the facts of each case and, if the individual is determined to be ineligible, a recommendation whether to seek denaturalization through criminal or civil proceedings. The plan should also require documentation and tracking of the decisions made and actions taken on these cases until each has been resolved.

Management Comments and OIG Analysis

DHS concurred with our recommendations and has begun implementing corrective actions. In response to recommendation 1, ICE indicated that it has taken steps to procure contractor services to help review the 148,000 files and to digitize and upload to IDENT available fingerprint records. ICE anticipates awarding the contract before the end of fiscal year 2016. We will track ICE's progress in completing this recommendation.

The Department appears to be taking actions to address recommendation 2. DHS has established a team to review the records of the 858 aliens with final deportation orders who were naturalized under a different identity. The team will also review the 953 cases that OPS identified more recently and that we mention in footnote 3. During these reviews, the team will determine which individuals appear to have been ineligible for naturalization and will coordinate with DOJ for possible prosecution and denaturalization.

In addition, as the 148,000 fingerprints that are available are uploaded to IDENT, the team will evaluate whether any fingerprints match other identities of individuals who have been granted naturalization or other immigration benefits. The team will review records that are identified to determine whether ICE should investigate the individuals and coordinate possible prosecution

with DOJ. DHS plans to complete its review of these cases by December 31, 2016. We will track the Department's progress until the work is complete.

Appendix A
Objective, Scope, and Methodology

DHS OIG was established by the *Homeland Security Act of 2002* (Public Law 107-269) by amendment to the *Inspector General Act of 1978.*

The objective of our review was to determine whether USCIS uses fingerprint information effectively to identify naturalization applicants with multiple identities and final deportation orders.

We examined the records of 216 naturalized citizens that DHS OPS identified to confirm whether they: (1) had received final deportation orders under a second identity and (2) did not admit to the final deportation orders or identities on their naturalization applications. We also assessed TECS records and summary information related to investigations of these cases.

We analyzed communications among USCIS, CBP, ICE, and OPS personnel about these cases of possible naturalization fraud. We also reviewed user manuals, policies, system documentation, and summary presentations about the DHS fingerprint repository, IDENT, and the United States Visitor and Immigrant Status Indicator Technology Program Secondary Inspection Tool. We assessed USCIS user manuals, standard operating procedures, policies, guidance, and training material, as well as statutes and regulations related to final deportation orders, the naturalization and denaturalization processes, fraud detection, and use of fingerprint records. We reviewed ICE and CBP policies and procedures for handling naturalized citizens and legal permanent residents who have final orders of deportation under different identities, mission priorities, and coordination between DHS components and the Department of Justice.

We interviewed headquarters staff from DHS OPS, USCIS, ICE, CBP, the National Protection and Programs Directorate, and the Office of Policy. In addition, we travelled to Missouri and Kansas where we interviewed USCIS National Benefits Center staff in the Lee's Summit and Overland Park offices, and ICE staff at ICE Homeland Security Investigations' Kansas City field office. In addition, we met with CBP and ICE personnel at Dulles International Airport, JFK International Airport, and Newark Liberty International Airport. We also visited USCIS field offices in New York, New York; Newark, New Jersey; and Baltimore, Maryland, where we spoke with immigration services officers and FDNS personnel. In Virginia, we interviewed several CBP employees who worked in the National Targeting Center and a TSA employee familiar with vetting applicants for TSA-approved credentials. We conducted telephone interviews with USCIS adjudicators in Houston, Texas and Atlanta, Georgia, and ICE investigators in Los Angeles, California, Seattle Washington, and

Houston, Texas. We interviewed 46 USCIS staff members, 34 ICE staff members, 21 CBP staff members, 3 OPS staff members, and 5 staff members from the DHS Office of Biometric Identity Management and the Office of Policy.

We also interviewed FBI subject matter experts about the FBI fingerprint repository and information exchange with DHS.

After December 2015, we contacted subject matter experts in OPS, ICE, and USCIS to clarify issues in our report and to confirm that the conditions we identified had not changed. In May 2016, we briefed these subject matter experts on our report's findings and conclusions.

We conducted this review from July 2014 to December 2015 under the authority of the *Inspector General Act 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.

Appendix B
Management Comments to the Draft Report

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

Homeland Security

August 19, 2016

MEMORANDUM FOR: John Roth
Inspector General

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

SUBJECT: Management's Response to OIG Draft Report: "Potentially Ineligible Individuals Have Been Granted U.S. Citizenship Because of Incomplete Fingerprint Records" (Project No. 14-127-ISP-DHS)

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

Over the past 12 years, DHS has developed an integrated data system that provides DHS components with access to digitized fingerprints of individuals stemming from DHS encounters as well as to many federal law enforcement fingerprint records. This system is accessed and reviewed by U.S. Citizenship and Immigration Services (USCIS) as part of the adjudication process of naturalization applications. DHS fingerprints are currently taken in digitized form and included in the DHS repository, which is accessible across DHS components. As the OIG report notes, however, legacy paper-based records of fingerprints taken by DHS or by other law enforcement agencies may not yet be included in DHS's digitized repository of records. Hence, the existence of such legacy paper-based fingerprint records may not be known or accessible at the time of an immigration benefit determination by USCIS.

The OIG recognizes that in the processing of certain naturalization cases, USCIS submitted fingerprint checks that did not return criminal histories and other encounter information due to the absence of digitized fingerprint records in the DHS repository at the time the check was conducted. As a result, USCIS was not made aware of information that may have affected the applicants' eligibility to naturalize. As the OIG report also notes, the fact that the availability of legacy fingerprint records may show that an applicant has a record under a different name, has a prior removal order, or has a prior

criminal conviction does not necessarily demonstrate that the applicant was ineligible for naturalization or that naturalization was fraudulently obtained. A complete review of the hardcopy DHS "A-file" is necessary to make such a determination.

Consistent with the OIG's recommendations, the Department is undertaking a review of each hardcopy file of the cases identified in OIG's report and will refer to the U.S. Department of Justice (DOJ) those cases that DHS believes warrant criminal or civil denaturalization proceedings. Additionally, the Department is continuing to digitize legacy paper fingerprint records and will continue to determine if the digitization of old records reveals other cases that warrant investigation or referral to DOJ for civil or criminal denaturalization proceedings. The Department is committed to combatting immigration benefit fraud and ensuring that immigration benefits, including naturalization, are only granted to those individuals deserving under the law, thus ensuring the integrity of our immigration system. This includes continuing to identify and remove aliens who present either a danger to national security or a risk to public safety.

As mentioned in the draft report, DHS and its components have taken actions to address challenges posed by the existence of legacy paper-based fingerprint records. Most significantly, transitioning to digital fingerprint records and the implementation of systems such as IDENT means most law enforcement encounters and all DHS immigration encounters are digitally available and searchable across DHS components. These advancements, in addition to continually reviewing new cases as they come to DHS's attention and in conjunction with the steps outlined in this response to address the OIG's recommendations, will assist in substantially mitigating the risk of returning false negative record check results in the future.

The OIG report contained two recommendations, with which the Department concurs. First, as recommended by OIG, the Department is taking action to confirm the enrollment into IDENT of the remaining 148,000 fingerprint records referenced in the OIG report. This will complete the digitization of the 315,000 cases where ICE identified potentially missing paper fingerprint records. As noted in the report, ICE had already completed enrollment of a prioritized set of 167,000 of these records. DHS will continue its ongoing efforts to identify and upload into IDENT any paper fingerprint records not digitally available at the time the Department's repository was being developed and that may not yet be included in IDENT.

Second, as recommended by the OIG, the Department is reviewing each of the cases cited in the OIG report to identify those that warrant referral to the DOJ for civil or criminal denaturalization proceedings. The Department understands that OIG did not conduct an

in-depth review of each individual case identified in its report[1] to determine if complete criminal histories were not provided to USCIS at the time of the original USCIS review and adjudication of the individuals' naturalization application. Out of an abundance of caution, the Department is reviewing both the cases that the draft identifies as not having digitized fingerprint records at the time of adjudication and cases that the report indicated might lack such records. This effort is being led by USCIS, in collaboration with ICE and DHS headquarters personnel. In consultation with DOJ, DHS will refer appropriate cases for civil or criminal proceedings, including for denaturalization.

This review builds on the prior and ongoing work by ICE and other DHS components to open investigations and work with DOJ to seek denaturalization through civil or criminal proceedings of individuals who are determined to have obtained citizenship unlawfully. The draft report correctly notes that ICE has already prioritized a set of approximately 120 cases that will be referred to DOJ for potential criminal prosecution. Through its operating components, the Department continues to identify and prioritize individuals for investigation, efforts that had previously coordinated under the aegis of Operation Janus.

The draft report contained two recommendations with which the Department concurs. Please find our detailed response to each recommendation attached.

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

Attachment

[1] The cases to be reviewed includes not only the 858 individuals OIG identified as not having a digital fingerprint record available in the DHS fingerprint repository at the time USCIS reviewed and adjudicated their naturalization applications, but also the 953 individuals the draft report indicated *may* not have had a digital fingerprint record available in the repository at the time the naturalization applications were reviewed and adjudicated and who had final orders of removal under a different identity. The report did not specifically recommend review of the additional 953 cases, but DHS is subjecting them to the same scrutiny as the 858 cases. Together these total 1,811 names.

Attachment: DHS Management Response to Recommendations Contained in OIG 14-127-ISP-DHS

Recommendation 1: We recommend that the ICE Deputy Assistant Director for Law Enforcement Systems and Analysis complete its review of the 148,000 files for fingerprint records of aliens with final deportation orders or criminal histories or who are fugitives. It should digitize and upload into IDENT all fingerprint records that are available.

Response: Concur. ICE's Enforcement and Removal Operations (ERO) Directorate is currently taking action to confirm the enrollment into IDENT of the 148,000 fingerprint records referenced above, which actually represent "A-files" that may or may not contain one or more fingerprint cards suitable for enrollment in IDENT. To that end, ERO has initiated procurement actions to award a contract by the end of Fiscal Year 2016 to perform this work.

As the draft notes, the enrollment of these fingerprint records will complete a project to enroll approximately 315,000 such records identified by ICE, of which 167,000 were previously reviewed for enrollment.

Estimated Completion Date (ECD): September 30, 2017.

Recommendation 2: We recommend that the Directors of USCIS, ICE and OPS establish a plan for evaluating the eligibility of each naturalized citizen whose fingerprint records reveal deportation orders under a different identity. The plan should include a review of the facts of each case and, if the individual is determined to be ineligible, a recommendation of whether to seek denaturalization through criminal or civil proceedings. The plan should also require documentation and tracking of the decisions made and actions taken on those cases until each has been resolved.

Response: Concur. DHS is taking action to develop and implement a plan for reviewing each of the 858 cases identified in OIG's report (as well as the 953 cases mentioned in footnote 3 of the report).

DHS actions include establishing a review team composed of staff from USCIS—which has primary responsibility for adjudication of naturalization applications—with support from ICE, OPS, and others; including oversight from the Department, as appropriate. The review team will analyze each case to determine whether naturalization was legally proper and whether referral to DOJ for criminal or civil denaturalization proceedings is

warranted[2] The Department understands that OIG did not conduct an in-depth review of each individual case identified in its report. DHS is reviewing both the 858 cases that the draft identifies as not having digitized fingerprint records at the time of adjudication and the 953 cases that the OIG indicates might have lacked such records.

The review team will coordinate with DOJ to ensure consideration of DOJ's standards for bringing civil or criminal proceedings in these cases. In addition, the team will develop procedures to ensure the retention of relevant documentation and will track this process from review initiation to completion. The team will also periodically keep senior Component and Headquarters leadership apprised of its efforts.

As noted in OIG's report, ICE Homeland Security Investigations (HSI) has already initiated a nationwide enforcement operation that identified and prioritized for potential criminal prosecution approximately 120 naturalized citizens with prior criminal or deportation records whose fingerprint records may not have been available at the time of naturalization. ICE HSI continues to work closely with the United States Attorneys Offices (USAO) responsible for the criminal prosecution s of these cases. For any cases where criminal prosecution is declined, USCIS will work with DOJ to determine the appropriateness of civil denaturalization proceedings.

Finally, as the remaining 148,000 records referenced in Recommendation 1 (and any other legacy paper fingerprint records found) are uploaded into IDENT, DHS will use the same process described above to identify and, when appropriate, refer to DOJ any additional cases where the facts and circumstances indicate that naturalization was obtained unlawfully.

The Department understands this recommendation to require DHS to develop and implement a plan for reviewing and evaluating the eligibility for naturalization of those individuals identified in this report. DHS expects to complete its review of these cases by December 31, 2016. The review plan will include referral of cases to DOJ for criminal or civil proceedings including denaturalization proceedings, as appropriate, and such further actions as DOJ determines is warranted.

ECD: September 30, 2017.

[2] Denaturalization may only be ordered by an Article III federal court. Proceedings for denaturalization must be brought by DOJ. DHS only reviews and refers cases to DOJ with a recommended course of action.

Appendix C
Office of Inspections and Evaluations Major Contributors to This Report

John D. Shiffer, Chief Inspector
Deborah Outten-Mills, Chief Inspector
Elizabeth Kingma, Lead Inspector
Jennifer Kim, Senior Inspector
Megan Pardee, Inspector
Joseph Hernandez, Inspector
Kelly Herberger, Communications Analyst
Natalie Fussell Enclade, Independent Referencer

Appendix D
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
Director, U.S. Citizenship and Immigration Services
Director, U.S. Immigration and Customs Enforcement
Director, Office of Operations Coordination
Under Secretary, National Protection and Programs Directorate
Audit Liaison, ICE
Audit Liaison, USCIS
Audit Liaison, OPS
Audit Liaison, NPPD

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

(b)(6)

Case Location: San Fernando Valley Field Office	**Phone #:** [redacted]	**Date Initiated:** 06/05/2013
Email: [redacted]	**Mobile Phone #:** [redacted]	**Event:** Assistance Regarding Alien Arrest
Submitted to ICE, etc. (Date): 06/05/2013	**Region:** Western	**Case/RFA#:** [redacted]
FDNS Officer: [redacted]	**Coordination:** ICE, SFV-FDNS, Adjudications	**Result:** USCIS & ICE Coordination on Operation Janus/TGIS arrests
Ongoing Information: See Below	**Scheme:** Subjects with NS concerns obtained political asylum by using false identities.	**Arrest/Prosecution, etc. (Date):** 06/05/2013 arrest of one of the spouses.

Operation Janus Case Coordination With ICE (SFV-IO):

On June 5, 2013, SFV-FDNS in coordination with Adjudications and ICE scheduled a naturalization interview for one member of a [redacted] married couple. Both parties have National Security concerns and each spouse obtained political asylum by using multiple identities to defraud the United States government. ICE has identified approximately 500 aliens from special interest counties that have obtained political asylum in the United States under similar circumstances and has named this large-scale criminal investigation "Operation Janus".

On 06/05/2013, one of the spouses scheduled for the naturalization interview failed to appear. However, ICE was able to effect the arrest of the other spouse at the address of record provided on the application for United States citizenship.

Results: Both aliens face criminal prosecution by ICE for violating Title 18 USC Section 1546 for Fraud and Misuse of Visas, Permits and Other Entry Documents, Title 18 USC Section 371 for Conspiracy to Commit Offense or Defraud the United States, and Title 18 USC Section 1001 for False Statements.

Privacy Impact Assessment
for the

Fraud Detection and National Security Data System (FDNS-DS)

DHS/USCIS/PIA-013(a)

May 18, 2016

Contact Point
Donald K. Hawkins
Privacy Officer
U.S. Citizenship and Immigration Services
202-272-8000

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
202-343-1717

Abstract

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS), developed the Fraud Detection and National Security Data System (FDNS-DS) as the primary case management system used to record requests and case determinations involving immigration benefit fraud, public safety, and national security concerns. Since its initial deployment, USCIS has incorporated a new screening functionality into FDNS-DS, known as ATLAS, to more effectively identify and review cases involving fraud, public safety, and national security concerns.[1] USCIS is updating and reissuing the entire FDNS-DS Privacy Impact Assessment (PIA), originally published on June 29, 2008, to capture these updates.

Overview

Every year, U.S. Citizenship and Immigration Services (USCIS) receives nearly 6.4 million applications for immigration benefits or service requests. USCIS is committed to ensuring the integrity of the United States (U.S.) immigration system. An integral part of USCIS's delegated authority to adjudicate benefits, petitions, or requests, and to determine if individuals are eligible for benefit or services, is to conduct screenings (*i.e.*, background, identity, and security checks) on forms filed with the agency. USCIS Fraud Detection and National Security Directorate (FDNS) developed the Fraud Detection and National Security – Data System (FDNS-DS) to record, track, and manage the screening processes related to immigration applications, petitions, or requests with suspected or confirmed fraud, public safety, or national security concerns. FDNS also uses FDNS-DS to identify vulnerabilities that may compromise the integrity of the legal immigration system.

The 2014-2018 Department of Homeland Security (DHS) Strategic Plan states that DHS will enforce and administer the nation's immigration laws by "ensuring that only eligible applicants receive immigration benefits through expanded use of biometrics, a strengthening of screening processes, improvements to fraud detection, increases in legal staffing to ensure due process, and enhancements of interagency information sharing."[2] Recent events highlight the importance of screening immigration benefit applicants for fraud, public safety, and national security concerns. Within FDNS-DS, FDNS developed a screening module known as ATLAS. ATLAS's event-based screening capability increases the timeliness and quality of fraud referrals. For the purpose of this PIA, the term FDNS-DS encompasses both the case management system and the screening module, ATLAS.

---

[1] ATLAS is not an acronym.
[2] Department of Homeland Security. "Fiscal Years 2014 – 2018 Strategic Plan."

FDNS-DS receives, tracks, and records information through the following processes: screening, referrals made to FDNS, administrative investigations, and through conducting studies related to benefit fraud and trends[3], as detailed below.

Screening and Referrals to FDNS

The types of screening performed on immigration forms vary by the benefit/request type. In general, USCIS conducts background checks[4] to obtain relevant information in order to render the appropriate adjudicative decision with respect to the benefit or service sought, identity checks to confirm the individual's identity and combat potential fraud, and security checks to identify potential threats to public safety or national security. Standard checks may include:

- Biometric fingerprint-based checks:
    1. Federal Bureau of Investigation (FBI) Fingerprint Check
    2. DHS Automated Biometric Identification System (IDENT) Fingerprint Check[5]
    3. Department of Defense Automated Biometric Identification System (ABIS) Fingerprint Check[6]
- Biographic name-based checks:
    1. FBI Name Check
    2. TECS[7] Name Check

USCIS uses several systems to support the checks identified above, which are described in detail in the Immigration Benefits Background Check Systems[8] and Customer Profile Management Service[9] PIAs, as well as the PIAs associated with USCIS's case management systems. As mentioned in those PIAs, USCIS adjudications staff must query multiple systems, in

[3] *See* DHS/USCIS/PIA-013-01 FDNS Program, *available at* www.dhs.gov/privacy, for more information on the administrative inquiry process, adjudication, and BFA Process. FDNS completes administrative investigations to obtain relevant information needed to render the appropriate adjudicative decision.
[4] During the adjudication process, USCIS conducts four different background checks, two biometric fingerprint-based and two biographic name-based, which are discussed in detail in the Immigration Benefits Background Check Systems (IBBCS) PIA. *See* DHS/USCIS/PIA-033 IBBCS, *available at* www.dhs.gov/privacy.
[5] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[6] For certain benefit types in which the beneficiary has a higher likelihood of having previously been fingerprinted by the U.S. military, USCIS conducts checks against the Department of Defense's Automated Biometric Identification System, as described in the Customer Profile Management System (CPMS) PIA. *See* DHS/USCIS/PIA-060 CPMS, *available at* www.dhs.gov/privacy.
[7] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), *available at* www.dhs.gov/privacy.
[8] *See* DHS/USCIS/PIA-033 IBBCS, *available at* www.dhs.gov/privacy.
[9] *See* DHS/USCIS/PIA-060 CPMS, *available at* www.dhs.gov/privacy.

some cases manually. Through the development of a screening module within FDNS-DS, known as ATLAS, the need to independently query each system is greatly reduced, thereby streamlining the screening process and limiting the privacy risks associated with using multiple systems. ATLAS interfaces with other systems in order to automate system checks and promotes consistent storage, retrieval, and analysis of screening results to enable FDNS to detect and investigate fraud, public safety, and national security concerns more timely and effectively. The specific system interfaces that enable screening through ATLAS are detailed at Appendix A.

Within FDNS-DS, ATLAS's automated, event-based screening is triggered when:

1. An individual presents him or herself to the agency (*e.g.*, when USCIS receives an individual's benefit request form[10] or while capturing an individual's 10-fingerprints at an authorized biometric capture site, for those forms that require fingerprint checks);
2. Derogatory information is associated with the individual in one or more DHS systems; or
3. FDNS performs an administrative investigation.

ATLAS receives information from the individual's form submission and from the biographic and biometric-based checks listed above. That information is screened through a predefined set of rules to determine whether the information provided by the individual or obtained through the required checks presents a potential fraud, public safety, or national security concern. The rules help standardize how information is analyzed and help to detect patterns, trends, and risks that are not easily apparent from the form submissions themselves.

Previously, FDNS-DS received information primarily through manual referrals of cases from USCIS adjudications staff. Since the development of ATLAS, cases can now be referred to FDNS for administrative investigation in the following manners:

Referrals through System Generated Notifications (SGNs)

The screening process described above automates the process of referring cases to FDNS for review. Certain events, such as when USCIS receives a benefit request form or the 10-print capture of an individual's fingerprints at a biometric capture center, trigger rules-based screening. If the benefit request form or biometric capture matches a rule, ATLAS produces an SGN, which is elevated in FDNS-DS for manual review. Once an SGN is produced, a specially trained FDNS Officer, known as a Gatekeeper, conducts a manual review of the SGN for validity, determines whether it is "actionable" or "inactionable," and, if "actionable," triages the SGN for further action. If an SGN is "actionable," it enters the formal FDNS-DS case management process. An SGN found to be "inactionable" may be closed without further action. The SGN itself is not considered derogatory. SGNs help FDNS Officers to detect potential threats earlier in the immigration benefit

[10] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.

application process, to demonstrate the fidelity of the individual's biographic and biometric information, and to identify discrepancies more efficiently.

Fraud Tip Referrals

Members of the public and other government agencies can voluntarily submit a fraud tip to USCIS directly by emailing ReportFraudTips@uscis.dhs.gov. In the future, a static page will be available at www.uscis.gov, where a link to the mailbox will be provided. The webpage lists suggested fields that FDNS has deemed useful when processing the tip. The list serves merely as a suggestion; a fraud or tip reporter can include as much or as little information as he or she wishes. More information about the fraud tip reporting process is described in Appendix H to the FDNS Directorate PIA.[11]

Upon receiving a tip, FDNS evaluates the tip to determine if it is "actionable" or "inactionable" for investigation. If FDNS deems the tip "actionable," FDNS manually inputs the information into FDNS-DS and prepares the tip for an administrative investigation.

Manual Referrals

USCIS adjudications staff can make manual referrals to FDNS through FDNS's Intranet Fraud Referral System (iFRS). Through this process, adjudications staff complete a fillable electronic form using the USCIS SharePoint Enterprise Collaboration Network (ECN).[12] FDNS Officers review the referrals and determine if the referral is "actionable" or "inactionable" and manually enter the information into FDNS-DS. If "actionable," FDNS prepares the referral for administrative investigation.

Administrative Investigations

If FDNS determines an administrative investigation is necessary, FDNS conducts further checks to verify information prior to an adjudicative decision on the immigration benefit or service requested, to include resolving any potential fraud, public safety, or national security concerns. In conducting an administrative investigation,[13] FDNS may perform one, or a combination, of the following:

- Research in Government and commercial databases and public records;
- Internet searches of open source information;
- Searches of publicly available information, including, but not limited to, social media sites;

[11] *See* DHS/USCIS/PIA-013-01 FDNS Directorate, *available at* www.dhs.gov/privacy.
[12] *See* DHS/ALL/PIA-059 Employee Collaboration Tools, *available at* www.dhs.gov/privacy.
[13] *See* DHS/USCIS/PIA-013-01 FDNS Directorate, *available at* www.dhs.gov/privacy, for more information on FDNS administrative investigations.

- File reviews;
- Telephone calls;
- Site visits;
- Interviews of applicants, beneficiaries, petitioners, and others;
- Requests for evidence;
- Administrative subpoenas;
- Requests for assistance from law enforcement agencies;
- Overseas verifications; and
- Referral to law enforcement agencies.

FDNS may perform administrative investigations or work with partner agencies, as appropriate, and ultimately produces findings to sufficiently inform adjudications.

Federated Immigration Screening and Application Report (FISAR)

The Federated Immigration Screening and Application Report (FISAR) within FDNS-DS is an advanced search functionality that allows FDNS-DS users to view the entire screening history on an individual, including records of standard checks, any SGNs produced by ATLAS that relate to the individual, and administrative investigations performed. If there are SGNs in the individual's screening history, the FDNS-DS user can easily determine the status of those SGNs (*e.g.*, pending or triaged). The gatekeeping process described above provides manual oversight to ensure that SGNs produced by the system are valid and that they relate to the individual.

Enhanced Analytical Capabilities

FDNS enhanced ATLAS with analytical capabilities to enable users to more easily query and visualize data within the system and to identify individuals who are filing for immigration and naturalization benefits who may potentially be engaging in fraudulent behavior or pose a risk to public safety or national security. During the screening process, ATLAS analyzes the results of biographic and biometric checks, applies rules, and performs link and forensic analysis and entity resolution among data received from multiple systems. ATLAS assists in confirming individuals' identities when individuals are potentially known by more than one identity by comparing the identity information provided by the individual with identity information in other systems checked against the background, identity, and security check process. As an example, ATLAS can determine if an individual has applied for benefits using multiple biographic identities or aliases. ATLAS also visually displays linkages or relationships among individuals to assist in identifying non-obvious relationships among individuals and organizations with a potential nexus to criminal

or terrorist activities. The results of this analysis may be produced and elevated in FDNS-DS in the form of an SGN or obtained through FISAR.

ATLAS's analytical capabilities do not alter the source data. All legal and policy controls around the source data remain in place.

USCIS is continuing to enhance its screening processes by incorporating seven core capabilities into ATLAS: (1) Predictive Analytics; (2) Link and Forensic Analysis; (3) Unstructured and Structured Analytics; (4) Intelligent Investigative Case Management; (5) Operational Decision Management; (6) Information Sharing and Collaboration; and (7) Entity Analytics. Before new analytical capabilities are deployed within FDNS-DS/ATLAS, the USCIS Office of Privacy will review them to determine additional privacy requirements, which may include updating or re-issuing FDNS PIAs or SORNs.

Types of Information Collected and Stored within FDNS-DS

The following information is collected and stored in FDNS-DS:

- Information collected during screening (*i.e.*, background, identity, and security check processes) to include information provided by the individual on a benefit request form, in response to a request for evidence, or during an interview; derogatory information received in response to checks; and audit trails or logs reflecting the history of checks conducted on the individual;
- Information collected during the adjudicative and administrative investigation process;
- USCIS investigative referrals to law enforcement agencies (LEA) of suspected or confirmed fraud, public safety issues, or national security concerns;
- Referrals and leads from other government agencies and LEAs related to individuals with an immigration history with USCIS;
- Information collected during response to a Request For Information (RFI) from law enforcement and intelligence agencies;
- Referrals from the public or other governmental entities or fraud case referrals from the Benefit Fraud Assessment (BFA) process ("other referrals");
- Information from cases that are selected for study of benefit fraud rates or trends;
- Adverse information identified by USCIS from applications, administrative files, interviews, written requests for evidence (RFE) or site visits; resolution of any of the above-described categories of adverse information; and
- Adjudicative summaries and decisions.

This PIA generally covers the privacy risks and mitigation strategies associated with the FDNS-DS system and its screening (rules-based referrals) and case management capabilities. USCIS will maintain operationally sensitive appendices to this PIA that will analyze privacy risks and mitigation strategies associated with enhanced analytical capabilities that have been approved for use within FDNS-DS.

The privacy risks and mitigation strategies associated with the overall administrative investigation process are described in the FDNS Directorate PIA. Additionally, other published USCIS PIAs available http://www.dhs.gov/privacy cover the benefit request intake process, benefit request form analysis and case management, as well as the collection of biographic and biometric information that is used as part of the screening process. These published PIAs provide an in-depth discussion of these separate processes and evaluate the privacy risks and mitigation strategies built into each process.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The legal authority to collect this information comes from the Immigration and Nationality Act 8 U.S.C. Section 1101 *et seq.* In addition, the Secretary of Homeland Security in Homeland Security Delegation No. 0150.1 delegated the following authorities to USCIS:

> "(H) Authority under section 103(a)(1) of the Immigration and Nationality Act of 1952, as amended (INA), 8 U.S.C. §1103(a)(1), to administer the immigration laws (as defined in section 101(a)(17) of the INA).
>
> Authority to investigate alleged civil and criminal violations of the immigration laws, including but not limited to alleged fraud with respect to applications or determinations within the Customs and Border Protection (CBP) or the CIS and make recommendations for prosecutions, or other appropriate action when deemed advisable."

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

Information collected, maintained, used, and disseminated by FDNS-DS is covered under the following SORNs:

- DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), August 8, 2012 (77 FR 47411)

- Final Rule for Privacy Act Exemptions, August 31, 2009 (74 FR 45084)

- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, September 18, 2017 (82 FR 43556)

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Yes. FDNS-DS was approved for entrance into the DHS Ongoing Authorization Program on August 26, 2014. A system privacy plan is pending the completion of this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. NARA approved the FDNS-DS retention schedule, N1-566-08-18. FDNS will retain the records 15 years from the date of the last interaction between FDNS personnel and the individual for records maintained in FDNS-DS. Records related to an individual's A-File will be transferred to the A-File and maintained under the A-File retention period. USCIS maintains records on individuals and all of their immigration transactions and law enforcement and national security actions (if applicable), in the A-File. A-File records are permanent records in both electronic and paper form. USCIS transfers A-Files to the custody of NARA 100 years after the individual's date of birth, in accordance with N1-566-08-011.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Almost all of the information within FDNS-DS is originally submitted on a benefit request form that is subject to the PRA. However, there are no forms associated specifically with the collection of information in FDNS-DS. Please see the benefit request PIAs and Appendices for a comprehensive list of the various forms that cover the initial collection of information from the individual.[14]

[14] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Due to the nature of the information within FDNS-DS, FDNS-DS contains sensitive personally identifiable information (SPII). Depending upon the category of information being collected in or attached to an FDNS-DS record, the system may collect the following SPII:

Information about individuals may include, if applicable:

- Full name;
- Alias(es);
- Physical and Mailing Addresses;
- Alien Number (A-Number);
- USCIS Online Account Number;
- Social Security number (SSN);
- Date of birth;
- Nationality;
- Country of citizenship;
- Place of birth;
- Gender;
- Marital status;
- Military status;
- Phone numbers;
- Email address;
- Immigration status;
- Government-issued Identification (*e.g.*, passport, driver's license):
    - Document Type;
    - Issuing Organization;

  - Document Number; and
  - Expiration Date.

- Signature;
- Other Unique Identifying Numbers (*e.g.*, Department of State (DOS)-issued Personal Identification Number, ICE Student and Exchange Visitor Number, USCIS E-Verify Company Identification Number);
- Arrival/Departure information;
- Immigration history (*e.g.*, citizenship/naturalization certificate number, removals, explanations);
- Family relationships (*e.g.*, parent, spouse, sibling, child, other dependents) and Relationship Practices (*e.g.*, polygamy, custody, guardianship);
- USCIS Receipt/Case Number;
- Personal background information (*e.g.*, involvement with national security threats, criminal offenses, Communist party, torture, genocide, killing, injuring, forced sexual contact, limiting or denying others religious beliefs, service in military or other armed groups, work in penal or detention systems, weapons distribution, combat training);
- Medical information;
- Travel history;
- Education history;
- Work information (contact information, position and relationship to an Organization, degree(s), membership(s), accreditation(s), license(s) identification numbers);
- Work history;
- Bank account or financial transaction history;
- Supporting documentation as necessary (*e.g.*, birth, marriage, or divorce certificates, licenses, academic diplomas, academic transcripts, appeals or motions to reopen or reconsider decisions, explanatory statements, criminal history documents, and unsolicited information submitted voluntarily by the applicants or family members in support of a benefit request);
- Physical description (*e.g.*, height, weight, eye color, hair color, race, ethnicity, identifying marks like tattoos or birthmarks);
- Photographs from Government-issued Identification (*i.e.*, passport, Driver's license, and

other identification card);

- Relationships to petitioners, representative, preparers, family members, and applicants;
- Case processing information such as date applications were filed or received by USCIS, application/petition status, location of record, other control number when applicable, and fee receipt data;
- Organizations associated with applications, petitions or other requests (Place of business or place of worship, if place of worship is sponsoring the individual);
- Civil or criminal history information;
- Uniform resource locators (URLs)[15] or Internet protocol addresses;
- Biometric identifiers or associated biographic information (*e.g.*, photographic facial image, fingerprints, Fingerprint Identification Number (FIN), Encounter Identification Number (EID), and signature);
- TECS, National Crime Information Center (NCIC), Federal Bureau of Investigation (FBI) Terrorist Screening Database, and any other data and analysis resulting from the investigation or routine background identity and security checks performed in support of the adjudication process; or
- Any other unique, identifying information.

2.2 What are the sources of the information and how is the information collected for the project?

Information in FDNS-DS is collected during the following processes: the screening (*i.e.*, background, identity, and security check) process, referrals made to FDNS, administrative investigations, and to conduct studies related to benefit fraud and trends.[16] Much of the information collected in the FDNS-DS is taken from the benefit request form submitted to USCIS by the individual or an authorized representative or preparer, or from systems against which that data is screened during the screening process. USCIS may also collect information through interviews and site visits and record this into FDNS-DS. Interviewees may include current/past employers, family members, applicants, or other authorized representatives or preparers.

The information can be collected automatically or manually, as described below.

---

[15] The URL is the unique address for a file that is accessible on the Internet.

[16] *See* DHS/USCIS/PIA-013-01 FDNS Program, *available at* www.dhs.gov/privacy, for more information on the administrative inquiry process, adjudication, and BFA Process. FDNS completes administrative investigations to obtain relevant information needed to render the appropriate adjudicative decision.

Automatic Collection

FDNS-DS's event-based screening capability through ATLAS is an automatic collection process that records certain information for review. Screening within ATLAS is triggered when:

1. An individual presents himself/herself to the agency;
2. Derogatory information is associated with the individual in one or more DHS systems; or
3. Administrative investigations are performed.

ATLAS queries internal and external systems automatically to obtain data relating to an individual's background, identity, and security check. ATLAS receives biographic data (*e.g.*, name, date of birth, alias) associated with the individual's benefit request form from USCIS case management systems or biographic data associated with the individual's biometric capture at an approved biometric collection site (*e.g.*, FIN, A-Number), which may be screened against data in IDENT,[17] TECS,[18] or the Terrorist Screening Database[19] and then against FDNS-DS's rules engine and analytical tools to produce SGNs.

In addition to the automatic collection that occurs during the screening process, FDNS-DS has a direct connection to the Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)[20] to obtain CLAIMS[21] information about benefit request forms, applications, or petitions that can be used to automate the population of case information within FDNS-DS, such as A-Number. This helps to reduce the risk of error from manual data entry and to preserve the integrity of the information found in source systems.

A comprehensive listing of source systems for this automatic collection is routinely updated at Appendix A.

Manual Collection

FDNS-DS users may query several DHS databases or systems to obtain information. Information gathered from these systems (*e.g.*, dates of birth, SSN, country of birth, address) may

[17] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[18] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing (TECS), *available at* www.dhs.gov/privacy.
[19] *See* DHS/ALL/PIA-027 DHS Watchlist Service, *available at* www.dhs.gov/privacy.
[20] *See* DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigrations Services Centralized Operational Repository (eCISCOR), *available at* www.dhs.gov/privacy.
[21] *See* DHS/USCIS/PIA-016(a) CLAIMS 3, *available at* www.dhs.gov/privacy.

be added to FDNS-DS. A complete list of DHS systems researched during this process is also included in Appendix A to this PIA.

Federal, State, and Local Government Sources

FDNS Officers may obtain information from various external sources, such as:

- Department of Labor;
- Department of State (DOS);
- Social Security Administration (SSA) Electronic Verification of Vital Events (EVVE) [22];
- Federal Aviation Administration websites;
- Intelligence and law enforcement communities;
- State and local government agencies;
- Local, county, and state police information networks;
- State motor vehicle administration databases and websites;
- Driver license retrieval websites;
- State bar associations;
- State comptrollers;
- State probation/parole boards or offices;
- County appraisal districts; and
- State sexual predator websites.

As described in the FDNS Directorate PIA, FDNS receives information from external partners or sources during the administrative inquiry process and as part of referrals, requests for assistance, or requests for information. The type of information collected depends on the specific context of a given case within FDNS-DS.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

FDNS collects information throughout the course of recording, tracking, and managing the screening and administrative investigation processes related to immigration benefit requests forms,

[22] EVVE system allows verification of vital record information from the states, including birth certificates. *See* Electronic Verification of Vital Events Program Operations Manual System, *available at* https://secure.ssa.gov/poms.nsf, for more information.

applications, or petitions. FDNS may obtain information from commercial sources or from publicly available information on the Internet. Examples of commercial or publicly available sources FDNS may access include, but are not limited to:

- Commercial data brokers (*e.g.*, Choicepoint AutoTrackXP, Lexis/Nexis Accurint, Thomson Reuters CLEAR)
- General legal research sites (*e.g.*, Legal Information Institute)
- Internet sites such as university websites and newspapers, news media websites, United Press International, Reuters, and foreign news media websites
- Various search engines (*e.g.*, Ask, Google, Yahoo, REFDESK)
- Social media websites (*e.g.*, Facebook, Twitter, LinkedIn, Pinterest, Google+)[23]

FDNS-DS enables Officers to note the exact URL and include attachments of any information collected from commercial sources or publicly available information.

FDNS uses these various commercial and publicly available sources to verify information provided by the individual, support or refute indications of fraudulent behavior, and identify any threat to public safety or nexus to known or suspected terrorists in the processing of their benefit request, consistent with authority granted by the Immigration and Nationality Act.[24] In addition, the Secretary has delegated USCIS the authority to investigate alleged civil and criminal violations of the immigration laws, not limited to alleged fraud with respect to applications or determinations.[25]

Compiling this information and taking action to prevent potentially malfeasant and sometimes dangerous people from staying in this country supports DHS's mission of preventing terrorist attacks within the United States and reducing America's vulnerability to terrorism, while facilitating the adjudication of lawful benefit applications.

2.4 Discuss how accuracy of the data is ensured.

FDNS-DS relies on the accuracy of the information as it is collected from the source. As such, the accuracy of the information in FDNS-DS is equivalent to the accuracy of the source information at the point in time when it is collected into FDNS-DS. During this process, FDNS conducts data validation to ensure accuracy of the data.

---

[23] FDNS Officers who seek to access, process, store, receive, or transmit PII obtained through the Operational Use of Social Media while conducting investigations are required to complete a "Rules of Behavior (ROB) for the Operational Use of Social Media." These ROBs ensure that users are accountable for their actions on social media, are properly trained, and aware of the authorized use of social media sites.

[24] 8 U.S.C. 1101 et seq.

[25] *See* Secretary of Homeland Security Delegation No. 0150.1, Section II (H) and (I), for more information.

FDNS Officers compare information obtained during the screening and administrative investigation processes with information provided directly by the individual (applicant or petitioner) in the underlying benefit request form or in response to Requests for Evidence or Notices to Appear, to ensure information is matched to the correct individual, as well as to ensure integrity of the data. As described above, the information contained in benefit request forms, applications, or petitions may be matched against public records, commercial data aggregators, and public source information, such as web sites or social media, to validate the veracity of information provided by the individual.

FDNS uses public source information only as means to verify information already on file with USCIS or identify possible inconsistencies. Due to the inherent data accuracy risks of relying on information from the Internet, USCIS requires that no benefit determination action can be taken based solely on information received from a public source. The information obtained from a public source must be corroborated with authoritative information on file with USCIS.

In the event FDNS Officers learn that information contained within other systems of records is not accurate, the Officer will notify appropriate individuals within the USCIS Records Office or the federal agency owning the data, who will facilitate any necessary notifications and changes.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk to individual participation because FDNS Officers rely on a considerable amount of information collected from external sources beyond what individual submitted on his or her benefit request form.

Mitigation: This risk is partially mitigated. FDNS collects information from a variety of sources to verify the information provided by individuals in the course of a review of possible fraud, public safety, and national security concerns. FDNS has determined that in order to have the best evidence available to support the adjudication process, it is necessary to collect large amounts of sensitive PII. This information is required to ensure that FDNS makes the correct determination about the correct individual regarding cases of fraud, criminal activity, public safety, and national security concerns and sufficiently informs the adjudication of the benefit application. This risk is also partially mitigated in that individuals have the opportunity to provide information directly to USCIS throughout the adjudication process and through interviews, Requests for Evidence, or Notices to Appear.

Privacy Risk: Due to FDNS's reliance on external sources, including commercial sources, public sources, or social media, there is a risk that USCIS will obtain and rely upon inaccurate data.

Mitigation: The risk is partially mitigated in that FDNS considers information derived from sources other than the individual, but also exercises caution about the information's accuracy. Due to its inherent lack of data integrity, public source information is not used as the sole basis upon which to adjudicate an immigration benefit or request, investigate benefit fraud, or identify public safety and national security concerns. FDNS compares historical, biographical, financial, and personal information presented by the individual against third-party sources, whenever possible.

In order to improve the accuracy of the information, USCIS has developed policies and procedures for safeguarding data aggregated within FDNS from several different sources. This includes using public record data, data from commercial data providers, as well as other publicly available data including social media and news and reviewing existing data in USCIS's files with information outside of USCIS. If inaccurate information is found during the process of reviewing a file, FDNS will contact personnel within the USCIS Records Division who are authorized to make the changes to the data in the source system. FDNS will also correct inaccuracies in FDNS-DS and other locations where FDNS records are maintained.

Privacy Risk: Because FDNS-DS aggregates information from multiple source systems, there is a risk of data inaccuracy if the data in the underlying system(s) change.

Mitigation: As noted above, FDNS has policies and procedures in place to confirm the veracity of the data being relied upon in resolving potential fraud, public safety, and national security concerns. FDNS-DS also queries other systems in real time to receive the most timely and accurate data available from the source system. Finally, individuals have opportunities to provide information directly through the adjudicative process.

Privacy Risk: In some cases, FDNS-DS users enter information into the system manually. There is a risk of human error, which could result in FDNS relying on inaccurate data.

Mitigation: FDNS has a vested interest and responsibility to maintain the most accurate data possible since the information could be used in support of an adjudicative decision or in support of criminal investigations undertaken by law enforcement partners. FDNS Officers rely on multiple sources to confirm the veracity of the data and, if discrepancies are uncovered, will take necessary steps to correct inaccuracies.

Privacy Risk: There is a risk that search functions that previously could only have been performed through separate searches of individual systems or databases will allow FDNS-DS users (or users of other case management systems that receive data from FDNS-DS) to access to more data than is necessary to perform their specific roles.

Mitigation: This risk is mitigated in that FDNS-DS maintains strict access controls so that only FDNS-DS users with a role in investigating cases for potential fraud, public safety, and national security concerns have access to raw data retrieved as part of the screening process.

FDNS-DS interfaces with other systems to help streamline the processes that FDNS-DS users currently perform manually, and its capabilities are designed to assist officers in obtaining information needed to confirm an individual's eligibility for the benefit or request sought while preserving the integrity of the legal immigration system. The output to other case management systems is reasonably tailored to provide adjudications staff with information relevant to making a determination on the benefit or request sought.

Privacy Risk: There is a risk of obtaining data from new sources that have not been reviewed for privacy and legal concerns in determining possible benefit fraud, criminal activity, public safety, and national security concerns.

Mitigation: The risk is partially mitigated. In order to reduce the risk of new data being incorporated into FDNS that has not been reviewed for privacy and legal concerns, multiple layers of privacy and legal review have been built into FDNS's processes. The process is memorialized via the Overarching Integrated Project Team (IPT) Charter, which is in the approval process. Additionally, new sources are reviewed through the FDNS weekly Screening and Case Management IPTs with participation from the FDNS Privacy Advisor and USCIS Office of Privacy. FDNS must submit a privacy threshold analysis and receive approval from the DHS Privacy Office before adding any new data sources.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

FDNS-DS records, tracks, and manages the screening process, thereby increasing the effectiveness of the U.S. immigration system in combating benefit fraud, protecting public safety, identifying potential threats to national security, and identifying vulnerabilities that may compromise the integrity of the legal immigration system.

Screening

FDNS uses FDNS-DS to manage the screening (*i.e.*, background, identity, and security check) process in support of the adjudication of USCIS benefit requests, in a pre-decisional and deliberative process. The information can be collected as a part of an automatic collection or manual collection, as described in Section 2.2.

FDNS uses commercial and publicly available sources, as well as information from other federal, state, and local government sources, to verify information provided by the individual/applicant or his/her petitioner or representative, support or refute indications of fraudulent behavior, and identify any public safety concerns or nexus to known or suspected

terrorists in the processing of the individual/applicant's benefit request, pursuant to the Immigration and Nationality Act.[26]

Case Management

FDNS-DS performs case management by recording, tracking, and managing the processes associated with detecting fraud, egregious or non-egregious public safety, and national security concerns. FDNS-DS is the central repository for all data gathered during the processes of performing screening on benefit request forms or applications received, performing administrative investigations, and conducting studies of benefit fraud rates and trends.

Studies Related to Benefit Fraud and Trends

FDNS uses FDNS-DS data to produce studies related to benefit fraud and trends.[27] Identification of fraud patterns and trends support operational decision management and inform future rules-based referrals.[28]

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Yes. FDNS is incorporating predictive analytics into FDNS-DS to assist in prioritizing the workload. Predictive technology is applied to known derogatory holdings (*e.g.*, background check results) in order to categorize information so that the cases most likely to result in a referral for criminal action are prioritized for the most immediate review. All cases, regardless of their priority, are reviewed manually by FDNS Officers.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes. FDNS-DS information is accessed by or shared with employees or contractors of DHS components on a need-to-know basis. Limited U.S. Immigration and Customs Enforcement (ICE) and CBP personnel have been granted read-only access to FDNS-DS. Information sharing includes tracking interactions with ICE to determine if further law enforcement activities should be pursued. ICE and CBP must request USCIS permission to share USCIS data with external third parties.

---

[26] 8 U.S.C. Section 1101 *et seq.*

[27] *See* DHS/USCIS/PIA-013-01 FDNS Program, *available at* www.dhs.gov/privacy, for more information on the administrative inquiry process, adjudication, and BFA Process. FDNS completes administrative investigations to obtain relevant information needed to render the appropriate adjudicative decision.

[28] *See* DHS/USCIS/PIA-055 SAS Predictive Modeling Environment, *available at* www.dhs.gov/privacy.

At the time of publication of this PIA, FDNS is also working with ICE to establish a connection to improve the quality and exchange of information with ICE, consistent with the joint USCIS/ICE anti-fraud strategy discussed in the FDNS Directorate PIA. Through this connection, FDNS-DS will share information with ICE on cases that may involve egregious public safety concerns or require further criminal investigation.

Furthermore, at the request of DHS, RFIs for national security purposes from external entities are coordinated through DHS Office of Intelligence and Analysis (I&A) Single Point of Service (SPS).[29]

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that information contained within the FDNS-DS system is not used consistently with its original purpose and authority or that individuals may use the data inappropriately.

Mitigation: Consistent with FDNS's mission of detecting, deterring, and combating immigration benefit fraud, all information contained within FDNS-DS is used to identify and track possible benefit fraud, public safety, and national security concerns. These uses are consistent with the notice provided to individuals in the Privacy Act Statements on all USCIS forms, as well as this PIA and the corresponding SORN.

Consistent with USCIS and FDNS governance, user permissions are managed in a stringent manner to ensure users are only granted the privileges and access necessary to perform their job. User roles within the application will also be managed in a manner that is reflective of the need for more restrictive access. Training of users will also incorporate the appropriate use and access of data.

External users (*i.e.*, CBP and ICE users) are granted read-only access to FDNS-DS only. USCIS shares FDNS-DS data with ICE, and in some cases with CBP, to determine if further law enforcement activities should be pursued. ICE and CBP must request USCIS permission to share USCIS data with external third parties. This ensures sharing is consistent with the routine uses allowable in the FDNS SORN.

Privacy Risk: There is a risk that SGNs may present FDNS Officers with results that may contain too many false positives, which may render the resulting data unusable or unreliable or unfairly subject individuals to further scrutiny.

[29] *See* DHS/ALL/PIA-044 DHS Single Point of Service Request for Information Management Tool, *available at* www.dhs.gov/privacy.

Mitigation: An onboarding phase allows for a period of refining rules before they are deployed across FDNS. This onboarding phase consists of FDNS-DS users in a limited rollout receiving rule alerts through e-mail notifications.

USCIS continually tunes the rules to narrow the scope of information provided to FDNS Officers. Rigorous quality control and assurance procedures are used to adjust rules as necessary to reduce the potential for false positives. FDNS continually monitors and refines rules based on appropriate metrics. The SGN process also provides for a layer of human review to confirm SGNs are actionable prior to routing them for further case management activity.

Privacy Risk: There is a risk of an inappropriate assumption that all individuals listed within FDNS-DS have engaged in fraudulent immigration-related practices or pose a public safety or national security risk.

Mitigation: Individuals that are listed within FDNS-DS have potentially engaged in activities that require further review for potential fraud, criminal activity, public safety, and national security concerns. However, the existence of a record in FDNS-DS is not in itself considered derogatory or a reflection on the individual's eligibility for a benefit, request, or service. In determinations when potential was not realized, cases are marked with "no fraud found." Statements of Findings (SOF) or assessments will contain a summary for adjudication's use.

Privacy Risk: For certain benefits or service requests, FDNS must share the results of background, identity, and security checks or other forms of screening with other USCIS case management systems in order to provide information in support of adjudications. There is a risk that data will be inaccurately copied or that it may be taken out of context.

Mitigation: The risk is partially mitigated in that FDNS-DS, as a standard practice with A-File handling, allows the ability to copy a non-changing SOF for adjudications. A SOF is an unchangeable, PDF document in FDNS-DS. In response to manual referrals made to FDNS-DS, FDNS users will complete a SOF or assessment, when required. The SOFs or assessments are shared with adjudications staff. Adjudications staff are trained on how to interpret information in the SOFs or assessments and their relevance in adjudicating immigration benefits and also coordinate closely with FDNS.

In future releases, FDNS-DS will interface with USCIS immigration case management systems to fully automate the screening process, as well as provide the background, identity, and security check results either in the form of a hit/no hit response, a summary of past screening history, or some usable form, in order to provide timely, meaningful information to adjudicative staff. The responses sent to the case management systems will be tailored to present adjudication officers with information relevant to determining the individual's eligibility for the immigration benefit or service sought.

Privacy Risk: With automating the screening process, there is a risk of recurrent screening or vetting of individuals beyond the original purpose.

Mitigation: USCIS has established a robust governance structure to ensure that screening rules are compliant with all legal and privacy requirements. New rules undergo several layers of operational, legal, privacy, and policy review before they are presented to the Deputy Director, USCIS, for final approval. Through this process, FDNS ensures that all screening activity is properly vetted and falls within USCIS's authority. All screening methods deployed are tailored to provide information that is relevant to the adjudication of a particular benefit or immigration service request. USCIS may conduct screening in situations in which USCIS has the authority to rescind, revoke, or otherwise terminate, to issue a Notice to Appear (NTA), or to refer to another government agency for criminal/civil actions. When USCIS may no longer take action on a benefit, service, or request, the screening will cease.

Privacy Risk: There is a risk that FDNS-DS users will create ATLAS rules without going through the appropriate rules review process.

Mitigation: The governance process ensures that new rules are not created or implemented within the system without review from the appropriate stakeholders, including privacy and legal review. Implementation of rules and generation of SGNs are required to be in compliance with the Privacy Act of 1974, E-Government Act of 2002, Homeland Security Act of 2002 and all DHS privacy policies. Additionally, the capture, use, and disclosure of PII through the rules process must be pursuant to applicable system of record notices and available routine uses.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

In addition to the publication of this PIA, USCIS has previously published a programmatic PIA and SORN for the FDNS Directorate. FDNS-DS collects information from other USCIS systems, which also have their own PIAs and SORNs published on the DHS website.

All applications for benefits from USCIS have a Privacy Act Statement providing notice to the individual regarding the use and collection of the information and these forms state the that information may be used for fraud detection. USCIS forms also notify the individual that

information provided may be checked for completeness, that certain background checks may be conducted, or that USCIS may request an interview or further evidence.[30]

When FDNS conducts interviews and site visits, FDNS Officers identify themselves and notify the individual or beneficiary of the reason for the interview or site visit. Notice is given to an individual's attorney when an administrative site visit or interview will occur, unless notice would jeopardize the site visit or interview.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

USCIS benefit request forms require that an individual provide specific information that may contain sensitive PII. The failure to submit such information could impact the processing or adjudication of an application or petition and thus preclude the individual from receiving the benefit, request, or service. Therefore, through the application process, individuals have consented to the use of the information supplied in the benefit request form or application to determine their eligibility for the benefit, request, or service sought. Further, fraud assessments and background, identity, and security checks are required by regulation on all requests/applications filed with USCIS. Benefits, requests, or services cannot be granted until those checks are complete, and the information submitted is essential to the conduct of those checks.[31]

USCIS provides notice to all individuals at the time of collection through a Privacy Act Statement on all USCIS forms. Individuals are notified at the point of data collection (generally in the form itself) of the right to decline to provide the required information; however, such action may result in the denial of the individual's request.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk to notice that benefit requestors will not know that FDNS will collect publicly available information about them, including information posted on public social media websites and platforms.

Mitigation: The risk has been mitigated to the extent possible because USCIS provides notice to individuals through an (e)(3) statement, the source system PIAs, the FDNS Directorate PIA, this PIA, and the associated SORNs. USCIS also provides notice of its fraud detection and national security work through its public website.[32]

---

[30] Adjudicators are responsible for making decisions regarding granting benefits.
[31] As required by Title 8 U.S.C. § 1101 et seq.
[32] *See* https://www.uscis.gov/about-us/directorates-and-program-offices/fraud-detection-and-national-security/fraud-detection-and-national-security-directorate.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

USCIS retains application information to assist in identifying individuals who threaten national security and public safety; detecting, pursuing, and deterring immigration benefit fraud; and identifying and removing systemic vulnerabilities in the process of the legal immigration system.

USCIS retains FDNS-DS records for 15 years from the date of the last interaction between FDNS personnel and the individual, no matter the determination. Records related to a person's A-File will be transferred to the A-File and maintained under the A-File retention period (N1-566-08-11). Upon closure of a case pertaining to an individual, any information that is pertinent to the adjudicative decision (such as a SOF), whether there was or was not an indication of fraud, criminal activity, public safety and national security concerns, is transferred to the associated A-File.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that data will be retained longer than necessary. This would increase the risk of unauthorized access, use, and loss of the data.

Mitigation: FDNS mitigates this risk by destroying FDNS-DS data in accordance with approved NARA records retention schedules. The 15-year retention schedule for FDNS data (N1-566-08-18) provides access to information that can be critical to research related to suspected or confirmed fraud, public safety, and national security concerns for individuals who may still be receiving immigration benefits or services. In addition, should the individual apply for another benefit, retention of the information can eliminate the need for research on concerns that were previously addressed.

Privacy Risk: There is a risk that data will be retained in FDNS-DS longer than allowed by the original source system.

Mitigation: This risk is mitigated in that FDNS-DS retains data relevant to the background check/screening process and to cases of suspected or confirmed fraud, criminal activity, public safety and national security concerns. The system's master 15-year retention period is shorter than that of many USCIS case management systems from which application data is derived.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state, and local government; and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

FDNS shares information outside of DHS when USCIS receives an RFI, when it proactively discloses based on information in the record, and when asking an outside organization for additional information related to an individual. RFIs may be received from federal law enforcement agencies (*e.g.*, Department of Justice (DOJ) FBI, DOS), the Intelligence Community, and authorized state or local law enforcement agencies who are parties to information sharing agreements managed by DHS. USCIS provides access to the requested data through direct user accounts or through copying of data to an electronic device or medium.

Requests for information are governed by the DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) System of Records[33], the DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records[34], or in some instances, the originating system of records notice for the underlying USCIS records, *e.g.*, DHS/USCIS-007 Benefits Information System (BIS).[35] When covered by an applicable routine use and when appropriate, USCIS may share the sensitive PII listed in Section 2.1 of this PIA with federal, state, tribal, local, international, or foreign law enforcement and intelligence agencies, in response to an RFI in support of criminal and administrative investigations, and background identity and security checks involving immigrant benefit fraud, criminal activity, public safety, and national security concerns.

Through direct user account access, DOS Bureau of Consular Affairs may view a comprehensive picture of a visa applicant's status and to reduce the likelihood that an individual or group might fraudulently obtain an immigration benefit under the INA, as amended. DOS has read-only access to FDNS-DS.

Proactive disclosure based on information in the system occurs when FDNS has an indication of possible fraud, criminal activity, public safety, and national security concerns. In these cases, FDNS may proactively share information with other government entities as described

---

[33] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (Aug. 8, 2012).
[34] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[35] DHS/USCIS-007 Benefits Information System 81 FR 72069 (Oct. 19, 2016).

under the FDNS and A-File SORNs.[36]

RFIs for national security purposes from external entities are coordinated through DHS I&A SPS. USCIS responses are provided via government secure networks. All other requests are processed by USCIS. Responses provided by field offices are also provided via secure methods.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Direct account access by DOS Bureau of Consular Affairs is covered by FDNS SORN routine use I and A-File SORN routine use O, which permits USCIS to share PII with DOS Bureau of Consular Affairs in the processing of applications for benefits. This is compatible with the original collection under the INA, which requires USCIS to administer immigration laws. Information may also be shared with DOS Bureau of Consular Affairs to provide a comprehensive picture of a visa applicant's status, and to reduce the likelihood that an individual or group might fraudulently obtain an immigration benefit under the INA, as amended.

Proactive disclosures are covered by the FDNS SORN, routine use H, which permits FDNS to share PII with federal and foreign government intelligence or counterterrorism agencies when USCIS reasonably believes there is a threat or potential threat to national or international security.

Proactive disclosures are also covered by routine use H and II of A-File SORN. Routine use H permits USCIS to share A-File information with appropriate federal, state, tribal, local, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, when DHS believes the information would assist in enforcing applicable civil or criminal laws. A-File SORN routine use II permits sharing with a federal, state, local, territorial, tribal, international, or foreign criminal, civil, or regulatory law enforcement authority when the information is necessary for collaboration, coordination, and de-confliction of investigative matters, prosecutions, or other law enforcement actions to avoid duplicative or disruptive efforts and to ensure the safety of law enforcement officers who may be working on related law enforcement matters.

---

[36] *See* DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (August 8, 2012).

These disclosures are compatible with the original collection because the INA requires USCIS to investigate alleged civil and criminal violations of immigration laws, including alleged fraud with respect to applications or determinations within USCIS. In addition, the INA provides for terrorist-related bars that may serve as the basis for denial of a requested benefit. The INA also requires USCIS to make recommendations for prosecutions or other appropriate actions when deemed advisable.

6.3 Does the project place limitations on re-dissemination?

Yes. A Memorandum of Agreement (MOA) between USCIS and DOS Bureau of Consular Affairs fully outlines responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination. Methods and controls over dissemination of information are coordinated between USCIS and DOS Bureau of Consular Affairs prior to information sharing. Depending on the context of other sharing, DHS may place additional controls on the re-dissemination of the information. FDNS also shares data internally via secure government networks.

A Memorandum of Understanding (MOU) between DHS and the FBI Terrorist Screening Center (TSC) for real-time screening against TSDB records also fully outlines responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination.

A MOA between DHS and the National Counter Terrorism Center also fully outlines responsibilities of the parties, security standards, and limits of use of the information, including re-dissemination in accordance with the United States Attorney General Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information (March 22, 2012).

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

FDNS maintains a record of disclosure of FDNS-DS information provided outside of the Department in FDNS-DS. A record is kept on file of each disclosure, and system audit trail logs are maintained to identify transactions performed by both internal and external users.

As mentioned in the FDNS Directorate PIA, FDNS may receive requests for assistance from external law enforcement partners. These requests are evaluated on a case-by-case basis, and disclosures must abide by all privacy laws and legal requirements. Some FDNS Officers are detailed to partner agencies to provide assistance as immigration subject matter experts. All FDNS Officers must abide by all privacy laws and legal requirements before sharing any immigration information. Disclosures made pursuant to these requests for assistance are tracked in FDNS-DS.

Further, at the request of DHS, Requests for Information for national security purposes from external entities are coordinated and tracked through the DHS I&A SPS process.[37]

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk of misuse, unauthorized access to, or disclosure of, information.

Mitigation: As discussed above, FDNS maintains a record of each disclosure of FDNS information made to every agency in accordance with a routine use and with whom it has an information sharing agreement. Otherwise, FDNS does not share its information. A record is kept on file of each disclosure, including the date the disclosure was made, the agency to which the information was provided, the purpose of the disclosure, and a description of the data provided.

The electronic sharing of data with external agencies is conducted over government secure networks. All personnel within the receiving agency and its components are trained on the appropriate use and safeguarding of data. In addition, each external agency with whom the information is shared has policies and procedures in place to ensure there is no unauthorized dissemination of the information provided by FDNS. Any disclosure must be compatible with the purpose for which the information was originally collected and only authorized users with a need to know may have access to the information contained in FDNS-DS.

DHS information is covered by the third-party discovery rule, which precludes agencies outside of DHS that have received the information from DHS from sharing with additional partners without the consent of DHS.

Risks are further mitigated by provisions set forth in MOAs or MOUs with federal and foreign government agencies. Finally, United States government employees and contractors must undergo annual privacy and security awareness training.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

Because FDNS-DS contains sensitive PII related to possible immigration benefit fraud and

[37] *See* DHS/ALL/PIA-044 DHS Single Point of Service Request for Information Management Tool, *available at* www.dhs.gov/privacy.

national security concerns, DHS has exempted FDNS from the notification, access, and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. § 552a(k)(2). Notwithstanding the applicable exemptions, USCIS reviews all such requests on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the U.S. or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of USCIS, and in accordance with procedures and points of contact published in the applicable SORNs.

Individuals seeking to access information maintained by FDNS should direct their requests to:

National Records Center
Freedom of Information Act/Privacy Act Program
P. O. Box 648010
Lee's Summit, MO 64064-8010

Requests for access to records must be in writing. Such requests may be submitted by mail or in person. If a request for access is made by mail, the envelope and letter must be clearly marked "Privacy Act Request" to ensure proper and expeditious processing. The requester should provide his or her full name, date and place of birth, and verification of identity in accordance with DHS regulations governing Privacy Act requests (found at 6 CFR Part 5.21), and any other identifying information that may be of assistance in locating the record.

The information requested may, however, be exempt from disclosure under the Privacy Act because FDNS records, with respect to an individual, may sometimes contain law enforcement sensitive information. The release of law enforcement sensitive information could possibly compromise ongoing criminal investigations.

Additional information about Privacy Act and Freedom of Information Act (FOIA) requests for USCIS records can be found at http://www.uscis.gov.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

As stated above, individuals may use the Freedom of Information Act/Privacy Act process to request access to and correction of records maintained about them. The data accessed by FDNS-DS from underlying USCIS source systems may be corrected by means of the processes described in the PIAs and SORNs for those systems. In the event inaccuracies are noted, files and FDNS-DS records may be updated.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals are notified of the procedures for correcting their information on USCIS forms, the USCIS website, and by USCIS personnel who interact with individuals in the course of processing requests for benefits or services. Furthermore, this PIA and the respective SORNs serve as notice to individuals.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may be able to access, correct, or make amendments to records in the source systems, but may not be able to do so for their records maintained in FDNS-DS due to the Privacy Act exemptions claimed.

Mitigation: While FDNS maintains pre-decisional, deliberative information in FDNS-DS, individuals may still request access to records that USCIS maintains about them. Notice on how to file a Privacy Act request about records contained in maintained by FDNS is provided by this PIA and the FDNS SORN. Individuals can request access to information about them through the Privacy Act and FOIA process, and may also request that their information be amended by contacting the National Records Center. The nature of FDNS-DS and the data it collects, processes, and stores is such that it limits the ability of individuals to access or correct their information. Each request for access or correction is individually evaluated.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Access and security controls have been established to mitigate privacy risks associated with authorized and unauthorized uses, specifically misuse and inappropriate dissemination of data. Access to FDNS-DS is generally read-only. Some FDNS-DS users have "read," "write," and "modify" privileges. All account access and privileges are approved by the USCIS business owner. When employment at USCIS is terminated or an employee's responsibilities no longer require access to FDNS-DS, access privileges are removed.

Audit trails are kept in order to track and identify unauthorized uses of FDNS-DS information. The audit trails include the ability to identify specific records each user accesses. A warning banner is provided at all access points to inform users of the consequences associated with

unauthorized use of information. The banner warns authorized and unauthorized users about the appropriate uses of the system, that the system may be monitored for improper use and illicit activity, and the penalties for inappropriate usage and non-compliance. A user must click on the agreement to proceed with login.

In addition, user access to FDNS-DS is limited to personnel who need the information to perform their job functions. Only users with proper permissions, roles, and security attributes are authorized to access the system. Each user is obligated to sign and adhere to a user access agreement, which outlines the appropriate rules of behavior tailored for FDNS-DS. The system administrator is responsible for granting the appropriate level of access. Finally, all employees are trained on the use of information in accordance with DHS policies, procedures, regulations, and guidance.

FDNS conducts continuous security assessments of FDNS-DS in accordance with FISMA requirements. Furthermore, FDNS-DS complies with the DHS 4300A security guidelines, which provide hardening criteria for securing networks, computers, and computer services against attack and unauthorized information dissemination. Additionally, FDNS is subject to random Office of Inspector General (OIG) or any DHS assigned third-party security audits.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

FDNS-DS users receive the required annual Computer Security Awareness training and Privacy Act Awareness training. In addition, users receive training in the use of FDNS-DS prior to being approved for access to the system. The training addresses the use of the system and appropriate privacy concerns, including Privacy Act obligations (*e.g.*, SORNs, Privacy Act Statements). FDNS Officers also have several mandatory, job-specific training requirements that include discussions on Privacy Act obligations and other restrictions on disclosure of information.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Users receive access to FDNS-DS only on a need-to-know basis. This need-to-know is determined by the individual's current job functions. Users may have read-only access to the information if they have a legitimate need to know as verified by their supervisor and the FDNS-DS business owner, and have successfully completed all required training.

A user requesting access must complete and submit Forms G-872A and B, *USCIS and End User Application for Access*. This application provides the justification for the level of access requested. Additionally the requestor signs the USCIS Rules of Behavior before access is granted.

The requestor's supervisor and the FDNS-DS business owner will review this request; if approved, the requestor's access level is independently confirmed and the user account established.

Criteria, procedures, controls, and responsibilities regarding FDNS-DS systems access are contained in the Sensitive System Security plan for FDNS-DS. Additionally, there are several department and government-wide regulations and directives that provide additional guidance and direction

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

MOAs and MOUs between USCIS and other components of DHS, as well as MOAs and MOUs between USCIS or DHS and other agencies, define information sharing procedures for data maintained by FDNS. MOAs and MOUs document the requesting agency or component's legal authority to acquire such information, as well as USCIS's permission to share in its use under the legal authority granted. All MOAs and MOUs must be reviewed by the program and all applicable parties.

Responsible Officials

Donald K. Hawkins
U.S. Citizenship and Immigration Service
Privacy Officer
Department of Homeland Security

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

APPENDIX A

List of Systems of Records Researched during the Screening Processes and Tracked in FDNS-DS

Below is a list of systems, both internal and external, that exchange data with FDNS-DS, including those used to support screening through ATLAS.

U.S. Citizenship and Immigration Services (USCIS) Systems

- National Benefit Center Process Workflow Repository (NPWR)[38] to facilitate screening on certain form types being processed through the National Benefit Center, Background Check Unit;

  ATLAS is the conduit to perform TECS (SQ-11 and NCIC) checks and return those results to NPWR. ATLAS also receives information from biographic-based checks and performs screening to produce system generated notifications (SGNs).

  - **PIA:**
    - Computer Linked Application Information Management System (CLAIMS 3)[39]
    - Computer Linked Application Information Management System 4 (CLAIMS 4)[40]
    - Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS)[41]
    - Case and Activity Management for International Operations (CAMINO)[42]
    - USCIS Electronic Immigration System (USCIS ELIS)[43]
  - **SORN:**
    - A-File, Index, and National File Tracking System[44]
    - Fraud Detection and National Security Records (FDNS)[45]

[38] NPWR is covered under DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems.
[39] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.
[40] *See* DHS/USCIS/PIA-015 CLAIMS 4 and subsequent updates, *available* at www.dhs.gov/privacy.
[41] *See* DHS/USCIS/PIA-027 RAPS/APSS and subsequent updates, *available at* www.dhs.gov/privacy.
[42] *See* DHS/USCIS/PIA-051 CAMINO, *available* at www.dhs.gov/privacy.
[43] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available* at www.dhs.gov/privacy.
[44] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).
[45] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (Aug. 8, 2012).

- Forthcoming Immigration Biometric and Background Check System
- Benefits Information System (BIS)[46]
- Intercountry Adoptions Security[47]

- Service Center Computer Linked Application Information Management System (SCCLAIMS)[48] to facilitate screening on forms processed in other USCIS case management systems;

  SCCLAIMS maintains a mirror copy of CLAIMS 3 data and is screened against rather than CLAIMS 3 for efficiency purposes. SCCLAIMS is an FDNS system, receives a daily refresh of CLAIMS 3 data, and maintains the CLAIMS 3 data elements needed to perform screening of those benefit request forms processed in CLAIMS 3.

  SCCLAIMS is also used by FDNS-DS/ATLAS to maintain records related to background, identity, and security checks performed through ATLAS's screening capabilities and the corresponding data from its screening algorithms. The types of data will depend on the type of checks performed.

  - **PIAs:**
    - FDNS Directorate[49]
    - FDNS-Data System (FDNS-DS)
    - CLAIMS 3[50]
  - **SORNs:**
    - Fraud Detection and National Security Records[51]
    - A-File, Index, and National File Tracking System[52]
    - Forthcoming Immigration Biometric and Background Check System

[46] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[47] DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (Nov. 8, 2016).
[48] SCCLAIMS is a mirror copy of CLAIMS 3 data.
[49] *See* DHS/USCIS/PIA-013-01 Fraud Detection and National Security (FDNS) Directorate, *available at* www.dhs.gov/privacy.
[50] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.
[51] DHS/USCIS-006 Fraud Detection and National Security Records (FDNS), 77 FR 47411 (Aug. 8, 2012).
[52] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017).

- CLAIMS 3;

  (U//FOUO) Through an automated connection to SCCLAIMS, ATLAS receives information from both biographic and biometric-based checks and performs screening to produce SGNs.

  - **PIAs:** CLAIMS 3[53]
  - **SORN:** BIS[54]

- CLAIMS 4;

  At present, ATLAS receives information from both biographic and biometric-based checks and performs screening to produce SGNs. ATLAS does not connect directly to or return information to CLAIMS 4.

  - **PIA:** CLAIMS 4[55]
  - **SORN:** BIS[56]

- USCIS ELIS;

  At present, ATLAS receives information from both biographic and biometric-based checks and performs screening to produce SGNs.

  FDNS is developing further options for invoking ATLAS's screening capability as described in this PIA in order to return a response to ELIS.

  - **PIA:** ELIS[57]
  - **SORN:** BIS[58]

- CAMINO;

  At present, ATLAS receives information from biometric-based checks and performs screening to produce SGNs. ATLAS does not return information to CAMINO.

  - **PIA:** CAMINO[59]
  - **SORN:**
    - A-File, Index, and National File Tracking System[60]

[53] See DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.
[54] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[55] *See* DHS/USCIS/PIA-015 CLAIMS 4 and subsequent updates, *available* at www.dhs.gov/privacy.
[56] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[57] *See* DHS/USCIS/PIA-056 USCIS ELIS, *available* at www.dhs.gov/privacy.
[58] DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016).
[59] *See* DHS/USCIS/PIA-051 CAMINO, *available* at www.dhs.gov/privacy.
[60] DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept.

- Forthcoming Immigration Biometric and Background Check System
- Intercountry Adoptions Security[61]
- BIS
- Asylum Information and Pre-Screening (AIPS)[62]

- RAPS/APSS;[63]

  At present, ATLAS receives information from biometric-based checks and performs screening to produce SGNs. ATLAS does not connect directly to or return information to RAPS/APSS.

  - **PIA:** RAPS/APSS[64]
  - **SORN:** AIPS[65]

- Marriage Fraud Assurance System (MFAS);

  At present, ATLAS receives information from biometric-based checks and performs screening to produce SGNs. ATLAS does not connect directly to or return information to MFAS.

  - **PIA:** CLAIMS 3[66]
  - **SORN:**
    - A-File, Index, and National File Tracking System
    - Forthcoming Immigration Biometric and Background Check System
    - BIS

- Adoption Case Management System (ACMS);

  At present, ATLAS receives information from biometric-based checks and performs screening to produce SGNs. ATLAS does not connect directly to or return information to ACMS.

18, 2017).
[61] DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (Nov. 8, 2016).
[62] DHS/USCIS-010 AIPS, 80 FR 74781 (November 30, 2015).
[63] *See* DHS/USCIS/PIA-027 RAPS/APSS, and subsequent updates, *available at* www.dhs.gov/privacy.
[64] *See* DHS/USCIS/PIA-027 RAPS/APSS, and subsequent updates, *available at* www.dhs.gov/privacy.
[65] DHS/USCIS-010 AIPS, 80 FR 74781 (November 30, 2015).
[66] *See* DHS/USCIS/PIA-016(a) CLAIMS 3 and Associated Systems, *available at* www.dhs.gov/privacy.

- **PIA:** Domestically Filed Intercountry Adoptions Applications and Petitions[67]
- **SORN:** Intercountry Adoptions Security[68]

- USCIS Lockbox[69] to retrieve data from digitized forms;
  - **PIA:** Benefit Request Intake Process[70]
  - **SORN:**
    - A-File, Index, and National File Tracking System
    - Forthcoming Immigration Biometric and Background Check System BIS
    - Intercountry Adoptions Security
    - AIPS[71]
    - Collections Records--Treasury/Financial Management Service[72]
- Person Centric Query Service (PCQS) to retrieve status information from the Central Index System (CIS);
  - **PIA:** PCQS[73]
  - **SORN:** See PCQS PIA Appendices for associated SORNs
- National File Tracking System (NFTS) to retrieve the physical locations of A-Files;
  - **PIA:** NFTS[74]
  - **SORN:** A-File, Index, and National File Tracking System
- Customer Profile Management System (CPMS) to retrieve data associated with biographic and biometric screening.
  - **PIA:** CPMS[75]

---

[67] *See* DHS/USCIS/PIA-003(a) Integrated Digitization Document Management Program (IDDMP), *available at* www.dhs.gov/privacy.
[68] DHS/USCIS-005 Inter-Country Adoptions Security, 81 FR 78614 (Nov. 8, 2016).
[69] *See* DHS/USCIS/PIA-007(b) Domestically Filed Intercountry Adoptions Applications and Petitions, *available at* www.dhs.gov/privacy.
[70] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.
[71] DHS/USCIS-010 AIPS, 80 FR 74781 (November 30, 2015).
[72] Treasury/FMS.017 - Revenue Collections Records, 74 FR 23006 (May 15, 2009).
[73] *See* DHS/USCIS/PIA-010 Person Centric Query Service (PCQS), *available at* www.dhs.gov/privacy.
[74] *See* DHS/USCIS/PIA-032 National File Tracking System (NFTS), *available at* www.dhs.gov/privacy.
[75] *See* DHS/USCIS/PIA-060 Customer Profile Management Service, *available at* www.dhs.gov/privacy.

- **SORN:** Forthcoming Immigration Biometric and Background Check System

Other Department of Homeland Security (DHS) Component System Interfaces

- DHS Automated Biometric Identification System (IDENT) to retrieve data associated with biometric screening;
  - **PIA:** IDENT[76]
  - **SORN:** IDENT[77]
- U.S. Customs and Border Protection (CBP) TECS system, to perform screening, including checks against the Federal Bureau of Investigation, National Crime Information Center (NCIC);
  - **PIA:** TECS[78]
  - **SORN:** CBP TECS[79]
- CBP Automated Targeting System-Passenger (ATS-P) to support vetting against Intelligence Community and Law Enforcement holdings for certain benefit types;

  ATLAS sends immigration request/application data to ATS to be recurrently vetted against law enforcement (and in the future, intelligence) holdings; ATLAS sends real-time adjudication status updates to ATS to indicate when recurrent vetting should cease. This effort is fully documented in Appendix D to this PIA.
  - **PIA:** ATS-P[80]
  - **SORN:** ATS[81]
- DHS Watchlist Service for real-time screening against Terrorist Screening Data Base (TSDB) records; and
  - **PIA:** FDNS WLS PIA Update[82]
  - **SORN:** DHS WLS SORN[83]

---

[76] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.
[77] DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) 72 FR 31080 (June 5, 2007).
[78] *See* DHS/CBP/PIA-009 TECS System: CBP Primary and Secondary Processing, *available at* www.dhs.gov/privacy.
[79] DHS/CBP-011 U.S. Customs and Border Protection TECS 73 FR 77778 (Dec. 19, 2008).
[80] *See* DHS/CBP/PIA-006(b) Automated Targeting System (ATS), *available at* www.dhs.gov/privacy.
[81] DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012).
[82] *See* DHS/USCIS/PIA-027(e) DHS Watchlist Service, *available at* www.dhs.gov/privacy.
[83] DHS/ALL-030 Use of the Terrorist Screening Database System of Records, 81 FR 19988 (April 6, 2016).

- DHS Email as a Service (EaaS) Simple Mail Transfer Protocol (SMTP) server for email.
    - **PIA:** E-mail Secure Gateway[84]
    - **SORN:**
        - General Information Technology Access Account Records System (GITAARS)[85]
        - General Personnel Records[86]

Other DHS Component Systems Accessed (Manually)

- CBP Analytical Framework for Intelligence (AFI)
    - **PIA:** AFI[87]
    - **SORN:** AFI for Intelligence System[88]
- CBP Arrival and Departure Information System (ADIS)
    - **PIA:** ADIS[89]
    - **SORN:** ADIS[90]
- ICE Student and Exchange Visitor Information System II (SEVIS)
    - **PIA:** SEVIS II[91]
    - **SORN:** SEVIS[92]
- ICE ENFORCE Alien Removal Module
    - **PIA:** Enforcement Integrated Database (EID)[93]
    - **SORN:** Criminal Arrest Records and Immigration Enforcement Records (CARIER)[94]

---

[84] *See* DHS/ALL/PIA-012 E-mail Secure Gateway and subsequent updates, *available at* www.dhs.gov/privacy.
[85] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[86] OPM/GOVT-1 General Personnel Records 77 FR 73694 (December 11, 2012).
[87] *See* DHS/CBP/PIA-010 AFI, *available at* www.dhs.gov/privacy.
[88] DHS/CBP-017 Analytical Framework for Intelligence System, 77 FR 13813 (June 7, 2012).
[89] *See* DHS/CBP/PIA-24 Arrival and Departure System (ADIS), *available at* www.dhs.gov/privacy.
[90] DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (November 18, 2015).
[91] *See* DHS/ICE/PIA-001(a) Student and Exchange Visitor Information System II (SEVIS), *available at* www.dhs.gov/privacy.
[92] DHS/ICE 001 Student and Exchange Visitor Information System, 75 FR 412 (January 5, 2010).
[93] *See* DHS/ICE/PIA-015 Enforcement Integrated Database (EID) and subsequent updates, *available at* www.dhs.gov/privacy.
[94] DHS/ICE-011 CARIER System of Records, 81 FR 72080 (Oct. 19, 2016).

APPENDIX D
Continuous Immigration Vetting

Summary

The U.S. Citizenship and Immigration Services (USCIS) Fraud Detection and National Security (FDNS) is working with the U.S. Customs and Border Protection (CBP) National Targeting Center (NTC) and Targeting and Analysis Systems Program Directorate (TASPD) to enhance and streamline background, identity, and security checks for certain USCIS benefit types through an interagency effort: continuous immigration vetting (CIV). CIV is an end-to-end solution that makes use of existing connections between USCIS and CBP, which are currently used in the refugee vetting process[95], to recurrently vet immigration service and benefit requests against relevant law enforcement and intelligence partner holdings. CIV screens individuals who have applied for a USCIS immigration benefit/request recurrently throughout the adjudication process, resulting in real-time notification of information that could potentially impact the adjudication.

This process uses a connection between USCIS Fraud Detection and National Security – Data System (FDNS-DS)/ATLAS and CBP Automated Targeting System (ATS) to automate certain checks that would otherwise be performed manually and to serve as a new data feed to the ATLAS rules/event-based referral process discussed in the body of this PIA[96].

ATLAS makes use of information already obtained through existing interfaces[97] with USCIS and DHS immigration case management and screening systems, such as USCIS ELIS[98] and DHS IDENT[99], to transmit biographic data from or associated with immigration benefit filings to CBP ATS for recurrent vetting. It is through these interfaces that ATLAS can also receive real-time adjudication status updates and provide notification to CBP ATS when recurring vetting should stop.

USCIS/CBP are implementing CIV in a phased approach, beginning with conducting security checks on applications or requests filed with USCIS against data available in ATS and eventually expanding to encompass checks for benefit and identity fraud, criminal/public safety issues, and, where appropriate, security checks against interagency or intelligence community

---

[95] *See* DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting and DHS/CBP/PIA-006(3) ATS, *available at* www.dhs.gov/privacy.

[96] Information about form intake and initial screening is also included in the various PIAs for the USCIS case management systems and background check systems that make up a part of this process (e.g., CLAIMS 4, ELIS, CPMS).

[97] *See* DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS) Appendix A, *available at* www.dhs.gov/privacy for a complete list of system interfaces to FDNS-DS/ATLAS.

[98] *See* DHS/USCIS/PIA-056 ELIS, available at www.dhs.gov/privacy.

[99] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* www.dhs.gov/privacy.

holdings. Throughout this implementation, USCIS and CBP will continue to assess the legal, privacy, and policy implications and to define rules for recurrent vetting.

In future phases of CIV, USCIS and CBP will work with external partners to develop a solution that perform security checks for certain immigration benefits. USCIS will update this PIA to account for any expansion of CIV.

Core Capabilities Supported

ATLAS Intelligent Investigative Case Management, Operational Decision Management, Information Sharing and Collaboration.

Characterization of the Information

ATLAS sends to CBP ATS information derived from immigration applications filed with USCIS or from the submission of biometrics, to include the same data elements currently used today when ATLAS conducts event-based background, identity, and security checks. This includes, but is not limited to:

- Unique Subject ID;
- Receipt number;
- Applicant name (First, Middle, Last);
- Date of birth;
- Gender;
- Country of birth;
- Citizenship;
- Country of residence;
- Current/Class of admission;
- Alien Registration number;
- Social Security number;
- I-94 number;
- Passport information;
- Address;
- Foreign address;
- Telephone number;

- Ethnicity;
- Sex;
- Height;
- Weight;
- Email;
- Adjudication status;
- Fingerprint Identification Number;
- Encounter ID; and
- Organization/Unit/Sub-Unit Code.

Data Use and Retention

As described in the body of this PIA and in Appendix A, ATLAS queries both internal and external systems automatically to obtain data relating to an individual's background, identity, and security risk. CIV will make use of existing connections between USCIS and CBP, which are currently used in the refugee vetting process[100], to recurrently vet immigration service and benefit requests against law enforcement and intelligence partner holdings throughout the adjudication process.

ATLAS will receive vetting results returned from CBP ATS (and in the future, will receive vetting results from interagency partners). ATLAS filters these results through its rules engine and then transmits the completed results to the end-user in the form of a system generated notification (or SGN). As discussed in the existing FDNS-DS/ATLAS PIA, the approved rules standardize how information is analyzed and filter the results so that only information that assists in the identification of potential benefit or identity fraud, public safety issues, or national security concerns (or trends) is returned. Specially trained FDNS officers serve as gatekeepers who conduct manual reviews of SGNs for validity and to determine if the referral is actionable before it enters the FDNS-DS investigative case management work stream. ATLAS is also able to consolidate information received from multiple sources (e.g., a TECS check vs. an ATS check) to avoid sending duplicate SGNs.

CBP ATS retains USCIS records and vetting results for the duration of CIV in order to assist USCIS in conducting recurrent vetting on immigration filings. This process ultimately supports adjudication of requests for immigration benefits pursuant to USCIS's authority under

[100] *See* DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting and DHS/CBP/PIA-006(3) ATS, *available at* www.dhs.gov/privacy.

the Immigration and Nationality Act.

ATLAS provides ATS with real-time adjudication status updates to inform CBP when recurrent vetting should stop. ATS stops recurrent vetting for ATLAS when encountering administrative closure from an Immigration Judge's calendar or from the Board of Immigration Appeal's docket, certificate of citizenship issue, denial, failure to pay, or withdrawn adjudication activities. Upon such notification, CBP must purge the records from ATS unless that information is linked to active law enforcement lookout records, enforcement activities, or investigations in which case the data will be maintained by CBP in ATS consistent with the ATS retention schedule, as reflected in the ATS system of records notice.

Results:

FDNS will use the CBP vetting results to augment the existing ATLAS rules-based referral process used to produce SGNs based on fraud, public safety, and national security concerns. This process will result in increased efficiencies in the background, identity, and security check process through receipt of real-time notifications of information that may impact adjudications.

Privacy Risks/Mitigation:

Privacy Risk: There is a risk that recurrent vetting will continue after the adjudication of an immigration benefit.

Mitigation: To mitigate this risk, ATLAS has been configured to receive real-time adjudication status updates and will deliver those updates to CBP ATS as notification of when vetting should stop. CBP will be required to return an acknowledgment of receipt of such notification as well as a real-time stopped recurrent vetting indicator. CBP will not retain this data in ATS post-adjudication unless that information is linked to active law enforcement lookout records, enforcement activities, or investigations or cases, in which case that data is maintained by CBP in ATS consistent with the ATS retention schedule as reflected in the ATS SORN (*i.e.*, for the life of the law enforcement matter to support that activity and other enforcement activities that may become related).

Privacy Risk: Under CIV, USCIS will send a greater volume of data elements to CBP than CBP would otherwise receive when encountering individuals as part of its border crossing mission thereby creating a risk of over-collection of information in ATS.

Mitigation: USCIS has determined this volume of information is necessary to ensure the fidelity of the ATLAS/ATS joint screening and matching capabilities. Further, retaining this data in CBP ATS throughout the adjudicative process is necessary to enhance vetting capabilities in the event an individual presents themselves to DHS again, either through travel or in connection with immigration applications, petitions, or requests. The requirement to purge the data from ATS post-adjudication mitigates the risk of over-collection and any potential misuse of information. CBP

will only access the data elements in these files if they are linked to a law enforcement or national security concern.

Privacy Risk: Because ATLAS also performs TECS checks on individuals at various points during the adjudication process, there is a risk that adding ATS as a source for law enforcement information may produce duplicate SGNs.

Mitigation: To mitigate this risk, ATLAS has been developed with the capability to consolidate information received from multiple sources and to suppress duplicate SGNs so that the end user in FDNS-DS is not presented with duplicate sets of the same information. Instead, the end-user will be notified of new or changed information, such as the receipt of new derogatory information related to an individual/subject.

Privacy Risk: Lastly, there is a risk that insufficient notice has been provided so that individuals understand they will be subject to recurrent vetting up through the point of adjudication of a benefit.

Mitigation: This risk is mitigated in that the results under CIV will be filtered through the existing rules-based referral process outlined in the body of this PIA. Through this PIA, USCIS has provided notice that the following events trigger rules-based referrals and SGNs:

1) when an individual presents him or herself to the agency (e.g., when USCIS receives an individual's benefit request form[101] or while capturing an individual's 10-fingerprints at an authorized biometric capture site, for those forms that require fingerprint checks);

2) when derogatory information is associated with the individual in one or more DHS systems (i.e., ATS); and

3) when FDNS performs an administrative inquiry or investigation.

USCIS has also updated Appendix A of this PIA to reflect the automated connection to ATS so that individuals are aware that ATS is a new data source added to the existing event-based referral process. USCIS's use of the information remains unchanged from the original PIA. Separately, CBP is reviewing its compliance documents to determine appropriate updates for added transparency.

[101] *See* DHS/USCIS/PIA-061 Benefit Request Intake Process, *available at* www.dhs.gov/privacy.