

THE HONORABLE RICHARD A. JONES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ABDIQAFAR WAGAFE, *et al.*, on behalf
of themselves and others similarly situated,

Plaintiffs,

v.

JOSEPH R. BIDEN, President of the
United States, *et al.*,

Defendants.

No. 2:17-cv-00094-RAJ

**DECLARATION OF JENNIFER
PASQUARELLA IN SUPPORT OF
PLAINTIFFS' MOTION FOR
SUMMARY JUDGMENT**

I, Jennifer Pasquarella, hereby declare:

1. I have personal knowledge of the facts stated below and am competent to testify regarding the same. I am one of the attorneys for Plaintiffs in this matter, *Wagafe v. Biden*, No. 17-cv-00094 RAJ.

2. [REDACTED]

3. [REDACTED]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 4. [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]

8 5. Attached as **Exhibit 1** is a true and correct copy of excerpts from the January 31,
9 2020 deposition of Kevin Quinn.

10 6. Attached as **Exhibit 2** is a true and correct copy of excerpts from the January 10,
11 2020 deposition of Daniel Renaud.

12 7. Attached as **Exhibit 3** is a true and correct copy of a document produced in this
13 case with a Bates range of DEF-00039006-10.

14 8. Attached as **Exhibit 4** is a true and correct copy of excerpts from a 2003 Audit
15 Report of Immigration and Naturalization Service’s Premium Processing Program.

16 9. Attached as **Exhibit 5** is a true and correct copy of a document produced in this
17 case with a Bates range of DEF-00041251-302.

18 10. Attached as **Exhibit 6** is a true and correct copy of a document produced in this
19 case with a Bates range from CAR001789-856.

20 11. Attached as **Exhibit 7** is a true and correct copy of Defendants’ Objections and
21 Responses to Plaintiffs’ Requests for Admission served on April 17, 2019.

22 12. Attached as **Exhibit 8** is a true and correct copy of excerpts from the September
23 3, 2020 deposition of USCIS’s 30(b)(6) representative.

24 13. Attached as **Exhibit 9** is a true and correct copy of Nermeen Arastu’s expert
25 report.

26 14. Attached as **Exhibit 10** is a true and correct copy of excerpts from the January 27,
27 2020 deposition of Cherie Lombardi.

28

1 15. Attached as **Exhibit 11** is a true and correct copy of excerpts from the December
2 12, 2019 deposition of Christopher Heffron.

3 16. Attached as **Exhibit 12** is a true and correct copy of excerpts from the December
4 10, 2019 deposition of Jamie Benavides.

5 17. Attached as **Exhibit 13** is a true and correct copy of a document produced in this
6 case with a Bates range of CAR000001-7.

7 18. Attached as **Exhibit 14** is a true and correct copy of a document produced in this
8 case with a Bates range of CAR000058-74.

9 19. Attached as **Exhibit 15** is a true and correct copy of a document produced in this
10 case with a Bates range of Def-00035377-402.

11 20. Attached as **Exhibit 16** is a true and correct copy of a document produced in this
12 case with a Bates range of DEF-00116759.0000-.0198.

13 21. Attached as **Exhibit 17** is a true and correct copy of a document produced in this
14 case with a Bates range of DEF-00402579.0000-.0008.

15 22. Attached as **Exhibit 18** is a true and correct copy of a document produced in this
16 case with a Bates range of CAR000345-48.

17 23. Attached as **Exhibit 19** is a true and correct copy of a document produced in this
18 case with a Bates range of DEF-0090968.0000-.0077.

19 24. Attached as **Exhibit 20** is a true and correct copy of a document produced in this
20 case with a Bates range of DEF-00359641.0001-.0231.

21 25. Attached as **Exhibit 21** is a true and correct copy of a document produced in this
22 case with a Bates range from DEF-00068350.0001-.0017.

23 26. Attached as **Exhibit 22** is a true and correct copy of a document produced in this
24 case with a Bates range of DEF-00052177.0000-.0185.

25 27. Attached as **Exhibit 23** is a true and correct copy of a document produced in this
26 case with a Bates range of DEF-000665280.0001-.0044

1 28. Attached as **Exhibit 24** is a true and correct copy of a document produced in this
2 case with a Bates range of DEF-00123589-655.

3 29. Attached as **Exhibit 25** is a true and correct copy of a document produced in this
4 case with a Bates range of DEF-00095009.0000-.0045.

5 30. Attached as **Exhibit 26** is a true and correct copy of a document produced in this
6 case with a Bates range of DEF-00022386-490.

7 31. Attached as **Exhibit 27** is a true and correct copy of a document produced in this
8 case with a Bates range of DEF-00065590.0001-.0314.

9 32. Attached as **Exhibit 28** is a true and correct copy of a document produced in this
10 case with a Bates range of DEF-00003593-791.

11 33. Attached as **Exhibit 29** is a true and correct copy of a document produced in this
12 case with a Bates range of CAR000010-55.

13 34. Attached as **Exhibit 30** is a true and correct copy of a document produced in this
14 case with a Bates range of DEF-00024886-7.

15 35. Attached as **Exhibit 31** is a true and correct copy of a document produced in this
16 case with a Bates range of CAR000366-95.

17 36. Attached as **Exhibit 32** is a true and correct copy of the March 2021
18 Supplemental Expert Report of Sean Kruskol.

19 37. Attached as **Exhibit 33** is a true and correct copy of excerpts from the January 8,
20 2020 deposition of Matthew Emrich.

21 38. Attached as **Exhibit 34** is a true and correct copy of a document produced in this
22 case with a Bates range from DEF-0094968-73.

23 39. Attached as **Exhibit 35** is a true and correct copy of a document produced in this
24 case with a Bates range of CAR000084-92.

25 40. Attached as **Exhibit 36** is a true and correct copy of a document produced in this
26 case with a Bates range of CAR000751-925.

1 41. Attached as **Exhibit 37** is a true and correct copy of the June 2020 Expert Report
2 of Marc Sageman.

3 42. Attached as **Exhibit 38** is a true and correct copy of the July 2020 Expert Report
4 of Jeffrey Danik.

5 43. Attached as **Exhibit 39** is a true and correct copy of a document produced in this
6 case with a Bates range of DEF-00429575-682.

7 44. Attached as **Exhibit 40** is a true and correct copy of a document produced in this
8 case with a Bates range of DEF-00193289-92.

9 45. Attached as **Exhibit 41** is a true and correct copy of a document produced in this
10 case with a Bates number DEF-00095124.

11 46. Attached as **Exhibit 42** is a true and correct copy of a document produced in this
12 case with a Bates range of DEF-00372280.0000-.0213.

13 47. Attached as **Exhibit 43** is a true and correct copy of a document produced in this
14 case with a Bates range of DEF-0094351-534.

15 48. Attached as **Exhibit 44** is a true and correct copy of a document produced in this
16 case with a Bates range of DEF-00432057-112.

17 49. Attached as **Exhibit 45** is a true and correct copy of a document produced in this
18 case with a Bates range of DEF-00431506-793.

19 50. Attached as **Exhibit 46** is a true and correct copy of a document produced in this
20 case with a Bates range of DEF-00024989-92.

21 51. Attached as **Exhibit 47** is a true and correct copy of a document produced in this
22 case with a Bates range of DEF-0094979-93.

23 52. Attached as **Exhibit 48** is a true and correct copy of a document produced in this
24 case with a Bates range of DEF-00373850.000-.0139.

25 53. Attached as **Exhibit 49** is a true and correct copy of a document produced in this
26 case with a Bates range of DEF-00373991.0000-.0174.

1 54. Attached as **Exhibit 50** is a true and correct copy of a document produced in this
2 case with a Bates range of DEF-0088069-155.

3 55. Attached as **Exhibit 51** is a true and correct copy of a document produced in this
4 case with a Bates range of DEF-00126193-245.

5 56. Attached as **Exhibit 52** is a true and correct copy of a document produced in this
6 case with a Bates range of DEF-00186424-5.

7 57. Attached as **Exhibit 53** is a true and correct copy of a document produced in this
8 case with a Bates range of DEF-00156318-20.

9 58. Attached as **Exhibit 54** is a true and correct copy of a document produced in this
10 case with a Bates range of DEF-00095963.0000-.0054.

11 59. Attached as **Exhibit 55** is a true and correct copy of a document produced in this
12 case with a Bates range of DEF-00366782-7105.

13 60. Attached as **Exhibit 56** is a true and correct copy of the July 2020 Expert Report
14 of Bernard Siskin.

15 61. Attached as **Exhibit 57** is a true and correct copy of the July 2020 Expert Report
16 of Sean Kruskol.

17 62. Attached as **Exhibit 58** is a true and correct copy of a document produced in this
18 case with a Bates range of DEF-0075968-6075.

19 63. Attached as **Exhibit 59** is a true and correct copy of a document produced in this
20 case with a Bates range of DEF-00095871.0000-.0091.

21 64. Attached as **Exhibit 60** is a true and correct copy of a document produced in this
22 case with a Bates range of DEF-00036314-385.

23 65. Attached as **Exhibit 61** is a true and correct copy of a document produced in this
24 case with a Bates range of DEF-00095760.0000-.0110.

25 66. Attached as **Exhibit 62** is a true and correct copy of a document produced in this
26 case with a Bates number DEF-00045893.

1 67. Attached as **Exhibit 63** is a true and correct copy of a document produced in this
2 case with a Bates range of DEF-00230963-1041.

3 68. Attached as **Exhibit 64** is a true and correct copy of a document produced in this
4 case with a Bates range of CAR000595-734.

5 69. Attached as **Exhibit 65** is a true and correct copy of a document produced in this
6 case with a Bates range of DEF-00045879-84.

7 70. Attached as **Exhibit 66** is a true and correct copy of a document produced in this
8 case with a Bates range of DEF-00173682-3.

9 71. Attached as **Exhibit 67** is a true and correct copy of a document produced in this
10 case with a Bates range of DEF-00021397.0000-.0066.

11 72. Attached as **Exhibit 68** is a true and correct copy of excerpts from the October 30,
12 2020 deposition of Bernard Siskin.

13 73. Attached as **Exhibit 69** is a true and correct copy of a document produced in this
14 case with a Bates range of DEF-00130853-61.

15 74. Attached as **Exhibit 70** is a true and correct copy of a document produced in this
16 case with a Bates range of DEF-00166783-86.

17 75. Attached as **Exhibit 71** is a true and correct copy of March 2008 remarks by
18 Homeland Security Secretary Michael Chertoff.

19 76. Attached as **Exhibit 72** is a true and correct copy of a document produced in this
20 case with a Bates range of CAR001674-1750.

21 77. Attached as **Exhibit 73** is a true and correct copy of a document produced in this
22 case with a Bates range of CAR00926-1139.

23 78. Attached as **Exhibit 74** is a true and correct copy of excerpts from a document
24 produced in this case with a Bates range of DEF-00422653.0009-.0272.

25 79. Attached as **Exhibit 75** is a true and correct copy of a document produced through
26 the Freedom of Information Act.

1 80. Attached as **Exhibit 76** is a true and correct copy of the July 2020 Expert Report
2 of Jay Gairson.

3 81. Attached as **Exhibit 77** is a true and correct copy of excerpts from a document
4 produced in this case with a Bates range of DEF-00420731.0017-.0590.

5 82. Attached as **Exhibit 78** is a true and correct copy of a document produced in this
6 case with a Bates range of DEF-00425683-88.

7 83. Attached as **Exhibit 79** is a true and correct copy of a document produced in this
8 case with a Bates range of DEF-00425698-9.

9 84. Attached as **Exhibit 80** is a true and correct copy of a document produced through
10 the Freedom of Information Act.

11 85. Attached as **Exhibit 81** is a true and correct copy of excerpts from a document
12 produced in this case with a Bates range of DEF-00421322.0000-.0752.

13 86. Attached as **Exhibit 82** is a true and correct copy of excerpts from a document
14 produced in this case with a Bates range of DEF-00419977.0175-.0753.

15 87. Attached as **Exhibit 83** is a true and correct copy of excerpts of the October 8,
16 2020 deposition of Nadia Daud.

17 88. Attached as **Exhibit 84** is a true and correct copy of a document produced in this
18 case with a Bates range of DEF-00425660-61.

19 89. Attached as **Exhibit 85** is a true and correct copy of excerpts from a document
20 produced in this case with a Bates range of DEF-00422120.0000-.0532.

21 90. Attached as **Exhibit 86** is a true and correct copy of excerpts from a document
22 produced in this case with a Bates range of DEF-00427012.0001-0251.

23 91. Attached as **Exhibit 87** is a true and correct copy of excerpts of an interview with
24 Plaintiff Ostadhassan.

25 92. Attached as **Exhibit 88** is a true and correct copy of the February 2020 Expert
26 Report of Narges Bajoghli.

1 93. Attached as **Exhibit 89** is a true and correct copy of the June 2020 Expert Report
2 of Thomas Ragland.

3 94. Attached as **Exhibit 90** is a true and correct copy of a document produced in this
4 case with a Bates range of CAR001857-1962.

5 95. Attached as **Exhibit 91** is a true and correct copy of excerpts of the February 11,
6 2020 deposition of Alexander Cook.

7 96. Attached as **Exhibit 92** is a true and correct copy of a September 2006
8 Government Accountability Office report titled “Terrorist Watch List Screening: Efforts to Help
9 Reduce Adverse Effects on the Public”.

10 97. Attached as **Exhibit 93** is a true and correct copy of a document produced in this
11 case with a Bates range of DEF-0089772-75.

12 98. Attached as **Exhibit 94** is a true and correct copy of a document produced in this
13 case with a Bates range of DEF-00230826-927.

14 99. Attached as **Exhibit 95** is a true and correct copy of a March 2008 Audit of the
15 U.S. Department of Justice Terrorist Watchlist Nomination Processes.

16 100. Attached as **Exhibit 96** is a true and correct copy of excerpts of a June 2008
17 report titled “The Federal Bureau of Investigation’s Security Check Procedures for Immigration
18 and Applications and Petitions.”

19 101. Attached as **Exhibit 97** is a true and correct copy of excerpts of the July 2012
20 Report titled “Evaluation of the Accuracy of E-Verify Findings,” *available at* <https://www.e-verify.gov/sites/default/files/everify/data/FindingsEVerifyEval2010.pdf>.

22 102. Attached as **Exhibit 98** is a true and correct copy of the August 2020 Expert
23 Report of Marc Sageman.

24 103. Attached as **Exhibit 99** is a true and correct copy of a document produced in this
25 case with a Bates range of DEF-00133750-56.

26 104. Attached as **Exhibit 100** is a true and correct copy of a document produced in this
27 case with a Bates number DEF-00436897.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

I declare under penalty of perjury that the foregoing is true and correct.

EXECUTED this 25th day of March, 2021, in Seattle, Washington.

/s/ Jennifer Pasquarella
Jennifer Pasquarella

EXHIBIT 1
FILED UNDER SEAL

EXHIBIT 2
FILED UNDER SEAL

EXHIBIT 3
FILED UNDER SEAL

EXHIBIT 4

United States Department of Justice
Office of the Inspector General
Audit Division

AUDIT REPORT



IMMIGRATION AND NATURALIZATION SERVICE'S PREMIUM PROCESSING PROGRAM

FEBRUARY 2003

03-14

IMMIGRATION AND NATURALIZATION SERVICE'S PREMIUM PROCESSING PROGRAM

EXECUTIVE SUMMARY

The Office of the Inspector General, Audit Division, has completed an audit of the Immigration and Naturalization Service's (INS) Premium Processing program. The Premium Processing program was established in June 2001 to allow for the payment of a service fee for expedited processing of certain employment-based applications. The INS guarantees processing of premium petitions within 15 calendar days for the basic application fee (\$130) and an additional service fee of \$1,000. According to the regulation that established the Premium Processing program and INS's internal budget documents, the INS will use Premium Processing revenue to hire additional adjudicators, contact representatives, and support personnel to provide service to all its customers and to improve the infrastructure so as to reduce backlogs for all types of petitions and applications. Currently, only the Form I-129, Petition for Non-Immigrant Worker, is eligible for the Premium Processing program.

The audit focused on determining if: (1) the INS was achieving the program goals for the expedited processing of employment-based petitions and applications; (2) the processing times for similar routine petitions and applications changed significantly after the implementation of the Premium Processing program; and (3) the implementation of the mandated Interagency Border Inspection System (IBIS) check procedures impacted the Premium Processing service.¹

Our audit examined the Premium Processing program for the period from June 2001 through October 2002. We reviewed Premium Processing activities at the INS Headquarters in Washington D.C., and at the INS's four service centers: St. Albans, Vermont; Dallas, Texas; Laguna Niguel, California; and Lincoln, Nebraska.

I. Summary of Audit Findings

Although we found that the INS is essentially meeting its 15-day processing requirement for premium petitions, we identified the following deficiencies in the Premium Processing program:

¹ IBIS is a shared multi-agency database of lookout information on individuals.

- The Premium Processing program has adversely affected the time required to adjudicate routine applications and petitions. Consequently, more applicants are paying the \$1,000 Premium Processing fee to assure adjudication within 15 calendar days. The mandate to adjudicate premium applications within 15 days has contributed in part to the increased backlog of routine petitions at the service centers. The backlog has steadily increased since the second quarter of fiscal year (FY) 2002, reaching 3.2 million in September 2002. Thus, a program whose purpose was ultimately to reduce or eliminate adjudications backlogs may be having the unintended consequence of increasing at least some of those backlogs.
- The INS service centers failed to institute IBIS checks in a timely manner. The INS had mandated IBIS checks on all petitions on January 28, 2002, but, due to a breakdown in communications between INS Headquarters and the field, the service centers did not institute IBIS checks for all petitions until March 2002. As a result, 11,830 Premium Processing petitions were adjudicated without IBIS checks between January 28, 2002, and March 18, 2002. In the absence of IBIS checks, the INS cannot be certain that applications from high-risk individuals were not approved.
- Program analysis of Premium Processing has been weak. The INS maintains statistical databases to track all types of adjudications, staff, and supervisory hours, but Premium Processing is not separately identified in these databases or others used for supporting budget requests, position allocations, and general analysis. Consequently, the INS lacks reliable data about the Premium Processing workload and the resources it requires.
- To date, the INS has not conducted a formal analysis of the Premium Processing service fee or the unit processing cost. Premium Processing generated revenue of more than \$115 million in FY 2002. Yet, without program analyses, the INS cannot determine whether staff and resources are appropriately allocated to the service centers for adjudication of Premium Processing applications.

II. Background

Premium Processing applications are adjudicated in the INS service centers located in St. Albans, Vermont (VSC); Dallas, Texas (TSC); Laguna Niguel, California (CSC); and Lincoln, Nebraska (NSC). Currently, only the Form I-129, Petition for a Nonimmigrant Worker, is available for the

premium service. However, the program is expected to expand in 2003 to include the Form I-140, Immigrant Petition for Alien Worker. To date, the program has generated over \$136 million in revenue as shown in the table below.

**PREMIUM PROCESSING REVENUE BY SERVICE CENTER
(IN THOUSANDS OF DOLLARS)**

	VSC	TSC	CSC	NSC	All Centers
FY 2001	\$ 7,366	\$ 4,986	\$ 5,266	\$ 3,764	\$ 21,382
FY 2002	40,765	29,946	25,475	18,848	115,034
Program Total	\$48,131	\$34,932	\$30,741	\$22,612	\$136,416

Source: INS Information Services Division

An additional \$100 million in annual revenue is expected once the Form I-140 is eligible for Premium Processing.

III. Implementation of IBIS Checks

IBIS was established in 1989 to provide a shared multi-agency database of lookout information to improve border enforcement and facilitate inspection of individuals applying for admission to the United States at ports of entry and pre-inspection facilities. Twenty-seven agencies contribute data to IBIS, including the INS, the Federal Bureau of Investigation, the United States Customs Service, and the United States Departments of State and Agriculture.

The data entered into IBIS by the participating agencies include lookouts, wants, warrants, arrests, and convictions. IBIS contains lookouts for suspected or known terrorists and information on individuals who may pose a threat to national security.

Installation of IBIS hardware and software in the service centers was completed in August 2001, but the INS did not mandate IBIS checks until November 15, 2001. On that date the INS required IBIS checks for four categories of applications.² The mandate was expanded on January 28,

² The four applications included the: Form I-485, Application to Register Permanent Residence or to Adjust Status; Form I-90, Application to Replace Permanent Residence Card; Form I-821, Application for Temporary Protected Status; and Form I-765, Application for Employment Authorization.

2002, to include all INS petitions and applications. However, as discussed in Finding I of this report, the service centers did not institute IBIS checks on all petitions until March 18, 2002, due to a lapse in communication between INS Headquarters and the field. INS officials informed us that the service centers were unaware of the January mandate until being verbally informed of it in March 2002.

We determined that between January 28, 2002, and March 18, 2002, the INS service centers adjudicated 387,596 petitions, including 11,830 Premium Processing petitions, without performing IBIS checks. It is unknown how many of the 387,596 beneficiaries of those petitions may have posed a threat to national security.

IV. Management Oversight

The Premium Processing program has had inadequate oversight from management at both the national and service center levels. For example, workload data on Premium Processing have not been incorporated into the INS's work measurement systems. INS officials maintain that because Premium Processing is intended to be a temporary program that will phase itself out as backlogs diminish, it is unnecessary to include it in general statistical and program analyses. We disagree. With over \$136 million in receipts to date, Premium Processing is clearly in need of active managerial scrutiny.

Because Premium Processing is exceeding initial revenue projections of \$80 million per year, we consider a unit cost analysis important for determining whether staff and resources have been adequately allocated to the service centers. Similarly, a fee analysis should be conducted to examine the appropriateness of the \$1,000 premium.

V. Conclusion and Recommendations

Although the immediate goal of Premium Processing is to expedite premium petitions, the long-term objective is to reduce or eliminate backlogs in the INS's total adjudications workload. In our judgment, the INS must bring about greater efficiency in both the Premium Processing and the general adjudications programs to reach this objective. Accordingly, the INS must develop adequate information about the resources that Premium Processing requires.

In this report we make five recommendations of actions the INS can take to improve oversight of the Premium Processing program and ensure that individuals whose petitions have been approved do not fall within the

five high-risk categories established by the INS.³ In brief, we recommend that the INS:

- Strengthen internal communications to assure that service centers and district offices are aware of policy and/or procedural changes that will affect the adjudication of applications and petitions before those changes are implemented.
- Ensure that an appropriate portion of Premium Processing revenues is used to reduce the INS's adjudications backlog.
- Employ the INS's nationwide work measurement system to collect management information about the Premium Processing program.
- Conduct a formal study to determine the unit costs for processing premium cases and to assign adequate staff and other resources to meet the needs of the program.
- Conduct a formal analysis of the \$1,000 premium to ensure that revenues are allocated as required by law.

Our audit objectives, scope, and methodology appear in Appendix I. The details of our work are contained in the Findings and Recommendations section of this report.⁴

³ The five high-risk categories are suspected terrorist, potential threat to national security, active want or warrant, aggravated felon, or prior deportation.

⁴ As part of our audit process, we asked INS headquarters to furnish us with a signed management representation letter containing assurances that our staff were provided with all necessary documents and that no irregularities exist that we were not informed about. As of the date of issuance of this report, the INS has declined to sign the letter. Therefore, our findings are qualified to the extent that we may not have been provided with all relevant information by INS management.

TABLE OF CONTENTS

	Page
INTRODUCTION	1
Background.....	1
Legislative History.....	1
Premium Processing Program Revenue Projections	3
Service Center Processing	5
Interagency Border Inspection System (IBIS)	9
FINDINGS AND RECOMMENDATIONS	12
I. INTERAGENCY BORDER INSPECTION SYSTEM (IBIS) CHECKS	12
History of Background Checks at the INS	13
IBIS Check Process	13
Recommendation	16
II. STATUS OF PREMIUM PROCESSING.....	17
Backlog Reduction.....	17
Effect of IBIS on Processing Times	18
Recommendation	21
III. INS MANAGEMENT OVERSIGHT.....	22
Premium Processing Statistical Data	22
Time and Motion Study	23
Processing Cost Analysis	25
Premium Processing Program Fee Analysis	26
Service Centers Differ in their Methodologies for Program Management and Processing Procedures	26
Recommendations.....	30
OTHER REPORTABLE MATTER	31
STATEMENT ON MANAGEMENT CONTROLS	32
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS	33

APPENDICES:

I.	– AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY	34
II.	– PREMIUM PROCESSING RECEIPT DATA	37
III.	– PREMIUM PROCESSING RECEIPTS BY SERVICE CENTER	43
IV.	– SERVICE CENTER AREAS OF RESPONSIBILITY.....	44
V.	– IBIS POLICY TIMELINE.....	45
VI.	– SUMMARY OF SERVICE CENTER OPERATIONS TEAM (SCOT) SUPPORT SERVICES CONTRACT	48
VII.	– SERVICE CENTER PROCESS FOR IBIS RECORD CHECKS	51
VIII.	– SIGNIFICANT INCIDENT REPORT.....	53
IX.	– ADJUDICATORS FIELD MANUAL.....	54
X.	– FORM I-129, PETITION FOR A NONIMMIGRANT WORKER.....	58
XI.	– FORM I-907, REQUEST FOR PREMIUM PROCESSING SERVICE	60
XII.	– FORM I-140, IMMIGRANT PETITION FOR ALIEN WORKER.....	61
XIII.	– INS RESPONSE TO THE DRAFT REPORT	64
XIV.	– OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION, ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT	74

IMMIGRATION AND NATURALIZATION SERVICE PREMIUM PROCESSING PROGRAM

INTRODUCTION

The Immigration and Naturalization Service (INS) administers the nation's immigration laws, and has both enforcement and benefit service responsibilities. The two objectives identified by the INS for providing benefit services are to adjudicate all immigration cases promptly and impartially in accordance with due process and to provide timely and consistent services and achieve a substantial reduction in the benefits processing backlog. According to the regulation that established the Premium Processing program and INS internal budget documents, the purpose of the Premium Processing program is to allow the payment of a \$1,000 premium to assure expedited processing (within 15 calendar days) of certain employment-based visas,⁵ and to generate revenue that will be used for infrastructure improvements to reduce backlogs for all types of petitions and applications.

Background

The premium service was conceived in 1999 when increasing pressure from Congress and private industry, mainly technology firms, was placed on the INS to expedite the processing of employment-based applications. In its Fiscal Year (FY) 2000 Conference Report, Congress mandated that the INS process certain employment-based applications within 30 days. According to INS officials, such a mandate would have had detrimental effects on adjudication efforts for other applications. In response, the INS sought to develop a program that would provide businesses with the services they needed without compromising other adjudications. The INS began working with the Department of Justice, the Office of Management and Budget, and various private and non-profit organizations to develop a program that would allow businesses to pay a premium for expedited processing of certain petitions.

Legislative History

On December 21, 2000, the President signed an amendment to the Immigration and Nationality Act (Act), which added the following new subsection:

⁵ The premium processing program to date has been available only for the Form I-129, Petition for a Nonimmigrant Worker. A nonimmigrant worker is an alien who comes to the United States temporarily to perform services or labor.

The Attorney General is authorized to establish and collect a premium fee for employment-based petitions and applications. This fee shall be used to provide certain premium-processing services to business customers, and to make infrastructure improvements in the adjudications and customer service process. For approval of the benefit applied for, the petitioner/applicant must meet the legal criteria for such benefit. This fee shall be set at \$1,000, shall be paid in addition to any normal petition/application fee that may be applicable, and shall be deposited as offsetting collections in the Immigration Examinations Fee Account. The Attorney General may adjust this fee according to the Consumer Price Index.

The amendment did not explicitly define "Premium Processing"; therefore, the INS used its authority under Section 103(a) of the Act to establish the details of this new service, such as the processing timeframe and the Standard Operating Procedures.

The INS published an interim rule in the Federal Register, Volume 66, No. 106, on June 1, 2001, establishing Premium Processing for employment-based petitions and applications. The interim rule states that Premium Processing will enable the INS to expedite its services to those business customers who must sometimes recruit and hire foreign workers to fill jobs in short timeframes. The interim rule also states that the INS will use Premium Processing revenue to hire additional adjudicators, contact representatives, and support personnel to provide service to all its customers. The fee is also be used for infrastructure improvements.⁶

The INS designated Form I-129, Petition for a Nonimmigrant Worker, as the application form eligible for Premium Processing. The classifications within the Form I-129 eligible for the premium service as of June 1, 2001 were:

1. E-1, Treaty Trader;
2. E-2, Treaty Investor;

⁶ The INS's FY 2001 Immigration Examinations Fee Account budget states that backlog reduction will be achieved through systems and infrastructure improvements. In addition, \$55 million in Premium Processing revenue will be used for such purposes. The Immigration Services Division's FY 2001 budget for Business and Premium Enhancements states that the \$55 million in additional revenue not required to support adjudication and quality initiatives will be earmarked to fund backlog reduction efforts at service centers and district offices; complete the deployment of CLAIMS 4 for citizenship applications; and replace the older CLAIMS 3 adjudications system at the service centers.

3. H-2A, Agricultural Worker;⁷
4. H-2B, Temporary Worker;
5. H-3, Trainee;
6. L-1, Intra-company Transferee;
7. O-1 and O-2, Aliens of Extraordinary Ability or Achievement;
8. P-1, P-2, and P-3, Athletes and Entertainers; and
9. Q-1, International Cultural Exchange Aliens.

Additional classifications within the Form I-129 eligible for the premium service as of July 30, 2001 were:

10. H-1B, Temporary Worker with Specialty Occupation;
11. R-1, Temporary Worker in Religious Occupation; and
12. TN NAFTA Professional.

These designations (1, 2, and 4 through 12) will continue until the INS publishes a notice of amendment or termination.

The INS estimated that Premium Processing would generate \$25 million in revenue in fiscal year 2001 (due to a mid-year implementation date), and \$80 million in revenue in fiscal year 2002.

In addition to the Act and the interim rule, the following new requirements were added to 8 CFR Part 103:

A petitioner or applicant requesting Premium Processing Service shall submit Form I-907, Request for Premium Processing Service, with the appropriate fee to the Director of the INS service center having jurisdiction over the petition or application. Premium Processing service guarantees 15-calendar day processing of certain employment-based petitions and applications. The 15-calendar day processing period begins when the INS receives the Form I-907, with the fee, at the designated address contained in the instructions to the form.

Premium Processing Program Revenue Projections

The premium service fees are deposited into the Immigration Examinations Fee Account (IEFA) along with fees from approximately 33 other routine applications and petitions. During discussions with INS officials we documented the INS's initial allocation of its estimated premium service revenues. In addition, we determined the INS's methodology for:

⁷ As of June 15, 2001, this classification was no longer eligible for Premium Processing.

- (1) establishing the revenue projections for routine applications; and
- (2) managing the IEFA.

Of the \$80 million in projected fee revenue from Premium Processing, \$17.5 million was allocated by the INS to hire 141 additional adjudicators, contact representatives, and support personnel to provide service to all INS customers. An additional \$7.5 million was allocated for fraud detection, which included the hiring of an additional 54 Special Agents and Intelligence Research Specialists. The remaining \$55 million in program revenue was earmarked for general infrastructure improvements (\$35 million) and additional staffing (\$20 million) that would contribute to the overall backlog reduction efforts. We confirmed that the \$25 million was spent to fill the 195 positions described above. However, we could not determine if the \$55 million was used for general infrastructure improvements because disbursements from the IEFA were not tracked by the source of the funds. Generally, the INS includes its revenue estimates for funding the IEFA as part of its budget request to Congress. Once the budget is approved the INS monitors the IEFA only to ensure that on an overall basis disbursements do not exceed receipts.

The INS process for projecting routine application fee revenues began in the early 1990's with the establishment of a working group (consisting of representatives from the INS Budget, Statistics, and Adjudications Program Offices) charged with developing the official agency revenue projections for the IEFA. This group convenes on a quarterly basis to review and update previous revenue projections. The group looks at every application and petition type where a fee is charged, estimates the number of applications and petitions that will be filed within a given year, and forecasts the resulting fee revenues. These revenue estimates become the basis for each new fiscal year budget request to Congress. The budget request submitted to Congress does not tie specific application revenue estimates to a line item in the budget, but rather the individual application revenue estimates are consolidated into a single IEFA revenue estimate.

Once Congress approves the budget, the INS is not expected to adjust field operation activity based on the receipt of actual fees by application type. It is the overall receipt of application and petition revenue that is monitored to ensure that the receipts match the appropriation level approved by Congress. The INS can spend only up to the level approved by Congress. Any revenue received in excess of the congressional appropriation cannot be spent. A reprogramming request to Congress would be needed to seek increased spending.

According to INS officials, in cases where premium service revenues are identified to have exceeded original budget estimates, the first thing that

would be evaluated is whether the overall revenue collected matched the congressional appropriation. If the revenue collected equaled the appropriation level, this would mean that revenues from routine applications came in lower than projected, and that higher revenues from premium processing covered the loss. If this happened, business would continue as usual and all programs and projects approved in the Examinations Fee Operating Plan would be pursued. The INS would justify the use of the additional premium revenue by stating that the funds were used to finance ongoing premium processing and backlog elimination efforts, albeit at a higher percentage than originally planned.

The reverse would be true if premium revenue was less than projected but revenue from routine applications was higher; the latter revenue would offset the shortfall in revenues from premium processing. In this case, the percentage of premium revenue dedicated to the backlog elimination efforts would be less than planned, and revenue from routine applications would be used to make up the difference.

As part of its annual budget request to Congress, the INS establishes estimates for the various revenue sources that make up the IEFA, such as fees for routine applications and petitions and for premium services. The individual revenue estimates are part of the consolidated IEFA revenue estimate. For expenditure projections, an annual operating plan is utilized to allocate the total IEFA revenue among the functions of the Information Services Division. During the year the IEFA is monitored to ensure that the overall receipts are meeting the appropriate level. The INS does not isolate premium service and individual application revenues from one another when determining if sufficient revenue has been collected to match the congressional appropriation. The fee revenue is consolidated and reported at the account level, which enables the INS to allocate the funds for field operations.

Service Center Processing

The four INS service centers that adjudicate Premium Processing petitions are: Vermont (VSC), Texas (TSC), California (CSC), and Nebraska (NSC). Each service center has its own jurisdictional and geographical responsibilities (see Appendix IV for areas of responsibility for each service center).

Premium Processing petitions are expedited through the adjudications process from the time they reach the service centers.⁸ Premium petitions are mailed to a separate post office box at each service center, and are collected and immediately processed through the mailroom and data entry centers. Mailroom staff check to ensure that the petition is eligible for Premium Processing, then gather all application materials and collect the attached fee payments. Data entry staff enter the petitioner and beneficiary information into CLAIMS (Computer Linked Application Information System), assign it an identification number, and place the entire application package in a color-coded file. The Premium Processing clock starts on the day the mailroom stamps Form I-907, Request for Premium Processing, as received.

Depending on the physical layout of the service center, premium petitions are either hand carried or shuttled to the adjudications staff.⁹ While the service centers vary in how they receive and process premium petitions, generally the current procedure is as follows:

- As premium petitions are received at the adjudications unit, they are batch checked against the IBIS database. IBIS checks are usually completed within one business day.
- Once cleared through IBIS, premium petitions are assigned to an adjudicator. Some adjudicators process only certain classification types, while others work on a range of premium and routine petitions. In the latter case, the premium petitions are adjudicated before any routine cases.
- Premium Processing petitioners have access to a phone number and e-mail address where they or their attorneys can directly contact an Immigration Information Officer or a Center Adjudications Officer with questions regarding their applications. Such access to INS staff is not available to routine Form I-129 petitioners. Adjudications Officers state that the increased contact between them and petitioners assists both in identifying fraud and quickly obtaining necessary information that may have been left out of the original application package.

⁸ The INS has contracted with the Service Center Operations Team (SCOT) to provide comprehensive mail distribution, data entry, and other records processing services at the four service centers involved in premium processing (See Appendix VI).

⁹ Contractor staff at the CSC, VSC, and NSC hand carry premium petitions to the adjudications staff as they are processed in the mailroom and data entry center. At the TSC, premium petitions are shuttled 30 miles from the mailroom to the adjudications staff twice daily.

- Depending on the classification type, the actual adjudication process takes from half an hour to two hours. The actual adjudication time is the same for petitions that are premium processed and for those that are not.
- A daily Critical Aging Report that lists every pending premium petition over eight days old is generated to ensure that adjudicators will not exceed the guaranteed 15-day processing time.
- Once completed, all adjudicated petitions that are premium processed are reviewed by Supervising Center Adjudications Officers. Once reviewed, an Approval, Intent to Deny, Request for Evidence, or Notice of Investigation for Fraud or Misrepresentation is sent to the petitioner.

Routine processing is similar to that of Premium Processing, without the priority given to premium petitions. For example, all routine petitions are mailed to a service center. Once received at the service center, they must be checked in IBIS, sorted, processed, and forwarded to the appropriate adjudications unit. However, mailroom and data entry processing may take significantly longer than one day.

During the adjudication process, routine petitioners do not have the same access to INS staff, and adjudicators are less likely to have personal contact with petitioners or their attorneys regarding missing or questionable information. Instead, any questions the adjudicators have on routine petitions are handled by sending a written Request for Evidence to the petitioners or their attorneys.

While the actual adjudication time is about the same for routine petitions, there is no Critical Aging Report for them and adjudicators are less aware of how long they have had a file. Also, while supervision differs in each service center, it is less stringent for routine petitions than for Premium Processing. For example, in some service centers, only denied petitions are reviewed by Supervising Center Adjudications Officers.

The following table shows the monthly number of premium petitions received and processed by each service center¹⁰ (Appendix II details the monthly receipts by type of classification for each of the service centers).

¹⁰ Because the INS does not accumulate Premium Processing data separately in its work measurement system, we relied on information that the INS's Information Services Division accumulated from the service centers.

Monthly Premium Processing Receipts by Service Centers

	VSC	TSC	CSC	NSC	All Service Centers
FY-2001					
June	547	353	360	202	1,462
July	914	657	640	589	2,800
August	3,641	2,383	2,447	1,851	10,322
September	2,264	1,593	1,819	1,122	6,798
TOTAL	7,366	4,986	5,266	3,764	21,382
FY 2002					
October	2,719	1,941	2,219	1,356	8,235
November	2,410	1,939	1,896	1,243	7,488
December	2,394	2,008	1,884	1,368	7,654
January	2,548	1,957	1,881	1,286	7,672
February	2,694	1,999	1,666	1,219	7,578
March	2,976	2,269	1,644	1,431	8,320
April	3,034	2,527	2,127	1,482	9,170
May	4,334	2,807	2,293	1,803	11,237
June	4,289	3,039	2,197	1,762	11,287
July	4,699	3,609	2,676	2,158	13,142
August	4,606	3,208	2,660	2,040	12,514
September	4,062	2,643	2,332	1,700	10,737
Total	40,765	29,946	25,475	18,848	115,034
Program Totals	48,131	34,932	30,741	22,612	136,416

Source: INS Information Services Division

The INS processed 136,416 premium service petitions from the inception of the Premium Processing program in June 2001 through September 2002. During the same period the INS issued 223 refunds, of which 129 were due to failure to complete processing within the guaranteed 15-day period. The following table delineates why the INS refunded these premium service fees.

**Refunds Processed by Service Centers
During FY 2001 and 2002**

Reasons for Refunds	VSC	CSC	TSC	NSC	Total
H-2A, Now Exempt from Premium Fee	4	0	1	4	9
Ineligible	1	0	6	0	7
Adjudicated Prior to PP Request	0	33	13	5	51
Misc. (no fee payment, duplicates, etc.)	3	9	15	0	27
Failed 15-day processing	29	43	55	2	129
Totals	37	85	90	11	223

Source: INS Information Services Division

Interagency Border Inspection System (IBIS)

As noted above, IBIS is a multi-agency database of lookout information that was initiated in 1989 to improve border enforcement and facilitate inspection of individuals applying for admission to the United States at ports of entry and pre-inspection facilities. IBIS is a joint effort of the INS, the Customs Service, and the Departments of Agriculture and State.¹¹ It combines lookout information from 27 agencies into the Treasury Enforcement Communications System II (TECS II) database. The system, created and maintained by United States Customs Service, supports federal agencies by collecting information on individuals suspected of illegal activities.

TECS II was created to maintain and receive information on persons entering the United States and now serves as the central database for IBIS.

IBIS utilizes document readers that permit the reading of travel documents, improve the exchange of data between agencies regarding alien arrival and departure, and provide staff at ports of entry with the ability quickly to detect fraud, share intelligence, and prosecute violators.

¹¹ Some of the other agencies participating in IBIS include: Intelligence Community Management Staff; Office of the Deputy Assistant Secretary of Defense for Drug Enforcement Policy and Support; Federal Bureau of Investigation; Central Intelligence Agency; Drug Enforcement Administration; Interpol; United States Marshals Service; Federal Aviation Administration; United States Coast Guard; Department of the Interior; Internal Revenue Service; Bureau of Alcohol, Tobacco, and Firearms; United States Secret Service; Bureau of Land Management; and, the Food and Drug Administration.

IBIS contains numerous database files and connects with other databases such as the FBI's National Crime Information Center (NCIC). The INS service centers generally search the IBIS database using name and date of birth and the results of the search can include the following:

- Lookout – Lookout information or adverse information linking individuals to disqualifying criminal activity, ongoing investigations of an individual's links to groups that pose a threat to national security, known or suspected terrorists, advisories as to whether to take or not to take action upon encountering the individual.
- Wants – Data indicating that the individual is wanted by a state or federal law enforcement agency in connection to criminal activity.
- Warrants – State or federally executed documents advising the hold of an alien or lawful permanent resident who is wanted for criminal activity.

In November 2001, the INS instructed the service center directors to begin conducting electronic IBIS checks on four types of applications and petitions.¹² By instructions issued in January 2002, the service centers are now required to conduct these checks on all types of benefit applications and petitions. Although the INS has successfully processed the vast majority of premium petitions within 15 calendar days, the expanded usage of the IBIS database in the adjudication process may adversely affect the meeting of this requirement.

In addition, we were made aware of other IBIS-related issues that can also affect the adjudication process. The INS has a Memorandum of Understanding (MOU) with the United States Customs Service regarding the use of TECS II information. The provisions of the MOU describe the common procedures to provide adequate security, data integrity, and performance. Generally, the INS agrees to comply with the appropriate administrative security provisions related to the use and dissemination of the information in TECS II and to consider all information in TECS II as "Unclassified, For Official Use Only." The INS is currently addressing the following policy issues with the intention of modifying them as appropriate:

¹² As stated previously, the four applications included the: Form I-485, Application to Register Permanent Residence or to Adjust Status; Form I-90, Application to Replace Permanent Residence Card; Form I-821, Application for Temporary Protected Status; and Form I-765, Application for Employment Authorization.

1. Under the MOU, the INS must abide by the "third agency rule", which prohibits the INS from contacting a petitioner regarding IBIS related information without the consent of the third agency (agency responsible for entering data into the IBIS database). For example, for a premium petition that has had an IBIS hit¹³ and is being held and reviewed to determine whether the beneficiary poses a threat to national security, the third agency rule prohibits the INS from contacting the petitioning business or individual to obtain additional information until it has communicated with the originating agency and received permission to do so. This constraint can delay the adjudication process.
2. The INS is limited in its use of the IBIS database information to determine the award or denial of immigration benefits. If, for example, a beneficiary is otherwise eligible for a particular benefit, the INS cannot deny that individual on the basis of an IBIS hit.

According to the INS officials and staff whom we interviewed, the INS is working towards addressing these issues through procedural changes for submitting and processing applications. The agency is also pursuing amendments to the current law based on recent changes in immigration practices. For example, according to INS officials, the INS is seeking provisions in the law that will allow petitions to be placed in abeyance for prolonged periods of time.¹⁴

¹³ An IBIS hit means the beneficiary's name and date of birth match an IBIS entry made by one of the participating agencies.

¹⁴ The INS requested that its Office of the General Counsel address these problems in December 2001; as of October 2002, the issues were still unresolved.

FINDINGS AND RECOMMENDATIONS

I. INTERAGENCY BORDER INSPECTION SYSTEM (IBIS) CHECKS

Between January and March 2002 the INS service centers adjudicated 11,830 Premium Processing petitions without checking them against the IBIS database. As a result, the INS cannot tell how many, if any, of the approved applicants were individuals who were in the INS's five high-risk categories of suspected terrorist, potential threat to national security, active want or warrant, aggravated felon, or prior deportation.

On August 21, 2001, INS Headquarters directed the district offices to conduct IBIS checks on four application types.¹⁵ On November 15, 2001, the INS expanded the mandate to include the same four applications processed in the service centers. Then, on January 28, 2002, IBIS checks were mandated for all applications and petitions, including Form I-129 petitions. However, the service centers did not implement IBIS checks for all applications until March 18, 2002. According to a senior INS official, "Although the 1/28/02 amendment to the Adjudicators' Field Manual provides the direction for full implementation, we were not aware nor were the Service Centers aware that this amendment had been put in place. During the time between January 2002 and the March 14, 2002, the Centers were given verbal direction to begin adding additional forms and to begin the preparation of their operations for full IBIS check implementation" (See Appendix V for a timeline of the IBIS policy changes).¹⁶

At the service centers, the applicant names were to be checked against the IBIS database on a batch basis for derogatory, lookout, criminal investigative, criminal history, and national security or intelligence interest information.

¹⁵ The four applications included the: Form I-485, Application to Register Permanent Residence or to Adjust Status; Form I-90, Application to Replace Permanent Residence Card; Form I-821, Application for Temporary Protected Status; and Form I-765, Application for Employment Authorization.

¹⁶ While our audit was in progress, the INS began requiring checks of the IBIS database for all applicants and petitioners seeking immigration benefits. This decision had a significant impact on the adjudication function of the INS; as a result, we expanded the scope of our audit to include testing of IBIS checks by the service centers that handle premium processed petitions.

The consequences of the delay in implementing IBIS checks on all applications and petitions are unknown but potentially serious. We determined that the INS processed 387,596 total applications (including 11,830 premium processing applications) without IBIS checks in the period between January 28, 2002 and March 18, 2002.

History of Background Checks at the INS

Prior to 2001 the INS had no standardized procedures for conducting background checks on petitioners and beneficiaries. The use of IBIS was not required until that year even though IBIS has existed since 1989. Instead, the INS relied on other resources, such as its own Service Lookout Book, FBI fingerprint checks, and selective verification of applications with the Department of State to check the background of beneficiaries; however, no data are available to document the extent to which the INS made use of these resources. In addition, the Center Adjudications Officers had access on a need-to-know basis to the Non-Immigrant Information System (NIIS), and the service center's Enforcement Operations Division could conduct NCIC checks on petitioners or beneficiaries. However, the use of NIIS and NCIC was not uniform among the service centers.

Beginning in 1999, two INS service centers (VSC and TSC), experimented with IBIS software on a limited basis to determine if this system could be incorporated into the INS adjudication process. In August 2001 the INS completed installation of IBIS hardware and software at all the service centers. The plan was to phase in IBIS gradually, applying the checks to selected petitions over several months.

IBIS Check Process

According to the current INS's Standard Operations Procedure Manual for the Interagency Border Inspection System (November 21, 2002), each service center must conduct IBIS checks on all petitions within 15 days of receipt. Checks are conducted in daily batches¹⁷ that include all petitions and applications received, transferred in, reopened, or that have had a data change. The IBIS check requirement mandates that checks be conducted for all petitioners, applicants, beneficiaries, and any derivatives (for example, businesses and attorneys) that will receive an immediate benefit from submitted applications and petitions. Premium petitions are not checked separately; rather they are generally included in the daily batches.

¹⁷ The batch checks are "front end" verifications at time of receipt. According to the Standard Operations Procedure, adjudicators also have the discretion to perform individual IBIS checks at the time of adjudication prior to final approval.

The IBIS check is valid for only 35 days. During our fieldwork, INS officials stated that the initial IBIS batch checks might not capture all new receipts, potentially missing up to 20 percent of petitions received.¹⁸ Although no reason was given for missing any receipts, we were told that if, at the time of adjudication, a petition does not contain evidence of an IBIS check, or if the check was conducted more than 35 days prior to adjudication, the Center Adjudications Officer must perform an individual check on that petition.¹⁹ Adjudicators are authorized to perform two different types of IBIS checks, as described below:

SQ-11 Query – Individual subject query, allows the user to check a person's name and date of birth against the IBIS database through data entry of the search criteria.

SQ-16 Query – Business subject query, allows the user to check the name of a business or school against the IBIS database through data entry of the search criteria

All matches or hits are sent to the service center's Triage Review Unit for a second, more detailed check to verify that all hits match the correct name and date of birth as recorded on the petition. According to INS staff, approximately one half of the initial IBIS hits are found to be actual matches. In those instances, the Triage Review Unit determines whether the reason for the hit is significant enough to affect adjudication. To accomplish this, the Triage Review Unit identifies cases relating to aggravated felonies, NCIC matches, terrorism, and threats to national security and forwards those applications to the service center's Enforcement Operations Division (EOD) for further evaluation. The IBIS Standard Operations Procedure requires the EOD to refer the terrorism and national security cases to the National Security Unit (NSU) and the Immigration Services Division (ISD) at INS Headquarters for investigation. All other types of hits may be resolved in the Triage Review Unit, or forwarded to the EOD when deemed appropriate.

The EOD determines those hits that may require investigation or further enforcement action. If an IBIS hit is an individual of interest to a local law enforcement agency, the EOD will notify that agency. The Premium Processing 15-day clock is not stopped in such cases. If a

¹⁸ Some receipts are missed in the initial IBIS batch checks because of IBIS's interface with NCIC and the CLAIMS databases.

¹⁹ If a second check is necessary, it is performed by the individual Adjudications Officer using an online query of the IBIS database, rather than as part of another batch check.

determination is not made as to how to proceed until after the 15-day period has expired, the \$1,000 premium fee is returned to the petitioner.

The service center EOD may also work in collaboration with the ISD and the Office of the General Counsel to resolve certain types of hits. For example, if uncertainty remains after a petition has been reviewed by the EOD, the petition may be sent to INS Headquarters where the IBIS Policy Coordinator reviews and responds to any complications. The IBIS Coordinator, in turn, may work with the FBI's Joint Terrorism Task Force and the INS National Security Unit, the Operating Coordination Cell, or the Command Center to address significant IBIS hits (A chart illustrating the IBIS process can be found at Appendix VII).

The ISD summarizes information about IBIS hits from the service centers (and the districts) in the IBIS – Significant Hits Summary. We reviewed the IBIS – Significant Hits Summary covering the period from May 20, 2002 through October 28, 2002. As of October 28, 2002, there were a total of 408 hits listed on the IBIS – Significant Hits Summary. Of the 408 significant IBIS hits, 23 were based on Forms I-129, and 385 were based on other types of applications and petitions. Only 2 of the 23 Form I-129 applications could be identified as Premium Processing applications.²⁰ The two IBIS hits on Premium Processing applications were identified as aggravated felons, and their applications were referred to INS General Counsel for review. With respect to the 385 IBIS hits based on other types of applications and petitions, 256 hits were related to possible terrorist threats and 24 related to threats to national security.

We reviewed the outcome of the 408 total significant IBIS hits and found the following: 354 were referred to the National Security Unit for investigation; 12 did not have an outcome identified in the Significant Hits Summary; and the remaining 42 had various outcomes, including being held in abeyance, denial of the application, or referral to local law enforcement agencies. The following table summarizes the essential data about the 408 significant IBIS hits.

²⁰ Premium Processing petitions with IBIS hits are not routinely tracked. As a result, the total number of premium petitions with significant IBIS hits is unknown.

Significant IBIS Hits

	I-129 Applications	Other Applications	Total
Terrorist Threat	16	256	272
Threat to National Security	2	24	26
Aggravated Felon	2	13	15
Prior Deportation	2	0	2
Active Warrant	1	5	6
Other	0	87	87
Total	23	385	408

Source: INS Significant Hits Report

As of October 23, 2002, approximately 30,000 petitions were in a pending status due to IBIS hits. Because Premium Processing petitions are not checked separately, the INS cannot determine how many of the 30,000 pending petitions are premium without conducting a manual count.

Recommendation

We recommend that the Commissioner, INS:

1. Strengthen internal communications to ensure that all service centers and district offices are fully informed of policy and/or procedural changes that will affect adjudication practices before those changes become effective.

II. STATUS OF PREMIUM PROCESSING

Although the INS has generally met the requirement of processing premium applications within 15 days, the Premium Processing program has adversely affected the time required to adjudicate routine applications and petitions. The mandate to adjudicate premium applications within 15 days has contributed in part to the increased backlog of routine petitions at the service centers. Thus, a program whose purpose was ultimately to reduce or eliminate adjudications backlogs may be having the unintended consequence of increasing at least some of those backlogs.

Backlog Reduction

The INS allocated \$55 million of the \$80 million in anticipated Premium Processing program revenues for general infrastructure improvements and backlog reduction efforts. Our audit showed that for FY 2002 the INS received 115,416 premium service applications. Consequently, the associated program revenue was actually \$115,416,000, which exceeded the original projection (\$80 million) by \$35,416,000. If we apply the INS's original percentages for the allocation of program revenue, the increased revenue of \$35.4 million would have been allocated as follows: adjudications processing (22 percent) \$7.8 million; fraud investigation (9 percent) \$3.2 million; infrastructure improvement (44 percent) \$15.6 million; and backlog reduction (25 percent) \$8.8 million.

Thus, for FY 2002, approximately \$24.4 million (\$15.6 million and \$8.8 million) should have been available for infrastructure improvements and the overall backlog reduction effort. However, because expenditures are not separately identified by revenue source in the IEFA, we could not determine whether any of the additional premium service revenues were actually used to fund the infrastructure improvements and backlog reduction efforts. However, we did determine that the backlogs of pending applications and petitions have continued to grow, as shown in the following table.

Pending Applications and Petitions by Service Centers

PERIOD	VSC	TSC	CSC	NSC	TOTAL
FY 2000	392,757	336,721	670,105	476,808	1,876,391
FY 2001	633,650	712,478	1,016,875	646,465	3,009,468
FY 2002:					
1 ST QTR	636,847	664,971	993,841	582,948	2,878,607
2 ND QTR	693,545	540,010	894,944	519,218	2,647,717
3 RD QTR	737,495	578,959	909,309	632,063	2,857,826
4 TH QTR	759,578	758,863	996,064	734,721	3,249,226

Source: INS Information Services Division

The table illustrates that backlogs reached a low in the second quarter of FY 2002 before beginning a steady increase. According to INS officials, the rising backlog is due in part to the implementation of IBIS checks servicewide in March 2002.

Effect of IBIS on Processing Times

Under ideal conditions the Premium Processing program should have little impact on the processing times of other visa types. However, when situations occur that disrupt general processing times, those times are likely to be further exacerbated by the premium service. As has occurred with the implementation of IBIS checks, more petitioners will choose the premium service if general processing times are prolonged. Because Premium Processing receives priority, backlogs for routine cases may continue to grow. In this way, a program that was intended to reduce backlogs may actually have the effect of increasing backlogs for routine applications.

Since implementation of the IBIS check procedures, the processing times for routine Forms I-129, Petition for a Nonimmigrant Worker, have increased about three-fold from about 37 to 112 days. According to INS officials, the primary reasons for the increases in the backlog of Forms I-129 are:

- Increases in naturalization and temporary protected status applications that were not projected in the resource allocation plan and have contributed to an increase in pending casework.
- Changes in regulations and the launching of new programs, such as the Student and Exchange Visitor and Information System (SEVIS) and the INS Entry and Exit Registration System (INSEERS), to

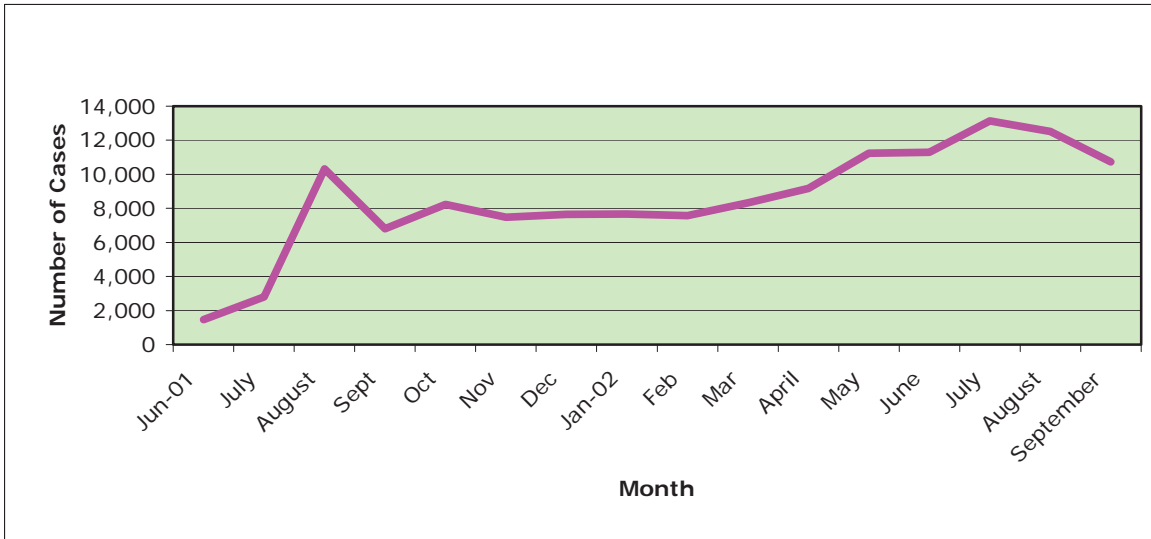
ensure that national security matters are now being taken into consideration when adjudicating applications.

- Failure of the INS to obtain reprogramming authority to hire additional staff to compensate for the more than 500 staff dedicated to conducting IBIS checks.
- The "Zero Tolerance Memorandum," dated March 22, 2002, from the INS Commissioner stating that there will be a "zero tolerance policy with regard to INS employees who fail to abide by Headquarters-issued policy and field instructions. Individuals who fail to abide by issued field guidance or other INS policy will be disciplined appropriately."

As a result of the increased time required to process routine applications, the service centers have reported sizeable increases in the number of premium service cases being filed. The increase in premium cases further prolongs processing times for routine cases because staffing and resources must be pulled from the general adjudication areas to meet the demands of Premium Processing.

The following graph illustrates the total number of premium cases adjudicated since the program's inception. In March 2002, when the IBIS checks were implemented for all applications, the requests for Premium Processing began to increase dramatically.

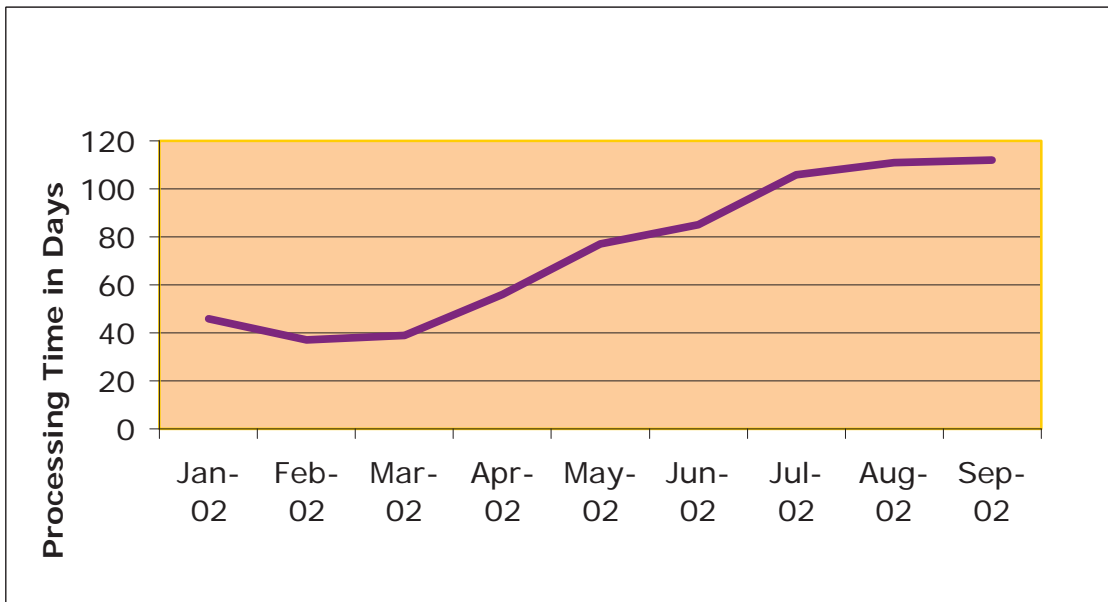
Total Premium Processing Receipts by Month



Source: INS Information Services Division

Increases in premium cases will bring in added revenue. However, they will also significantly impact the processing times for routine Forms I-129, Petition for a Nonimmigrant Worker. The following graph shows the average processing days for routine Forms I-129 for calendar year 2002 through September 2002. It is clear that the processing times have increased significantly since the start of the IBIS checks in March 2002.

Average Processing Times for Routine Forms I-129



Source: INS Information Services Division

There is also some indication that IBIS checks are adversely affecting processing times for Premium Processing petitions. Thirteen refunds were made to Premium Processing petitioners for failure to adjudicate within the guaranteed 15-day period in the 9 months between the program's inception in June 2001 and the start of the IBIS checks in March 2002. In the 7 months from March 2002 through September 2002, an additional 116 refunds were issued for failure to meet the 15-day requirement. Although the number of refunds is small in comparison to the total number of applications processed through the Premium Processing program (less than 0.2 percent), this is an eight-fold increase in the number of refunds.

The mandate for the IBIS checks was a procedural change for INS adjudications. However, the INS did not adequately plan for the implementation of IBIS checks. IBIS existed in the United States Customs Service since 1989 and the INS began experimenting with its usage in 1999. Impacts on both premium and routine employment-based visas can be expected whenever program or procedural changes are put into place. Without adequate planning, the service centers were not prepared to handle unexpected shifts in their workloads, and the processing times for routine petitions has increased dramatically.

Recommendation

We recommend that the Commissioner, INS:

2. Ensure that the excess program revenues, not used for adjudication processing and fraud investigation, are utilized for backlog reduction efforts.

III. INS MANAGEMENT OVERSIGHT

Management oversight of the Premium Processing program has been weak since its inception. The Premium Processing applications and related statistical data are not tracked in the same manner as other national adjudication statistics. In addition, the INS has yet to conduct formal analyses to determine the added costs associated with processing premium applications or the justification for the \$1,000 premium. Because each service center has autonomy over its own organizational structures and methods of program administration, there is little consistency among service centers in these areas. The centers vary considerably in their processing procedures, processing times, and refund rates. However, the INS does not have the mechanisms to evaluate these variations. Without Premium Processing statistical data in the national reporting databases, the INS is unable to determine if the resources devoted to the program are being used effectively, or if the premium is sufficient to cover the costs of premium processing.

Premium Processing Statistical Data

The four service centers that adjudicate Premium Processing petitions submit reports to INS Headquarters. The reports include: (1) a general daily contact report that outlines the number of premium petitions that were approved, denied, or held with a Request for Evidence (RFE) and the corresponding reason; (2) a Critical Aging Report that lists every premium petition over eight days old; (3) a daily summary report listing the day's activity; and (4) an RFE report that lists all pending requests for evidence.

While we do not question the utility of these four reports, we do not consider them sufficient. In our judgment, data on Premium Processing should be incorporated into the INS's general work measurement system, the Performance Analysis System (PAS).²¹ Between June 1, 2001 and September 30, 2002, the INS received 136,416 premium processing applications and more than \$136 million in associated fees. Nevertheless, the INS has not incorporated Premium Processing data in PAS.

²¹ The PAS is a statistical database used for a wide range of purposes, including supporting budget requests, determining position allocations, measuring planned versus actual accomplishments, analyzing application backlogs, and responding to inquiries.

Officials from the INS Office of Policy and Planning stated that they did not include Premium Processing data in the PAS because Premium Processing is not considered a permanent program. However, we disagree with this line of reasoning. The Premium Processing program generated over \$115 million in fiscal year 2002, and the INS estimates that the program will generate over \$180 million once the program is expanded to include the Form I-140, Immigrant Petition for Alien Worker, in 2003. Unless the INS incorporates Premium Processing data in its established databases, it must rely on the various reporting systems from the individual service centers for its program statistical data. These individual systems are inconsistent in methodology and accuracy, and do not provide standardized reporting and adequate program analyses. As a result, we believe the INS management lacks the information needed to determine the proper allocation of resources among the service centers.

PAS data are also useful for determining the strengths and weaknesses of the service centers. Since each service center differs in program administration and organizational structure, the inclusion of Premium Processing information in PAS would assist the INS in determining those operations that are most efficient or effective in meeting their program goals.

Time and Motion Study

Since implementing the Premium Processing program, the INS has not conducted a time and motion study to determine the program's unit cost for processing premium cases. Without a unit cost analysis, the added costs associated with Premium Processing are unclear. For example, the premium service requires extensive customer service, including exclusive telephone lines and e-mail addresses for questions from attorneys and petitioners. However, the costs of these services are unknown.

During our audit, we monitored the adjudication process for premium petitions from beginning to end, and we observed as petitions were hand-carried between the contractor staff and the INS adjudicators. After meeting with all levels of adjudications staff, we determined that Premium Processing petitions are adjudicated by the most experienced and skilled workers, and are reviewed much more frequently and thoroughly than routine cases. Also, adjudicators are far more likely to contact Premium Processing petitioners directly with questions or concerns than they are for routine cases, because of the increased contact already established by the Premium Processing telephone lines and e-mail addresses. These additional services could be more costly to provide, but the INS cannot make a determination of these costs without a cost analysis.

A time and motion study is important because the number of Premium Processing petitions is growing while the total number of Forms I-129, Petition for A Nonimmigrant Worker, is declining. Since reaching 62,474 petitions in February 2002, Form I-129 receipts have dropped every month until reaching 37,972 in June 2002. However, the number of Premium Processing cases has grown since March 2002, so that the total percentage of premium receipts among Forms I-129 is on the rise. The INS initially estimated that premium filings would range from 10 to 25 percent of total filings for eligible petitions. As indicated in the table below, the percentage of premium receipts (to total receipts) increased dramatically from March 2002 to July 2002, after which they started to decline.

Growing Percentage of Premium Receipts

Period	Total I-129 Receipts	Number of I-129 Premium Receipts	Premium Receipts as Percentage of Total I-129 Receipts
FY 2001			
June	68,932	1,462	2%
July	68,439	2,800	4%
August	61,431	10,322	17%
September	51,342	6,798	13%
October	53,867	8,235	15%
November	67,649	7,488	11%
December	40,248	7,654	19%
FY 2002			
January	44,944	7,672	17%
February	62,474	7,578	12%
March	61,962	8,320	13%
April	46,285	9,170	20%
May	41,726	11,237	27%
June	37,972	11,287	30%
July	39,390	13,142	33%
August	44,598	12,514	28%
September	38,668	10,737	28%
Total	829,927	136,416	16%

Source: INS Office of Policy and Planning

If the increasing rate of premium petitions continues, the program will bring in considerably more revenue, up to 50 percent more than anticipated

by the INS.²² Additional revenue notwithstanding, the increase in premium filings is likely to place a disproportionate amount of pressure on service centers and contractor management and staff. Without a study to determine the added costs associated with processing premium cases, INS managers will not have all the information needed to make sound decisions about the allocation of resources for the adjudication of both premium and routine applications and petitions.

Processing Cost Analysis

We conducted a limited analysis to determine how much of the \$1,000 premium is used for processing adjudications. Our analysis determined that approximately \$219 per petition was allocated for processing premium applications. This amount is based on the \$17.5 million,²³ or 22 percent, of the projected \$80 million in program revenue allocated by the INS for Premium Processing staffing and program maintenance. This amount is in addition to the normal application fee of \$130 (the cost of processing routine applications).²⁴ The following table is a breakdown of the \$1,000 program fee, which we calculated based on the INS's allocations of the projected \$80 million in annual program revenue.

Premium Processing \$1,000 Service Fee Breakdown

Fee Utilization Category	Million (\$)	Percent	Fee Breakdown
Adjudication Processing	\$ 17.5	21.88	\$ 218.75
Fraud Investigation	7.5	9.37	93.75
Backlog Reduction and Processing	20.0	25.00	250.00
General Infrastructure Improvements	35.0	43.75	437.50
Total	\$ 80.0	100%	\$1,000.00

Source: INS Information Services Division and OIG Analysis

²² Premium receipts for FY 2002 were \$115,034,000, which is a 44 percent increase over the planned \$80 million.

²³ \$17.5 million divided by 80,000 projected premium petitions equals \$219.

²⁴ The adjusted fee schedule for the IEFA was published in the Federal Register, Vol. 66, No.246, December 21, 2001. The fee for Form I-129, Petition for a Nonimmigrant Worker, was adjusted from \$110 to \$130.

Premium Processing Program Fee Analysis

In addition to the failure to perform a time and motion study for Premium Processing, the INS did not perform a formal analysis to support the \$1,000 Premium Processing service fee. Congress authorized the \$1,000 premium service fee because the program is voluntary and will allow the INS to generate revenue for additional staffing resources, backlog reduction efforts, and infrastructure improvements. However, the fee amount was based primarily on recommendations from potential users, and not on a formal study. In fact, INS officials stated that the fee amount was somewhat arbitrary in its development. Without an adequate analysis, it is unclear how the \$1,000 premium fee will impact users, particularly small businesses. The fee analysis should be completed before the INS expands the Premium Processing program to include other petitions. Furthermore, when Congress authorized Premium Processing, it established the fee at \$1,000 but authorized the Attorney General to adjust the fee according to the Consumer Price Index.

Service Centers Differ in their Methodologies for Program Management and Processing Procedures

During our fieldwork at each of the service centers, we interviewed premium processing management and staff, reviewed staffing allocations, and documented processing procedures. Because the service center directors have considerable discretion to manage their own workloads and allocate staff, we found significant differences in methodology among the four service centers. Our observations are as follows.

St. Albans, Vermont – The VSC is the largest of the four service centers and processed the most premium petitions, 48,131 through September 2002.²⁵ The VSC Premium Processing Unit has a designated staff that processes premium cases along with other petitions. Premium cases have priority, but must be managed along with other work. At the time of our fieldwork, the VSC had a total of 55 service center personnel working on premium cases: 35 Center Adjudications Officers, 8 Immigration Information Officers, and 12 Clerks. The 35 Adjudications Officers included staff that had been hired in anticipation of the introduction of Premium Processing for the Form I-140, Immigrant Petition for Alien Worker. The VSC also has two Supervising Center Adjudications Officers who oversee only Premium Processing cases. The number of staff designated to Premium Processing is flexible, changing depending on the volume of filings. Currently, this group of adjudications staff is working almost exclusively on premium cases, due to the volume of premium receipts.

²⁵ The program began in June 2001 at all service centers.

The VSC is the only center to establish a Premium Processing steering committee to address various concerns from staff and management. The committee is comprised of two Supervising Center Adjudications Officers, two Center Adjudications Officers, one Immigration Information Officer, and one Clerk. The group meets weekly and has the authority to recommend or make changes to the center's Premium Processing program design. In our judgment, this is a best practice that should be implemented by the other service centers.

With the exception of the monthly reports mandated by the ISD, the VSC does not track Premium Processing program data. The VSC employee performance based evaluation system does not call for such performance measures as staff and supervisory hours spent on Premium Processing or other cases.

Dallas, Texas – The TSC processed 34,932 premium petitions through September 2002. The TSC management created a completely separate unit, which processed only Form I-129, Petition for a Nonimmigrant Worker, premium petitions. At the time of our fieldwork, the unit consisted of 17 service center personnel: 9 Center Adjudications Officers, 4 Immigration Information Officers, and 4 Clerks. A Supervising Center Adjudications Officer is also dedicated to premium cases.²⁶ While staff in the Premium Processing Unit focus primarily on premium cases, they may also work with routine applications and petitions if time permits.

The TSC Premium Processing program management worked with the center's Director and the EOD to provide EOD with staff that work exclusively on Premium Processing petitions. Premium Processing Adjudicators have specific IBIS contacts and Information Officers within EOD who work only with premium cases.

Laguna Niguel, California – The CSC processed 30,741 premium petitions through September 2002. At the time of our fieldwork, the CSC had 33 service center personnel working on premium cases: 27 Center Adjudications Officers, 2 Immigration Information Officers, and 4 Clerks. Like the VSC, the CSC designated certain staff to work on Premium Processing cases in addition to other routine petitions. However, unlike the VSC, the Supervising Center Adjudications Officers at the CSC oversee both premium and routine cases.

²⁶ When the Form I-140, Immigrant Petition for Alien Worker, becomes eligible for Premium Processing, separate units at TSC and the NSC, with a manager or supervisor and staff whose first priority will be Premium Processing, will adjudicate the ensuing petitions.

Lincoln, Nebraska – The NSC, the smallest of the four service centers, processed 22,612 premium petitions through September 2002. Like the TSC, the NSC has a separate unit specifically dedicated to Premium Processing. At the time of our fieldwork there were 14 service center personnel (8 Center Adjudications Officers, 2 Immigration Information Officers and 4 Adjudications Clerks) who worked primarily on premium cases, although they handled other types of cases if time allowed. A Supervising Center Adjudications Officer was also dedicated to premium cases.

The four service centers that adjudicate the petitions eligible for Premium Processing differ significantly in their program management, staffing, and processing procedures. The physical characteristics of the centers account for many of the differences, but variations in operations design and management may also contribute to more efficient adjudications processing. However, without comparable data for the four service centers it is difficult to recommend any best practices.

However, we did perform a brief analysis of the average number of premium service applications processed in FY 2002. For purposes of this analysis, we utilized the number of Center Adjudications Officers (CAOs) allocated to each service center by INS Headquarters and the actual number of CAOs working on premium cases at the time of our on-site audit work. The following table compares certain data about staffing and accomplishments that we acquired from each of the service centers and provides our limited analysis of the data.

Fiscal Year 2002
Average Number of Premium Service Applications Processed

FY 2002	VSC	TSC	CSC	NSC	ALL
Premium Service Applications Processed	40,765	29,946	25,475	18,848	115,034
Allocated CAOs	31	28	29	23	111
Applications Processed per Allocated CAO	1,315	1,070	878	819	1,036
Actual CAOs	35	9	27	8	79
Applications Processed per Actual CAO	1,165	3,327	944	2,356	1,456
Allocated vs. Actual CAOs	4	(19)	(2)	(15)	(32)
Dedicated Premium Processing Unit	No	Yes	No	Yes	

Sources: INS Information Services Division, Service Centers, and OIG Analysis.

Our analysis resulted in the following general observations:

- Nationwide the number of CAOs actually performing Premium Processing as of the time of our fieldwork was 32 less than the total number allocated to the service centers for this purpose by INS Headquarters. The number of CAOs actually adjudicating Premium Processing applications at two service centers (TSC and NSC) was significantly lower than the number of CAOs allocated for that function.
- For the CAOs actually performing Premium Processing, the average number of applications processed per CAO was significantly higher at the two service centers that have dedicated Premium Processing units (TSC and NSC). The comparable averages at the other two service centers might have been affected by the extent to which the CAOs process routine applications and petitions.

It also raises certain questions.

- Why did the ratio of applications processed per allocated CAO vary so widely, from 819 (NSC) to 1,315 (VSC)? Were the service centers with higher ratios more efficient than the others? Did the service centers with lower ratios process a larger volume of difficult or time-consuming applications?
- Why was the number of CAOs actually working on Premium Processing less than the number of allocated CAOs at three service centers? Did local management assign CAOs allocated for Premium Processing to other functions? If so, was the Premium Processing workload adversely affected by that assignment?

Without consistent data for all the service centers, it is difficult to answer these questions. More important, the INS does not have adequate data to evaluate the Premium Processing program. The lack of consistent data for all the service centers denies INS management the kind of information needed to provide strong program oversight and to make sound managerial decisions about such matters as position allocation.

As previously mentioned, the inclusion of Premium Processing statistical data in the existing Performance Analysis System would enable program management to determine proper staffing allocations, measure actual versus planned production, and develop adequate information to support budget requests.

Recommendations

We recommend that the Commissioner, INS:

3. Accumulate statistical data for Premium Processing by adding a separate category in the INS work measurement databases.
4. Conduct a comprehensive time and motion study to determine appropriate unit costs for processing premium cases in order to ensure that the service centers have adequate staff and resources to meet the added demands associated with Premium Processing.
5. Conduct an analysis of the \$1,000 premium to ensure that the allocations for processing applications, fraud investigations, backlog reduction, and infrastructure improvements are completed as approved by Congress.

OTHER REPORTABLE MATTER

Program Expansion of Premium Processing

At the time of the program's inception, the INS anticipated it would expand its Premium Processing to include the Form I-140, Immigrant Petition for Alien Worker, yet did not include the related revenue projections in its proposal to Congress or in its early program planning. Focus group meetings conducted with potential users six months before the inception of the program addressed the Form I-129, Petition for a Nonimmigrant Worker, as well as the program's expansion to include the Form I-140. However, all initial program data, such as budget and revenue projections, staffing allocations, and standard operating procedures were based solely on the Form I-129. The INS did not begin including the Form I-140 in budget projections until May 2002.

The Forms I-140 were expected to become eligible for Premium Processing in May 2002, and were to be phased in by classification.²⁷ However, the date was changed several times, and eventually postponed indefinitely because of the focus on the implementation of the IBIS check procedures. If Premium Processing had been expanded to include the Forms I-140 on May 1, 2002 as initially planned, program revenue to date would be approximately 39 percent higher. Based on the INS's initial projections, the inclusion of the Forms I-140 in Premium Processing was expected to generate an additional \$45 million in FY 2002. The INS now estimates that the inclusion of the Forms I-140 in Premium Processing will more than double program revenues in FY 2003 and beyond.

²⁷ The Form I-140, Immigrant Petition for Alien Worker, is an application for permanent residence in the United States based on employment. There are several classifications within the Form I-140. The initial timeline for implementing Premium Processing to the Forms I-140 is as follows:

- May 1, 2002: Schedule A Group 1, Registered Nurse; Schedule A Group 2 Physical Therapist; E13, Multinational Executive/Manager; EW3, Other Workers (less than two years training or work experience).
- July 1, 2002: E31, Skilled worker (two years education, training or work experience); E32, Professional (Baccalaureate Degree or foreign equivalent and beneficiary is professional).
- September 1, 2002: NIW, National Interest Waiver; I11, Extraordinary Ability.
- November 1, 2002: E12, Outstanding Professor/Researcher; E21, Advanced Degree/Exceptional Ability.

STATEMENT ON MANAGEMENT CONTROLS

In planning and performing our audit of the INS's Premium Processing program, we considered the INS's management controls for the purpose of determining our auditing procedures. This evaluation was not made for the purpose of providing assurances on the management control structure as a whole.

We identified the following weaknesses in the INS's Premium Processing program and made appropriate recommendations. They are:

- The INS service centers failed to implement IBIS checks in a timely manner and that failure resulted in 11,830 premium processing petitions and 375,766 routine petitions being adjudicated without being checked against the IBIS database between January and March 2002.
- The INS failed to meet its goal of reducing the servicewide backlog for all petitions. Our analysis found that the backlog has increased steadily since the second quarter of 2002.
- The Premium Processing program oversight is weak. Premium Processing applications and related statistical data are not separately identified in the national adjudication statistics. Furthermore, the INS did not conduct formal analyses to determine the added costs associated with the Premium Processing program or the justification of the \$1,000 premium.

Because we are not expressing an opinion on the INS's overall management control structure, this statement is intended solely for the information and use of the INS in managing its premium service program.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

We conducted our audit of the INS's administration of the Premium Processing program in accordance with government auditing standards.

As required by the standards, we tested selected transactions and records to obtain reasonable assurance about the INS's compliance with laws and regulations that, if not complied with, we believe could have a material effect on operations. Compliance with laws and regulations applicable to the Premium Processing program is the responsibility of the INS management.

An audit includes examining, on a test basis, evidence about laws and regulations. The specific requirements for which we conducted tests are contained in the United States Code, Title 8, §1356, concerning the collection of fees.

Except for the issues discussed in the Findings and Recommendations section in this report, nothing came to our attention that causes us to believe that the INS management was not in compliance with the section of the United States Code cited above.

EXHIBIT 5
FILED UNDER SEAL

EXHIBIT 6
FILED UNDER SEAL

EXHIBIT 7
FILED UNDER SEAL

EXHIBIT 8
FILED UNDER SEAL

EXHIBIT 9
FILED UNDER SEAL

EXHIBIT 10
FILED UNDER SEAL

EXHIBIT 11
FILED UNDER SEAL

EXHIBIT 12
FILED UNDER SEAL

EXHIBIT 13
FILED UNDER SEAL

EXHIBIT 14
FILED UNDER SEAL

EXHIBIT 15
FILED UNDER SEAL

EXHIBIT 16
FILED UNDER SEAL

EXHIBIT 17
FILED UNDER SEAL

EXHIBIT 18
FILED UNDER SEAL

EXHIBIT 19
FILED UNDER SEAL

EXHIBIT 20
FILED UNDER SEAL

EXHIBIT 21
FILED UNDER SEAL

EXHIBIT 22
FILED UNDER SEAL

EXHIBIT 23
FILED UNDER SEAL

EXHIBIT 24
FILED UNDER SEAL

EXHIBIT 25
FILED UNDER SEAL

EXHIBIT 26
FILED UNDER SEAL

EXHIBIT 27
FILED UNDER SEAL

EXHIBIT 28
FILED UNDER SEAL

EXHIBIT 29
FILED UNDER SEAL

EXHIBIT 30
FILED UNDER SEAL

EXHIBIT 31
FILED UNDER SEAL

EXHIBIT 32
FILED UNDER SEAL

EXHIBIT 33
FILED UNDER SEAL

EXHIBIT 34
FILED UNDER SEAL

EXHIBIT 35
FILED UNDER SEAL

EXHIBIT 36
FILED UNDER SEAL

EXHIBIT 37
FILED UNDER SEAL

EXHIBIT 38
FILED UNDER SEAL

EXHIBIT 39
FILED UNDER SEAL

EXHIBIT 40
FILED UNDER SEAL

EXHIBIT 41
FILED UNDER SEAL

EXHIBIT 42
FILED UNDER SEAL

EXHIBIT 43
FILED UNDER SEAL

EXHIBIT 44
FILED UNDER SEAL

EXHIBIT 45
FILED UNDER SEAL

EXHIBIT 46
FILED UNDER SEAL

EXHIBIT 47
FILED UNDER SEAL

EXHIBIT 48
FILED UNDER SEAL

EXHIBIT 49
FILED UNDER SEAL

EXHIBIT 50
FILED UNDER SEAL

EXHIBIT 51
FILED UNDER SEAL

EXHIBIT 52
FILED UNDER SEAL

EXHIBIT 53
FILED UNDER SEAL

EXHIBIT 54
FILED UNDER SEAL

EXHIBIT 55
FILED UNDER SEAL

EXHIBIT 56
FILED UNDER SEAL

EXHIBIT 57
FILED UNDER SEAL

EXHIBIT 58
FILED UNDER SEAL

EXHIBIT 59
FILED UNDER SEAL

EXHIBIT 60
FILED UNDER SEAL

EXHIBIT 61
FILED UNDER SEAL

EXHIBIT 62
FILED UNDER SEAL

EXHIBIT 63
FILED UNDER SEAL

EXHIBIT 64
FILED UNDER SEAL

EXHIBIT 65
FILED UNDER SEAL

EXHIBIT 66
FILED UNDER SEAL

EXHIBIT 67
FILED UNDER SEAL

EXHIBIT 68
FILED UNDER SEAL

EXHIBIT 69
FILED UNDER SEAL

EXHIBIT 70
FILED UNDER SEAL

EXHIBIT 71

Press Room Archive

- [Press Releases](#)
- [Speeches and Statements](#)
- [Testimony](#)
- [Multimedia](#)
- [Contacts](#)
- [En Español](#)


This is Archived Material

This information is not current, is not being updated, and may contain broken links.

Remarks by Homeland Security Secretary Michael Chertoff at Roundtable With Bloggers

Release Date: March 3, 2008

Secretary Chertoff: So, this is the first of what may be a number of these conferences or discussions. So I'll give you kind of a quick overview, and then take questions.

Five year anniversary. There are basically five major bands in which I'll kind of analyze our work. There is keeping bad people out of the country, keeping bad stuff out of the country, protecting the infrastructure, building a capable response agency, and integrating the department.

Let me tell you where I think we are with each of these five where I think we need -- I'd like to just go by the end of the year, so that I can turn the keys over to the next individual with -- in a pretty good functioning car.

Keeping people out that are dangerous: At the ports of entry, we are very significantly ahead of where we were five years ago, and where we were three years ago when I was -- you know, first started here at the department. US-VISIT, two fingers, is up and running at all of our ports of entry. We're now moving to 10 fingers overseas, at the consulates, and here at the airports. That gives us a capability not only to check fingerprints in our existing records, but to check against latent fingerprints that we collect in safehouses or battlefields around the world.

We have an agreement with the Europeans that will enable us to use Passenger Named Record Data, which gives us better information about who's coming into the country, so we can analyze whether there are connections that we need to be worried about so that we maybe take a closer look at somebody when they arrive.

We're getting somewhat more advanced warning of who's getting on the airplane. That, again, eliminates the risk of having to turn a plane around when we discover a "No-Fly" is on the plane when they're coming in here.

When you put all these things together -- tougher documentation requirements at the land border, requiring passports, if you're traveling in the Western Hemisphere by air -- we are strengthening the document requirements, the biometric requirements, and the information that we gather, in order to have a better picture of who ought to go into secondary, and perhaps not be let into the country. And time and again, we have turned people away who you would not want to have in the country based upon what is -- you know, what their connections are, or what their fingerprints turn up on, or something of that sort.

Between the ports of entry, we're on track to build 670 miles of fencing by the end of this year. We are at over 15,400 Border Patrol; that's on track to over 18,000 by the end of the year, which will double the Border Patrol.

SBlNet -- which, contrary to Spencer Hsu, is not P-28; I'm going to really spell it out really clearly: P-28 is to SBlNet as one cruiser is to the United States Navy. It is not the same thing.

So we have, as of last week, four unmanned aerial vehicles up over the southwest border. We expect by the end of this year to have 40 ground-based radar systems, 7,500 individual sensors. And we do have P-28, which is an integrated approach to radar and cameras, which we've accepted as being functionally workable, and which we're now going to take to 2.0 before we deploy it at other parts of the border. It was never intended to be one-size-fits-all across the border, nor will it be one-size-fits-all across the border. All these tools are going to be deployed in various ways, depending on what the particular typography of the border is.

So I think we've made a lot of progress there, and the results show a decrease in apprehensions, and other metrics that show, in my sense, that the flow across the southwest border is diminishing, although it isn't -- certainly not, by no means, eradicated.

In terms of keeping bad stuff out of the country, five years ago we had zero containers scanned for radiation when they came into the U.S. Now we have almost a hundred percent. We are putting out a new general aviation rule that's going to result in ultimately getting more information about who's flying private planes in from overseas, and who is -- and what is on those planes, including -- we're ultimately anticipating having screening overseas, before the plane takes off and lands in the continent of the United States, because we don't want people putting a bomb on a plane and then just putting a plane into a building.

We're building a small boats strategy to deal with the possibility of small boats as an attack vector.

Protecting infrastructure. We have our new chemical plant regulations. The most dangerous chemical plants are held in tank cars in a stable position. In other words, where they're just left idle. We want to move them; we don't want to have them sitting idly in urban areas or populated areas.

Working with the rail industry, we've dramatically decreased the amount of time that toxic chemicals are held in tank cars in a stable position. In other words, where they're just left idle. We want to move them; we don't want to have them sitting idly in urban areas or populated areas.

We are beginning our cyber strategy. That will not be done this year, but I'm hoping we can get it, a cyber center, up and running, and have a full set of plans and a funding budget to move forward over the next several years to get to the next level of cyber security.

On response, we've got -- I think FEMA has done a significant job retooling itself: much better capability to track in real time commodities and things that are being provided; moving from a part-time reserve system of disaster assistance employees to a corps of several thousand full-time employees, so they're not -- it's so that it is their day job to be ready and trained to do disaster assistance; much better metrics and computer tracking, with respect to claims that are being received and being paid out in a way that we didn't have three years ago.

And finally, on the issue of integration, much better cost component planning. Metrics, now, they track how we're doing at the border and how we're doing with claims management -- what our flow time is through our ports of entry; what our flow time is through or TSA check points -- all of which makes it easier to manage as a single institution.

Two things remain to be done as the kind of building blocks of maturing the institution. One is to implement the management directive I issued sometime back to drive career progression, so that you have to have joint service, or service in another component, in order to reach the senior levels of the department. That would build the same kind of jointness that you have in DOD.

The last one is to get a campus. We've put it in the budget again this year. I read somewhere, and this may be incorrect, that there is as many 90 individual locations around the greater Washington area, in which various elements of DHS are housed. We've got to have a place where the leadership can be operating in a single office the way it is with most other -- with all other departments. That is important for morale, it makes it easier to manage, and it saves time.

URL

https://web.archive.org/web/20120212183120/http://www.dhs.gov/xnews/releases/pr_1204587093735.shtm

Timestamp

Thu Mar 25 2021 10:18:21 GMT-0700 (Pacific Daylight Time)

So that's kind of an overview. Things I want to get done I've kind of mentioned. I want to get the general aviation piece done; I want to get REAL ID, and enhanced driver's licenses -- continue to build momentum on that; I want to get the cyber piece planned and the funding stream put out there. Those are some of the major things I want to get done before the end of the year.

Question: Mr. Secretary, you had, at the very beginning, laid out some great progress that's been made in terms of preventing bad people from getting in. And part of the Homeland Security mission, which is a challenging one, is that while you are responsible for protecting against bad things, you're also responsible for facilitating good things. And be that the flow of people, in this case, USCIS is responsible for that for the department. They've begun a \$3.5 billion transformation.

And I'm hoping you could speak to that in two ways. What's your concept of success in that, in terms of the national security part of it, the operational excellence part of it, and customer service part of it?

Secretary Chertoff: Three -- two main things. One is, we have to move from a paper-based system to a totally electronically-based system. We still have too much paper, and it's hard to track, it's hard to manage, and it takes a lot of time.

The second piece is, I want to rebuild -- re-engineer the system in a couple of ways. One is, and the most urgent, is to deal with the background check problem. It just takes way too long for the Bureau to complete background checks for a small but a significant number of people. The majority of people -- you know, if the name doesn't pop up on anything in the -- it's pretty quick. But for a small number -- but still significant, and certainly to the individual, significant -- if their name crops up and it's an older case, and it's in a file somewhere, someone has got to hunt it down. And to be perfectly honest, that is not a top-priority job for an agent, is to go through an old paper record sitting in a warehouse.

Looking forward as we go electronically, and as the Bureau goes electronically, that problem will diminish. But looking backwards we have to re-engineer the system to be a little tougher. And one of the things we did, for example, with the green cards was we said, for background checks that took longer than six months, we would give you a green card, and then if it turned out the background check later revealed a problem, we would take the green card away.

Now why did we do that -- because I got criticized, "Oh, you're sacrificing national security." Here's why. First of all, if you haven't been -- if it's going to take longer than six months, it's clear that you're not on a Terrorist Watch List, you haven't been convicted of a crime, you haven't been indicted for a crime. In other words, most of the major things you would worry about -- it's a very easy thing to determine whether you've had a problem or not. What you're not going to get in that six months is the guy whose name came up in a file somewhere. And the vast majority of those are benign mentions.

Secondly, you're here. If you're going to do something bad, you're still here legally. The green card -- it's not like we're bringing you in from overseas. So if you think about it logically, the risk of giving you the green card with the understanding that it can be pulled away if something turns up, it's a minimal risk. It's a minimal, marginal risk. Whereas the customer service value of giving someone the green card is high. That's an example of trying to be more cost-benefit in the system.

Question: On the Al Capone style method of pursuing terrorism-related cases on the Visa Waiver program, Friday we held a session on cyber security, and that followed the day after the hearing by the House Homeland Security on cyber initiative. And committee members were critical of cyber initiative, and very concerned about the implementation of that. What can you do to address the committee's concerns about cyber security, and do you have any comments on the stories about the DNI pursuing -- trying to gather some intelligence on web-gaming through a new initiative?

Secretary Chertoff: The DNI and I ought to talk about his initiatives.

In terms of cyber security, you know, we came -- a lot of it's classified, and so -- and the hearing you're talking about was an open hearing. I mean, I've been in a couple of classified hearings where we've talked about this with the intelligence committee, and we've had some briefings, classified briefings, with members of the Homeland Committees and other committees.

The basic proposition with cyber is this: We're nibbling at the edges now, and we need to have kind of a game-changing approach to this. And part of that game-changing approach is to rationalize what we're doing in the federal domain, and get better control of what enters the federal domain so we can determine whether it's a threat or not.

We came -- you know, we are -- there are a series of plans we are developing to get this thing done. We came early to Congress; we came before the plans were developed. Why did we do that? Because when we go to Congress after the plans are developed, here's what I hear: "Why do you wait until the plans are developed? You don't consult with us." Now we go and we say, "Well, we want to consult with you while we're in the early stages," they go, "How come you don't have a plan yet?" That falls in the category of "got you coming and going." You can't win. If you do X, we yell at you. If you don't do X, we yell at you.

I still think it's the right way to do it. We've told them there's an issue here, here's a general sense of how we want to proceed with it; we acknowledge there's more work to be done. It's a hard problem, particularly in the private sector, because the private sector we can only work in partnership with. We don't want to mandate that the private sector do something. We don't want to suggest that we're going to sit on the Internet over everybody and monitor what they do. That would get people's hackles raised. We need to figure out a way to give the private sector the opportunity to partner with the federal government -- but not make them do it. And so it's a very tricky issue.

One of the reasons, honestly, it hasn't been addressed aptly in the last five years is because it's very hard. It's hard conceptually to figure out how best to do it, and it's hard politically because as soon as you talk about the government and the Internet, you really send some people into orbit. So there's been a tendency to avoid the issue, because it's just hard; let's not think about it.

But I think we all collectively agreed, and certainly the President, I think, has this view, that our job is not to avoid hard problems; it's to tackle them. And it is hard. It's going to be tough to design this. But there's no reason to delay the beginning of the process. And so we're going -- you know, we've kind of, you know, got to Congress early in the process, and I hope that they proceed in the same spirit; they recognize that we're giving them opportunity to have input. Input means not just saying no to everything, but also means, have a constructive -- if you have an alternative solution, we're all ears. But just saying that's not -- you know, the super Goldilocks approach, "The porridge is always too hot or too cold," does -- it's not constructive. What's constructive is, "Okay, here's a better way to do that." And, you know, if you have a better way, God bless you. We'll certainly listen.

Question: Is it fair to say that cyber security is -- that that whole area is far behind -- that DHS has been far behind on cyber security --

Secretary Chertoff: I would say it's the one area in which I feel we've been behind where I would like to be. That's fair to say -- which is why we're trying to really grab it.

Question: Mr. Secretary, to follow up on that, my -- I asked my readers what questions to ask, and they focused a little bit on the new cyber security initiative, because there was -- I don't know if you saw the profile of DNI McConnell in The New Yorker, one of his aides told The New Yorker that the cyber security initiative would mean giving the government the authority to examine basically any packet on the Internet.

Secretary Chertoff: Yes, that's just wrong.

Question: Okay. So, for you, what is the -- what are the main threats that you think that, you know, on the Internet, that Homeland Security has a role in --

URL

https://web.archive.org/web/20120212183120/http://www.dhs.gov/xnews/releases/pr_1204587093735.shtm

Timestamp

Thu Mar 25 2021 10:20:07 GMT-0700 (Pacific Daylight Time)

Secretary Chertoff: I mean, the biggest role we have is to deal with protecting the federal government -- that's our primary responsibility. We do some of this with EINSTEIN -- what I call EINSTEIN 1.0, which is kind of a first cut at a system of detection. But for a number of reasons, it's not as capable as it could be. Part of that is we've deliberately not taken the next step -- taken it up to the next level. Part of it is that not all of the component agencies, all of which run their own cyber shops, not all of them have the same level of capabilities; they're not -- they don't have emergency watches up 24/7.

So I think the minimal thing we need to do is get our own house in order, federally. And that means herding all the different cats of the executive branch agencies into a kind of a single pen where we can have some capability of detecting what's coming in and out of the federal domain.

Question: Mr. Secretary, I've interviewed you before about the unilateral things you've done with the environment, as well as the travel initiatives. And before you came in, he was telling us a lot about the bureaucratic oversight that you're having difficulty with. So kind of a two-part question. The first part: Are you happy with those actions you've taken --

Secretary Chertoff: Yes.

Question: -- and have those pandered out? And what is the role for congressional oversight, and how do you think that should be streamlined?

Secretary Chertoff: You see, I think congressional oversight is a very helpful and very good thing and appropriate, and I have nothing but good things to say about it. But it needs to be rationalized. I've heard estimates -- 86 to 88 different committees or sub-committees that supervise our activity.

In the main, what I would like to see happen is, we have two authorizing committees and two appropriating committees; one in the Senate and one in the House. They should own responsibility for oversight. We work well with them. They don't always agree with me, I don't always agree with them, but we work constructively. And at least they have the big picture of what we do. And so when they propose things or they deal with us, they have a sense of what the full menu of challenges we have is.

The danger with having a lot of other committees is this: not just that we have to write more reports or testify more, but that committees -- additional committees, they have a jurisdiction over a little narrow slice of the Department, and their agenda becomes promoting that slice. And they don't have the visibility into the trade-offs that are involved. So you wind up getting a lot of conflicting direction. This committee is concerned about this problem, that committee is concerned about that problem -- and they want their problem attended to. And you can't satisfy a hundred masters.

So if Congress could funnel these things through, like most departments, to -- you know, each House has one authorizer and one appropriator -- then I think we'd have a good balance. Congress could certainly do oversight and -- but at least it would come through a perspective that sees the whole range of what our issues are, as opposed to simply one issue.

Question: Do you have any idea how many times you've testified before Congress? I mean, I know it seems like every other week.

Secretary Chertoff: I don't -- I actually do not wind up testifying all that much. I probably testified less than 10 times a year. But the Department testifies a lot, and we do a lot of briefings, and a lot of requests for information. We do hundreds and hundreds of reports. That's where the real burden comes in.

Question: Okay, one last question, sorry. I didn't realize that you were housed in 90 different sites.

Secretary Chertoff: I figure 90 -- but a lot.

Question: Okay, something like that. What else would you propose that Congress do, just to make the functionality of the Department work better?

Secretary Chertoff: I think consolidating us; I think funding our budget requests for the not-particularly-glamorous-but-indispensable things having to do with management, acquisition capability, IT capability. You know, this is stuff which -- you know, when they're trying to make the budget at the end, and often, in order to have more money for grants, they cut that stuff. And the problem is when you cut that stuff, invariably what happens is, six months later, we get a criticism for, we're not managing our acquisitions well. Well, you can't manage your acquisitions well if you can't hire people to do it.

So I'd like to have a balanced program of funding, and I think that -- you know, and I think our budget requests does that -- I think that, plus our getting into a single campus, would be very, very big steps forward.

Question: Sir, when you came onboard, you immediately started talking about risk, and how risk analysis and risk management would play a role in how resources were put out, how firms would run, et cetera. And you mentioned the chemical area earlier, as to what was working there. It seems, though, that there aren't necessarily commonalities to risk on how we're looking at different infrastructures. And how can we give this President and his successor a really good -- I would say, a really good map of where we are with risk in this country, when all the various infrastructure pieces that we've got, those puzzle pieces don't match up by how we're looking at risk?

Secretary Chertoff: Well, I think for us they do in this sense. We generally look at risk as consequence, vulnerability, and threat -- and threat includes intent and capability. And of those things, probably the most significant is consequence, because it's the least variable. I mean, threat, in terms of intent and capability, can change quite readily. Vulnerability, if we're doing our job right, gets reduced -- so that should be a risk reducer. But consequence, really, generally means the same. And that's the template we use across everything.

So we use that with -- and the other technique we use is, we tend to be performance standard-based as opposed to specification-based. And I will say, to reduce the risk, you've got to be able to do the following things, and we talk about outcomes, like: defend against this kind of attack for this period of time; or, in the cases of the railroads, reduce the percentage of stationary dwell time in a population area by, let's say, 75 percent. And that's all funneled under this notion if you reduce the vulnerability, that's reducing the risk because if the consequence stays the same, and the threat stays the same, you've at least -- you know, they're all multiplied by each other. So I think that we actually do use that formula.

Now, others, of course -- the states and localities -- measure things a little differently. When individuals look at risk, or individual communities look at risk, they look at their own risk. They don't trade off against somebody else's risk. So sometimes you get -- that's why you get a lot of criticism from local or state officials, because from their perspective, we're not seeing their risk, and they're not paying attention to the risk of other communities. So when we get into the big city -- you know, the urban grants -- everybody always feels they're getting too little. But we have to look at the whole menu across the board.

Question: Mr. Secretary, if I may --

Secretary Chertoff: I want to make sure everybody has a chance --

Question: The debate in Congress this week, as it's been for much of the past three months, is about the reauthorization of FISA, and the debate over -- especially from the telecom community. Can you provide any kind of categorical statement as to whether ICE agents, CBP agents, have had to drop investigations, or if there has been a loss of information about new terrorism groups since the law expired?

Secretary Chertoff: Well, unless our agents are operating through a JTTF, we don't usually have FISA coverage. You know, ICE and CBP in its normal course, it is not dealing directly with FISA. Now we may get -- you know, intelligence information may come to me that will include FISA stuff, but it's not necessarily going to be something that you could say a CBP or an ICE investigation was based on that, except insofar as part of the JTTF. Look, more generally, I think that we need to get this up and running for reasons the DNI can speak to much more specifically and authoritatively than I can.

URL

https://web.archive.org/web/20120212183120/http://www.dhs.gov/xnews/releases/pr_1204587093735.shtm

Timestamp

Thu Mar 25 2021 10:20:50 GMT-0700 (Pacific Daylight Time)

And the one issue on retroactive liability, it's just kind of a simple proposition, which I'll come to you at next as a -- in my current job, but just having been a lawyer for a long time and I've read a lot of cases. If the Court is going to find that the government has a right to do that, will not get that help in the future. And some day a President -- there's going to be an unintended thing, and a President is going to need to go to somebody in the private sector and say, "This is an emergency; help me out." And you would not want to be in the circumstance where the person says, "No, I want to have -- I'm not going to do it because I'm afraid I'm going to get sued."

That's why we have, for example -- I'll give you an example -- that's why we have such a thing as congressional immunity. Why is there a speech and debate clause that the Constitution has that allows a member of Congress to get up, if he wants, and literally defame an individual maliciously -- it could be done -- and is protected against being sued? It's because the recognition by the framers was that in order to allow the system as a whole to work, you have to tolerate the fact there may be some bad behavior, because it's important to protect the ability to make those kinds of statements.

That principle of immunity -- judges get it, prosecutors get it. I think there's a reason for that. And it does mean that sometimes, you know, someone can't be sued for something that they do that's wrong, but it's designed so that the system isn't constantly being gummed up because lawyers have to, you know, say time out, and then write opinions and, you know, people become risk-averse.

Question: Okay, just to follow up, you haven't asked -- you wouldn't normally find out whether those investigations have been halted or --

Secretary Chertoff: It would be hard for me, because I don't get a direct visibility. I get the product. I don't -- I'm not involved in the collection.

Question: I want to clarify this relationship with NSA. So you get -- in what form do you get NSA-intercept information? Then, where does it go? How do you use it?

Secretary Chertoff: If we get intelligence, we get it from all over the intelligence community. It can be in -- largely, it's analytic stuff; stuff that has been analyzed and, you know, viewed by the NCTC, or something of that sort. And if we're talking about -- let me step back.

Question: I'm talking directly -- specifically about NSA.

Secretary Chertoff: All right, so let me tell you. In terms of FISA stuff, or things of that sort, we don't operate FISA. We don't do FISA wiretaps in our department. So we do not collect any signals information under FISA or under NSA-type authorities.

All we get is product. We may get product that is incorporated in analysis, and we may not know exactly what the source of each is, or it may be generically described. In some circumstances, if it's relevant, I may get a fragment or an excerpt or a summary -- probably a summary -- of something that's intercepted through FISA or through, you know, some other type of capability.

Question: In that case, you would say, okay, this needs to go to Border Patrol.

Secretary Chertoff: In that case, depending on what it is, you know, we would say, okay -- if it suggested, for example, that there's going to be an effort to smuggle a bomb in through a container, it would cause us then to make some adjustments at the port in order to prevent this kind of thing from happening.

Question: And then would this information be labeled as coming from NSA?

Secretary Chertoff: Not necessarily.

Question: But it could be.

Secretary Chertoff: Could be.

Question: And so therefore you would have been a recipient of, and a user of, information collected by NSA without a warrant.

Secretary Chertoff: Well, it depends whether it needed a warrant or not. I mean --

Question: I'm talking about, say, with the telecoms.

Secretary Chertoff: I'm not going to speculate where it comes from. I can tell you, stuff comes from various intelligence --

Question: Well, you already said it comes from NSA.

Secretary Chertoff: Yes, but that doesn't mean it was done without a warrant. It might have been done with a warrant; it might not have been done with a warrant. It might have required a warrant --

Question: So you don't know if it was done with a warrant or not?

Secretary Chertoff: Right. I would have no visibility into what the legal requirement was, whether a warrant was obtained, whether a warrant was necessary. None of that is visible to me, or revealed to me.

Question: But you are aware --

Moderator: We're tight on time --

Question: I have to finish this --

Secretary Chertoff: I was aware of what?

Question: Were you aware that this program was ongoing with the telecom companies?

Secretary Chertoff: I don't know what program you're talking about.

Question: I'm talking about harvesting information --

Secretary Chertoff: I'm not -- but you see, you're assuming stuff you've read in the paper.

Question: I'm not. I'm asking you for information.

Secretary Chertoff: I'm telling you I have received -- we get information from the intelligence community. It can be collected from a variety of sources. I don't know which program it comes under. I don't know whether it's got a warrant or doesn't have a warrant. I don't know whether it's collected -- I mean, as soon as I can contextually tell where it's collected or not collected.

So I don't know if it's under this program or that program. None of that is known to me. All I know is, incorporated in the massive intelligence we get is all these different streams of intelligence, which help us decide whether we need to do something to protect the country or not. I can't verify your assumptions concerning whether something was under this program or that program. I have no basis to accept your characterization of harvesting, which doesn't strike me as having any legal significance.

So there's a whole bunch of assumptions I want to be clear I'm not buying into. I'm only telling you we had to try --

Moderator: We've got to go to the last question, I'm sorry.

Secretary Chertoff: No. Finish the thing.

Question: Well, you're redefining what I'm saying. I'm not making any assumptions whatsoever.

Secretary Chertoff: I'm only telling you, we get --

Question: The administration, as far as I know, has conceded that information was gathered from wiretaps on telephone companies. Otherwise, why would they be asking for immunity for these companies, right?

URL

https://web.archive.org/web/20120212183120/http://www.dhs.gov/xnews/releases/pr_1204587093735.shtm

Timestamp

Thu Mar 25 2021 10:21:46 GMT-0700 (Pacific Daylight Time)

Question: Well, you already said it comes from NSA.

Secretary Chertoff: Yes, but that doesn't mean it was done without a warrant. It might have been done with a warrant. It might not have been done with a warrant. It might have required a warrant --

Question: So you don't know if it was done with a warrant or not?

Secretary Chertoff: Right. I would have no visibility into what the legal requirement was, whether a warrant was obtained, whether a warrant was necessary. None of that is visible to me, or revealed to me.

Question: But you are aware --

Moderator: We're tight on time --

Question: I have to finish this --

Secretary Chertoff: I was aware of what?

Question: Were you aware that this program was ongoing with the telecom companies?

Secretary Chertoff: I don't know what program you're talking about.

Question: I'm talking about harvesting information --

Secretary Chertoff: I'm not -- but you see, you're assuming stuff you've read in the paper.

Question: I'm not. I'm asking you for information.

Secretary Chertoff: I'm telling you I have received -- we get information from the intelligence community. It can be collected from a variety of sources. I don't know which program it comes under. I don't know whether it's got a warrant or doesn't have a warrant. I don't know whether it's collected -- I mean, as soon as I can contextually tell where it's collected or not collected.

So I don't know if it's under this program or that program. None of that is known to me. All I know is, incorporated in the massive intelligence we get is all these different streams of intelligence, which help us decide whether we need to do something to protect the country or not. I can't verify your assumptions concerning whether something was under this program or that program. I have no basis to accept your characterization of harvesting, which doesn't strike me as having any legal significance.

So there's a whole bunch of assumptions I want to be clear I'm not buying into. I'm only telling you we had to try --

Moderator: We've got to go to the last question, I'm sorry.

Secretary Chertoff: No. Finish the thing.

Question: Well, you're redefining what I'm saying. I'm not making any assumptions whatsoever.

Secretary Chertoff: I'm only telling you, we get --

Question: The administration, as far as I know, has conceded that information was gathered from wiretaps on telephone companies. Otherwise, why would they be asking for immunity for these companies, right?

Secretary Chertoff: I would not necessarily know --

Question: So if you have -- if you received NSA information -- I'm merely asking if you received information during this time period from NSA -- like you said, we get a bit of a piece of information and we might give it to, say, border control or port security, whatever. Therefore, is it safe to assume, whether you knew it or not, that you would have gotten information from this program? Or are you saying, I don't know, I wouldn't know?

Secretary Chertoff: I don't know. It's not safe to assume, because I don't know. Because I - - because it doesn't come labeled as the particular source. So it would be a guess.

Question: One of the things that I'm curious about is, we're talking about airlines, who's getting on the planes, and so forth. To what extent do you think that it might actually be more efficient to, say, have security on these airlines being dealt with by the companies themselves that run the airlines rather than have it centralized under Homeland Security?

Secretary Chertoff: So that private companies would have all the intelligence and would use it for commercial purposes?

Question: No, no, no, I'm talking about screening passengers as they're getting onto the plane; I'm talking about that. I'm talking about, like, looking at the --

Secretary Chertoff: Well, here's the deal. We tried the private sector screening approach and the company that did it was indicted once, and then when I was head of the criminal division, we indicted them a second time because they hadn't learned the lesson from the first time. So, fool me once, shame on you; fool me twice, shame on you; fool me three times, shame on me.

Question: Wow, you got that right.

Secretary Chertoff: I don't think there's any reason to -- that we even want to entrust -- I mean, they do -- they're certainly welcome and should do screening themselves, for their own purposes, but in terms of deciding who should be admitted into the country and screening for purposes of knowing whether someone is --

Question: That's not what I'm talking about.

Secretary Chertoff: Well, what are you talking about?

Question: I'm talking about getting onto the plane.

Secretary Chertoff: You mean instead of TSA?

Question: Yes.

Secretary Chertoff: I have no reason to believe that the airline -- first of all, the airlines were never in that business, nor do I think they want to be in that business. There were private companies that were in the business that did a woefully poor job prior to 9/11. And we have actually offered the private sector the option of doing private companies in some airports, and, frankly, there's been very little interest. They do it in a couple of airports; I think San Francisco does it. It is not -- there's not been a widespread clamor to do it.

Question: Do you think that that's because they think that the government is better at it or do you think that they're just trying to avoid getting any blame in case something happens?

Secretary Chertoff: I'm sure the latter. I expect that the latter as is probably -- it's not a moneymaker for them. It's not a big -- and nor is it, frankly, to be honest, part of their core expertise, so I can't -- I'm not blaming them, but it's not -- I'm sure if it was -- but I'm sure liability issues play a role in it. There's probably a whole lot of things.

All right, thanks a lot.

###

This page was last reviewed/modified on March 3, 2008.

URL

https://web.archive.org/web/20120212183120/http://www.dhs.gov/xnews/releases/pr_1204587093735.shtm

Timestamp

Thu Mar 25 2021 10:22:23 GMT-0700 (Pacific Daylight Time)

EXHIBIT 72
FILED UNDER SEAL

EXHIBIT 73
FILED UNDER SEAL

EXHIBIT 74

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 75

Abdiqafar Aden WAGAFE

DS# 1-13 [REDACTED]

Case Summary

A#: A [REDACTED]
 Name: [REDACTED]
 DOB: [REDACTED]
 POB: Somalia
 COC: Somalia
 COA: RE6
 Address: [REDACTED]
 SS#: [REDACTED]
 Jurisdiction: Seattle, WA
 Application: N-400, NBC [REDACTED]
 Filing Date: November 8, 2013
 Interview Date: None yet

Timeline

08/24/2006	I-590 approved	(a)(j)(2)
05/24/2007	Entry to US as Refugee	
05/28/2008	I-485 filed	(b)(7)(e)
11/03/2008	I-485 approved (RE6)	
07/03/2012	First N-400 filed	
09/21/2012	[REDACTED] response from FBI Name Check	
10/29/2012	Initial N-400 interview conducted; UUE/UWE result	
01/03/2013	Second/Re-ex on N-400; UUE/UWE result	
11/08/2013	Second N-400 filed	
12/08/2013	[REDACTED] from FBI Name Check	

Family:

Single/Never Married; No children

Travel

Claims none. ATSP indicates no travel since refugee admission on 5/24/2007.

Criminal History

None claimed and FBI check came back [REDACTED] on 08/03/2012 again on 12/18/2013

National Security Concerns

Unknown at this time. LHM was reviewed

Completed Actions

04/19/2014 Completed Checks of TECS, Accurint, ATSP, CLAIMS, NLETS by prior CARRP Officer

06/23/2014 Completed checks of TECS and ATSP; LHM reviewed.

FOR OFFICIAL USE ONLY (FOUO)

LAW ENFORCEMENT SENSITIVE

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator

[REDACTED]

DS# 1-13

[REDACTED]

Eligibility Assessment

(a)(J)(Z)

There is no other derogatory information in the file apart from the subject's [REDACTED] name check response. Review of the subject's file does not indicate any current grounds for denial.

Plan of Action

[REDACTED]

(b)(7)(c)

(a)(k)(2)

(b)(7)(e)

**FOR OFFICIAL USE ONLY (FOUO)
LAW ENFORCEMENT SENSITIVE**

This document is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator

(b)(7)(e)

(b)(7)(c)

Case Summary

[Redacted]

A#: [Redacted]
 FDNS-DS# 1-134 [Redacted]
 Name: [Redacted]
 DOB: [Redacted]
 POB: Somalia
 COC: Somalia
 Pending App. N-400, NBC [Redacted]
 Address: [Redacted]
 SS#: [Redacted]

Timeline

08/04/2006 I-590 approved
 05/24/2007 Entry to U.S. as Refugee
 05/28/2008 I-485 filed
 11/03/2008 I-485 approved (RE6)
 07/03/2012 N-400, Application for Naturalization filed
 10/29/2012 Initial N-400 interview resulting in UUE/UWE
 01/03/2013 Second N-400 interview resulting in UUE/UWE
 01/09/2013 N-400 Denied for UUE/UWE
 11/08/2013 Second N-400 filed

Travel History

Claims no travel. No travel found during systems checks.

National Security Issues

Unknown at this time. Need to have HSDN LHM pulled. As of this date, April 9, 2014, nobody is available to pull the information.

Criminal History

(b)(7)(e)

No criminal history claimed and FBI check for criminal history is [Redacted]

Systems Checks Completed on 04/09/2014

TECS, Accurant, ATSP, AR11, CLAIMS, NLETS, Google on name and address, (a)(j)(2)

Eligibility Assessment

Address histories on N400 match those in systems checks. AR11s were not filed. No derogatory information found in systems checks and file review other than [Redacted] name check response. Applicant appears eligible absent confirmation of NS issues. Nothing was found that would deem the applicant ineligible for Naturalization at this time. However, he has been denied before for not understanding English and being unable write in English. Will forward case for external vetting and based on results will have additional information that will help with adjudication.

EXHIBIT 76

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 77

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 78

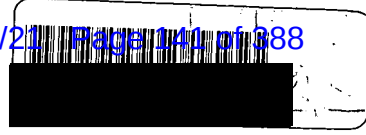
Filed Pursuant to
General Order
No. 03-21

EXHIBIT 79
FILED UNDER SEAL

EXHIBIT 80

COMPLAINTE T21E12-3949
NBC EXC60 A. 29-13

NF	✓	FCO	Date	Initials
		N5C	9-16-08	NE4012
VERIF	✓	N5C	9-16-08	NE1005
CONS A#		FCO	Date	Initials
19		10005	5/19/08	N5C 10/13/08
				NE 3/10



NBC*003782715

LOCATION: NRC
 FILE ROOM NUMBER: 1 UL D
 ROW: BD SHELF 3578 - BD3578
 SEND TO: NRC National Records Center
 System Area
 External Requests
 ALIEN NAME: JIHAD, MUSHTAQ
 PRIORITY:
 P/A: N400
 REQ. DATE: 7/11/2013
 PRINT DATE: 7/11/2013
 1 of 1

VISUAL VERIFICATION

SUMMARY VIEW

(a)(k)(2)

(b)(7)(e)

IDENTITY SUMMARY >>> FIN: 1077740794 | NAME: LNU, FNU



DOB	Country of Birth	Citizenship
[REDACTED]		

Gender	Race
U	

Person Ids
NUIN27737707
FBI [REDACTED]
A [REDACTED]
SOC [REDACTED]

Encounter Summary	
Agency	Number of Encounters
DOJ.TSC.INAX	1
DOJ.FBI	1
DOD	1
DHS.CIS.ASC	2
DHS.CBP.SAR	1
DHS.CIS.REFUGEE	1

IDENTITY DETAILS VIEW

02/05/2016 DOJ TSC INAX >>> FIN: 1077740794 | EID: 3481829208 | NAME: LNU, FNU

BIO DATA

(a)(k)(2)

(b)(7)(e)

EID 3481829208



FIN 1077740794

NAME		
LNU, FNU		
DOB	Country of Birth	Citizenship
[REDACTED]		
Gender	Race	Height (ins.)
U		
Weight (lbs)	Eye Color	Hair Color

Person ID Type / ID

NUIN / 27737707

ENCOUNTER DETAILS

DEROGATORY DATA		
Source	Type	Entry Date
	TSC-KST-A	February 05, 2016 13:33:15 EST
(a)(k)(2)	COMMENT	(b)(7)(e) (b)(7)(c)
[REDACTED]		

TRANSACTION DATA				
Date Finger Printed	Site Code	Terminal ID	Date Loaded	Reason Finger Printed
July 26, 2013 00:00:00 EST	TSC		February 05, 2016 13:33:34 EST	TSC INAX ENROLLMENT

11/03/2014 DOJ FBI >>> FIN: 1077740794 | EID: 2863051399

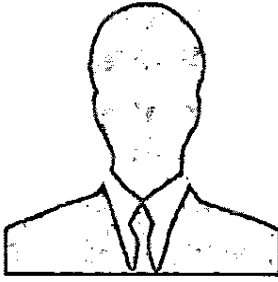
NAME: ALRUKABI, MUSHTAQ



(a)(k)(2)

(b)(7)(e)

BIO DATA

EID 2863051399	NAME		Person ID Type / ID
	ALRUKABI, MUSHTAQ		FBI / [REDACTED]
	DOB	Country of Birth	Citizenship
FIN 1077740794	[REDACTED]		
Gender	Race	Height (ins.)	
M			
Weight (lbs)	Eye Color	Hair Color	

ENCOUNTER DETAILS

DEROGATORY DATA

Source	Type	Entry Date
	FBI-FNU	November 03, 2014 12:34:10 EST

COMMENT

FNU = [REDACTED]

TRANSACTION DATA

Date Finger Printed	Site Code	Terminal ID	Date Loaded	Reason Finger Printed
November 03, 2014 12:34:10 EST	CIMS		November 03, 2014 12:34:12 EST	CJIS SEARCH OF US-VISIT

08/28/2014 DOD >>> FIN: 1077740794 | EID: 2787448591 |
NAME: JIHAD, MUSHTAQ

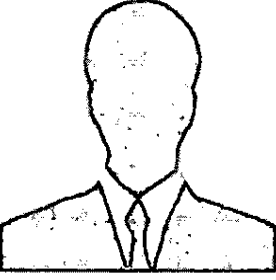


BIO DATA



(a)(k)(2) (b)(7)(e)

EID 2787448591



FIN 1077740794

NAME		
JIHAD, MUSHTAQ		
DOB	Country of Birth	Citizenship
[REDACTED]	XX	
Gender	Race	Height (ins.)
M	U	60
Weight (lbs)	Eye Color	Hair Color
0	XXX	XXX

ENCOUNTER DETAILS

DEROGATORY DATA

Source	Type	Entry Date
	DOD-LO	August 28, 2014 02:00:00 EST

COMMENTS (a)(k)(2) (b)(7)(c) (b)(7)(e)



TRANSACTION DATA

Date Finger Printed	Site Code	Terminal ID	Date Loaded	Reason Finger Printed
August 28, 2014 02:00:00 EST	UNK		August 28, 2014 15:08:48 EST	DOD OM-TICKET-3208 [REDACTED]




(a)(k)(2) (b)(7)(e)

- 07/26/2013 DHS CIS ASC >>> FIN: 1077740794 | EID:
2369346923 | NAME: JIHAD, MUSHTAQ

DEROGATORY STATUS:
NONE

Collect Biometrics

BIO DATA

EID 2369346923		NAME		Person ID Type / ID	
		JIHAD, MUSHTAQ		A / [REDACTED]	
		DOB	Country of Birth	Citizenship	
FIN 1077740794		[REDACTED]	IQ	IRQ	
Gender	Race	Height (ins.)			
M	W	69			
Weight (lbs)	Eye Color	Hair Color			
110	BRO	BRO			

ENCOUNTER DETAILS

TRANSACTION DATA

Date Finger Printed	Site Code	Terminal ID	Date Loaded	Reason Finger Printed
July 26, 2013 00:00:00 EST	XSH	02	July 26, 2013 21:36:02 EST	N400

- 11/03/2009 DHS CIS ASC >>> FIN: 1077740794 | EID:
1375834406 | NAME: JIHAD, MUSHTAQ

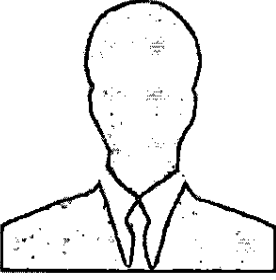
DEROGATORY STATUS:
NONE

Collect Biometrics

BIO DATA

(a)(k)(2) (b)(7)(e)



EID 1375834406		NAME		Person ID Type / ID	
		JIHAD, MUSHTAQ		A / [REDACTED]	
		DOB	Country of Birth	Citizenship	
FIN 1077740794		[REDACTED]	IQ	IRQ	
Gender		Race		Height (ins.)	
M		W		509	
Weight (lbs)		Eye Color		Hair Color	
110		BRO		BLK	

- ENCOUNTER DETAILS

TRANSACTION DATA

Date Finger Printed	Site Code	Terminal ID	Date Loaded	Reason Finger Printed
November 03, 2009 00:00:00 EST	XSH	01	November 04, 2009 02:46:17 EST	I485


- 09/10/2008 DHS CBP SAR >>> FIN: 1077740794 | EID: 75903164 DEROGATORY STATUS: NONE
 | NAME: JIHAD, MUSHTAQ ABED

BIO DATA

(a)(k)(2) (b)(7)(e)



EID 75903164



FIN 1077740794

NAME		
JIHAD, MUSHTAQ ABED		
DOB	Country of Birth	Citizenship
[REDACTED]	[REDACTED]	[REDACTED]
Gender	Race	Height (ins.)
M		
Weight (lbs)	Eye Color	Hair Color

- ENCOUNTER DETAILS

COMMENTS

NOTE: COMMENT TEXT MAY BE INCOMPLETE. REFER TO ENFORCE EVENT ID# CHI0809000930 FOR DETAILS. REFUGEE [REDACTED]

TRANSACTION DATA

Date Finger Printed	Site Code	Terminal ID	Date Loaded	Reason Finger Printed
September 10, 2008 20:33:02 EST	CHX	CBCHX826	September 10, 2008 20:32:17 EST	

- 07/07/2008 DHS CIS REFUGEE >>> FIN: 1077740794 | EID: 1203244265 | NAME: JIHAD, MUSHTAQ DEROGATORY STATUS: NONE

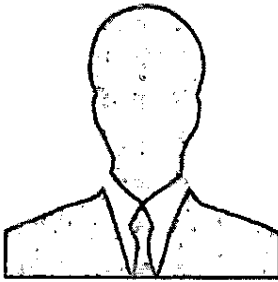
Information related to refugee claim, including the fact that a person applied for refugee status, cannot be released to 3rd parties without the written consent of the applicant except as provided in 8 CFR 208.6.

Collect Biometrics

BIO DATA

(a)(k)(2) (b)(7)(e)



EID 1203244265	NAME		Person ID Type / ID
	JIHAD, MUSHTAQ		A / [REDACTED]
	DOB	Country of Birth	Citizenship
FIN 1077740794	[REDACTED]	IQ	IRQ
Gender	Race	Height (ins.)	
M	W	508	
Weight (lbs)	Eye Color	Hair Color	
115	BRO	GRY	

ENCOUNTER DETAILS

TRANSACTION DATA

Date Finger Printed	Site Code	Terminal ID	Date Loaded	Reason Finger Printed
June 23, 2008 00:00:00 EST	REF	01	July 07, 2008 23:21:13 EST	R590

[Back to Search Panel](#)
[Collapse All](#)
[Expand All](#)

Welcome to the Customer Profile Management System (CPMS) Identity Verification Tool (IVT) Version: USCIS CPMS 6.1
 To request a User ID or if you have any difficulty accessing your account, please contact the USCIS Service Desk at 888-220-5228 or submit your request/issue with myIT (<http://oit.uscis.dhs.gov/MyIT>)
 Accessibility Statement

(a)(k)(2) (b)(7)(e)



EXHIBIT 81

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 82

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 83
FILED UNDER SEAL

EXHIBIT 84

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 85

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 86

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 87

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 88

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 89

Filed Pursuant to
General Order
No. 03-21

EXHIBIT 90
FILED UNDER SEAL

EXHIBIT 91
FILED UNDER SEAL

EXHIBIT 92

GAO

Report to Congressional Requesters

September 2006

TERRORIST WATCH LIST SCREENING

Efforts to Help Reduce Adverse Effects on the Public



September 2006



Highlights of [GAO-06-1031](#), a report to congressional requesters

Why GAO Did This Study

A consolidated watch list managed by the FBI's Terrorist Screening Center (TSC) contains the names of known or suspected terrorists, both international and domestic. Various agencies whose missions require screening for links to terrorism use watch list records. For example, U.S. Customs and Border Protection (CBP) screens travelers at ports of entry. **Because screening is based on names, it can result in misidentifications when persons not on the list have a name that resembles one on the list. Also, some names may be mistakenly included on the watch list.** In either case, individuals can be negatively affected and may express concerns or seek agency action, or redress, to prevent future occurrences. This report addresses: (1) the extent to which the numbers of misidentified persons are known and how they could be affected, (2) the major reasons misidentifications occur and the actions agencies are taking to reduce them or minimize their effects, and (3) the opportunities for redress available to individuals with watch list-related concerns. In conducting work at TSC and the principal federal agencies that use watch list data, GAO reviewed standard operating procedures and other relevant documentation and interviewed responsible officials.

GAO makes no recommendations at this time because the agencies have ongoing initiatives to improve data quality, reduce the number of misidentifications or mitigate their effects, and enhance redress efforts.

www.gao.gov/cgi-bin/getrpt?GAO-06-1031.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Eileen Larence at (202) 512-8777 or larencee@gao.gov.

TERRORIST WATCH LIST SCREENING

Efforts to Help Reduce Adverse Effects on the Public

What GAO Found

Annually, millions of individuals—from international travelers to visa applicants—are screened for terrorism links against the watch list. At times, a person is misidentified because of name similarities, although the exact number is unknown. In some cases, agencies can verify the person is not a match by comparing birth dates or other data with watch list records, but agencies do not track the number. In other cases, they ask TSC for help. **From December 2003 (when TSC began operations) to January 2006, agencies sent tens of thousands of names to TSC, and about half were misidentifications, according to TSC.** While the total number of people misidentified may be substantial, it likely represents a fraction of all people screened. Even so, misidentifications can lead to delays, intensive questioning and searches, missed flights, or denied entry at the border.

Misidentifications most commonly occur with names that are identical or similar to names on the watch list. To rapidly screen names against the watch list, agencies use computerized programs that account for differences due to misspellings and other variations. TSC has ongoing initiatives to improve computerized matching programs and the quality of watch list records. Also, CBP and the Transportation Security Administration (TSA) have established procedures designed to expedite frequently misidentified persons through screening, after confirming they are not on the watch list.

Because security measures regrettably may cause personal inconveniences, TSA and CBP, with the support of TSC, provide opportunities for people who have been misidentified or mistakenly included on the watch list to seek redress. Most of these are misidentified persons who are not on the watch list but have a similar name and, therefore, may be repeatedly misidentified. Thus, TSA, for example, provides redress that relies heavily on efforts to expedite frequently misidentified persons through screening by allowing them to submit personal information that helps airlines more quickly determine that they are not on the watch list. If TSA and CBP cannot resolve questions from the public, they ask TSC for help. For 2005, TSC reported that it processed to completion 112 redress referrals and removed the names of 31 mistakenly listed persons from the watch list. To ensure that opportunities for redress are formally documented across agencies and that responsibilities are clear, the Justice Department is leading an effort to develop an interagency memorandum of understanding and expects a final draft to be ready for approval by fall 2006. TSC and frontline-screening-agency officials recognize that, after the agreement is finalized, the public needs to clearly understand how to express concerns and seek relief if negatively affected by screening. So, these officials have committed to making updated information on redress publicly available.

GAO provided a draft copy of this report to the departments of Justice, Homeland Security, and State. They provided technical clarifications that GAO incorporated where appropriate.

Contents

<hr/>	
Letter	1
Results in Brief	4
Background	6
Although Likely a Small Percentage of All People Screened, the Thousands of Persons Misidentified to the Terrorist Watch List Can Experience Additional Questioning, Delays, and Other Effects	12
Most Misidentifications Occur Because of Similarities to Names on the Terrorist Watch List; Agencies Are Attempting to Reduce the Incidence of Misidentifications or Otherwise Facilitate Individuals through the Screening Process	19
The Terrorist Screening Center and Frontline-Screening Agencies Are Addressing Concerns Related to Watch List Screening, and an Interagency Agreement Is Being Developed to Further Ensure an Effective Means for Seeking Redress	27
Concluding Observations	42
Agency Comments	44
<hr/>	
Appendix I	Objectives, Scope, and Methodology
	47
Objectives	47
Scope and Methodology	47
Data Reliability	54
<hr/>	
Appendix II	Terrorist Screening Center Terrorist-Watch-List Redress Process
	55
<hr/>	
Appendix III	Transportation Security Administration Traveler Identity Verification Program
	61
Exhibit A: "Our Traveler Identity Verification Program"	61
Exhibit B: Traveler Identity Verification (TSA Form 2301, May 2006)	64
<hr/>	
Appendix IV	U.S. Customs and Border Protection Online Information
	66
Background and Preliminary Observation	66
Interagency Border Inspection System Fact Sheet	66

Appendix V	Comments from the Department of Homeland Security	68
Appendix VI	Comments from the State Department	71
Tables		
	Table 1: Number and Disposition of Redress Queries Referred to the Terrorist Screening Center, Calendar Year 2005	32
	Table 2: U.S. Customs and Border Protection Ports of Entry Visited by GAO	48
Figures		
	Figure 1: General Overview of the Name-Matching Process Used to Screen Individuals against the Terrorist Watch List	11
	Figure 2: General Overview of the Terrorist Screening Center's Process for Handling Concerns Involving Watch-List-Related Screening	30

Abbreviations

CBP	U.S. Customs and Border Protection
FBI	Federal Bureau of Investigation
IAFIS	Integrated Automated Fingerprint Identification System
IDENT	Automated Biometrics Identification System
IBIS	Interagency Border Inspection System
RFID	radio frequency identification
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

September 29, 2006

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
House of Representatives

The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

To identify individuals with known or potential links to terrorism, since the tragedies of September 11, 2001, agencies such as the departments of State, Justice, and Homeland Security have implemented enhanced procedures to screen international travelers, airline passengers, and visa applicants. One important homeland security tool used by these federal frontline-screening agencies is the terrorist-screening database, otherwise known as the consolidated watch list, containing the names of individuals with known and suspected links to terrorism. The database, which contains names of foreign and U.S. citizens, is maintained by the Terrorist Screening Center, an entity that has been operational since December 2003 under the administration of the Federal Bureau of Investigation (FBI). Based upon agency-specific policies and criteria, relevant portions of the Terrorist Screening Center's consolidated watch list can be used in a wide range of security-related screening procedures. For instance, the Transportation Security Administration's No Fly and Selectee lists—used by airlines to screen passengers prior to boarding—are portions of the Terrorist Screening Center's consolidated watch list.¹ Also, to help ensure that known or suspected terrorists do not enter the United States, applicable portions of the watch list are to be checked by Department of State consular officers before issuing U.S. visas and by U.S. Customs and

¹According to the Transportation Security Administration, persons on the No Fly list should be precluded from boarding an aircraft bound for, or departing from, the United States. In contrast, being on the Selectee list does not mean that the individual will be precluded from boarding a plane or entering the United States. Instead, any person on the Selectee list is to receive additional screening, which may involve a physical inspection of the person and a hand-search of luggage.

Border Protection officers before admitting persons at air, land, and sea ports of entry.

Because terrorist watch list screening involves comparisons based on personal-identifying information such as names and dates of birth, there is potential to generate misidentifications—given that two or more persons, for example, may have the same or similar names.² As such, the screening inevitably can raise concerns from individuals who assert that they are being misidentified because of a name similarity to some other person whose name is on the watch list. Misidentifications can result in travel delays and other inconveniences for the respective individuals. Specific instances have been widely reported in newspapers and other media, including cases involving members of Congress and other high-profile individuals. Misidentifications highlight the importance of having a process—often referred to as redress—for affected persons to express their concerns, seek correction of any inaccurate data, and request other actions to reduce or eliminate future inconveniences.³ Similarly, such a process would apply to other persons affected by the maintenance of watch list data, including persons whose names are actually on the watch list but should not be (“mistakenly listed persons”) as well as persons who are properly listed.⁴ Accordingly, in reference to terrorist watch list screening, this report addresses the following questions:

- To what extent are the numbers of terrorist watch list misidentifications known, and generally, how could misidentified persons be affected?
- What are the major reasons that misidentifications occur, and what actions are the Terrorist Screening Center and frontline-screening

²The term “misidentification” refers to a person initially matched by a screening agency to a name on the watch list, but upon closer examination, the person is found to not match any watch list record.

³As used in this report, the term “redress” generally refers to an agency’s complaint-resolution process, whereby individuals may seek resolution of their concerns about an agency action. In the report, we describe elements of the opportunities for redress offered by several agencies, and we generally analyze their respective policies and procedures. However, we do not address the relation between agency redress and other possible remedies, such as judicial review.

⁴For purposes of this report, the term “mistakenly listed persons” includes two categories of individuals—(1) persons who never should have been included on the watch list but were due to some type of error and (2) persons who were appropriately included on the watch list at one time but no longer warrant inclusion on the terrorist watch list due to subsequent events.

agencies taking to reduce the number of misidentified persons or expedite them through the screening process?

- To address concerns from misidentified and mistakenly listed persons, what opportunities for redress have the Terrorist Screening Center and frontline-screening agencies established?

In answering these questions, we reviewed the Terrorist Screening Center's standard operating procedures, statistics on watch-list-related screening encounters that resulted in referrals to the center, and other relevant documentation; and we interviewed Terrorist Screening Center officials, including the director, principal deputy director, chief information officer, and privacy officer. Similarly, we interviewed officials at and reviewed documentation obtained from the principal frontline-screening agencies—Transportation Security Administration, U.S. Customs and Border Protection, and the Department of State—whose missions most frequently and directly involve interactions with travelers.⁵ Regarding the screening of air passengers, in addition to contacting the Transportation Security Administration to broadly discuss the procedures of air carriers, we interviewed security officials at five major, domestic air carriers. Also, we visited various land and air ports of entry in four states—California, Michigan, New York, and Texas. Collectively, these states have ports of entry on both the northern and southern borders of the United States. Regarding statistical data we obtained from the Terrorist Screening Center—such as the number of misidentifications and the results of the redress process, particularly the number of mistakenly listed persons whose names have been removed from the watch list—we discussed the sources of the data with center officials, including the chief information officer, and we reviewed documentation regarding the compilation of the statistics. We determined that the statistics were sufficiently reliable for the purposes of presenting overall patterns and trends. We performed our work from April 2005 through August 2006 in accordance with generally accepted government auditing standards. Appendix I presents more details about our objectives, scope, and methodology.

⁵Although the terrorist watch list is used for a variety of screening purposes, such as conducting background checks of workers who have access to secure areas of the national transportation system, our work generally focused on the screening of travelers. At the Transportation Security Administration, we examined the screening of air passengers prior to their boarding a flight; at U.S. Customs and Border Protection, we examined the screening of travelers entering the United States through ports of entry; and at the Department of State, we examined the screening of nonimmigrant visa applicants.

Results in Brief

Although the total number of misidentifications that have occurred as a result of watch-list-related screening conducted by all frontline-screening agencies and airlines is unknown, Terrorist Screening Center data indicate that about half of the tens of thousands of potential matches sent to the center between December 2003 and January 2006 for further research turned out to be misidentifications.⁶ The frontline-screening agencies and, in the case of air travel, airlines are able use other identifying information to resolve some possible matches without Terrorist Screening Center involvement, but when the agencies are unable to do so, they are to refer the information to the center for clarification and resolution. Frontline-screening agencies and airlines generally do not have readily available statistics quantifying the number of potential matches they have been able to resolve without consulting the Terrorist Screening Center. Although the total number of misidentified persons may be substantial in absolute terms, it likely represents a small fraction of the hundreds of millions of individuals screened each year. For example, in fiscal year 2005, U.S. Customs and Border Protection alone reported that its officers managed about 431 million border crossings into the United States at land, air, and sea ports of entry. Nonetheless, misidentifications resulting from terrorist watch list screening can affect the respective individuals by, for example, delaying their travel, subjecting them to more intensive questioning and searches, and denying them conveniences such as self-serve check-in at airports. Also, in some cases, travelers have missed flights.

Misidentifications most commonly occur because the names of some persons being screened are similar to those on the terrorist watch list. The federal screening agencies we studied and most airlines use computer-driven algorithms to rapidly compare the names of individuals against the terrorist watch list.⁷ Generally, these name-recognition technologies may be designed to balance minimizing the possibility of false negatives—that is, failing to identify an individual whose name is on the terrorist watch list—while not generating an unacceptable number of false positives (misidentifications). Thus, the computerized algorithms may be configured to return a broad set of possible matches based on the name input in order

⁶According to the FBI, the specific number of potential matches sent to the Terrorist Screening Center that turned out to be misidentifications is sensitive information; however, the total is substantially less than 100,000.

⁷An algorithm is a prescribed set of well-defined, unambiguous rules or processes for the solution of a problem in a finite number of steps. Pursuant to Transportation Security Administration security directives and implementing guidance, airlines are to prescreen passengers by matching their names against the No Fly and Selectee lists.

to account, for example, for differences in names due to misspellings or transcription errors. The Terrorist Screening Center has formed an interagency working group to improve the effectiveness of identity matching across agencies, and the group's efforts were ongoing the time of our review. The center also has ongoing quality-assurance initiatives to identify and correct incomplete or inaccurate records that contribute to misidentifications. Further, agencies are taking actions to expedite frequently misidentified persons through the screening process. For example, in February 2006, U.S. Customs and Border Protection began annotating its database to help ensure that travelers who have been inadvertently stopped in the past—because they have the same or similar name as a watch list record—are no longer subjected to intensive screening, unless warranted by new data. As a future enhancement, the Terrorist Screening Center is planning to have links to other agencies' biometric data, such as fingerprints. According to center officials, the capability to link biometric data to supplement name-based screening may be more relevant for confirming the identities of known terrorists than minimizing misidentifications or false positives.

The Terrorist Screening Center, the Transportation Security Administration, and U.S. Customs and Border Protection have processes in place to help resolve concerns or complaints submitted by persons adversely affected by terrorist watch list screening.⁸ The processes are interdependent in that the frontline-screening agencies are to receive all redress queries, resolve those that, based on other identifying information, clearly involve misidentified persons, and refer the other queries to the Terrorist Screening Center—particularly queries submitted by persons whose names are actually contained on the watch list. For calendar year 2005, the center reported that it processed to completion 112 redress referrals and removed the names of 31 mistakenly listed individuals from the watch list. In contrast, the frontline-screening agencies processed thousands of redress queries. Most redress queries are submitted by misidentified persons, and their names cannot be removed from the watch list because they are not the persons on the list. Instead, some frontline-screening agencies have undertaken initiatives to expedite the future

⁸Any such concern or complaint raised formally by an affected individual is what the Terrorist Screening Center calls a redress query. Specifically, the Terrorist Screening Center defines a "redress query" as communication from individuals or their representatives inquiring or complaining about an adverse experience during a terrorist watch-list-related-screening process conducted or sponsored by a federal agency, including congressional inquiries to federal agencies on behalf of their constituents.

processing of persons who are frequently misidentified. For example, under the Transportation Security Administration's process, affected individuals can voluntarily provide additional personal-identifying information as a basis for the agency to determine whether their names can be put on a cleared list. Airlines are to use the cleared list to more quickly distinguish these individuals from persons who are on the No Fly and the Selectee lists. This procedure is intended to reduce delays in obtaining airline-boarding passes. The Terrorist Screening Center, from its unique position as administrator of the consolidated terrorist watch list, has noted significant differences among agencies in providing watch-list-related redress. For instance, whereas the Transportation Security Administration has designated an official accountable specifically for redress, U.S. Customs and Border Protection does not and also has not followed consistent procedures in referring appropriate redress queries to the Terrorist Screening Center. Thus, at the Terrorist Screening Center's request, the Department of Justice is leading an effort to develop an interagency memorandum of understanding to ensure that opportunities for redress are formally documented and that agency responsibilities are clear, with designated officials specifically accountable for supporting the continued success of watch-list-related redress. This effort, according to the Terrorist Screening Center, has been ongoing since fall 2005, and a final draft of the memorandum of understanding is expected to be ready for interagency clearances by fall 2006. The Department of Justice and the Terrorist Screening Center have acknowledged that, upon finalization of an interagency agreement that documents the redress opportunities and designates agencies' responsibilities, it is important that appropriately updated information on redress and points of contact be made available to the public, including updates of Web-based guidance.

We are not making recommendations at this time because the agencies have ongoing efforts to improve data quality and otherwise either reduce the number of misidentifications or mitigate their effects and to provide more effective redress.

Background

In April 2003, we reported that watch lists were maintained by numerous federal agencies and that the agencies did not have a consistent and uniform approach to sharing information on individuals with possible links to terrorism.⁹ Our report recommended that the Department of Homeland

⁹GAO, *Information Technology: Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing*, GAO-03-322 (Washington, D.C.: Apr. 15, 2003).

Security's Secretary, in collaboration with the heads of the departments and agencies that have and use watch lists, lead an effort to consolidate and standardize the federal government's watch list structures and policies. Subsequently, pursuant to Homeland Security Presidential Directive 6, dated September 16, 2003, the Terrorist Screening Center was established to consolidate the government's approach to terrorism screening and provide for the appropriate and lawful use of terrorist information in screening processes. The center began "24/7" operations on December 1, 2003, and, about 3 months later, on March 12, 2004, announced that watch list consolidation was completed with establishment of the terrorist-screening database. This consolidated database is the U.S. government's master repository for all known and suspected international and domestic terrorist records used for watch-list-related screening. Records for inclusion in the consolidated database are submitted to the Terrorist Screening Center from the following two sources:

- Identifying information on individuals with possible international terrorism ties is provided through the National Counterterrorism Center, which is managed by the Office of the Director of National Intelligence.
- Identifying information on individuals with ties to purely domestic terrorism, such as Ted Kaczynski (the "Unabomber"), is provided by the FBI.

In their terrorist-screening processes, the three federal frontline-screening agencies that we reviewed use records exported by the Terrorist Screening Center. That is, the applicable exported records are incorporated, respectively, into the Transportation Security Administration's No Fly and Selectee lists, U.S. Customs and Border Inspection's Interagency Border Inspection System, and the State Department's Consular Lookout and Support System. The following listing discusses the frontline-screening agencies' use of watch list records more specifically:

- **Transportation Security Administration's No Fly and Selectee Lists:** As needed, the Transportation Security Administration provides updated No Fly and Selectee lists to airlines for use in prescreening passengers. Through the issuance of security directives, the agency requires that airlines use these lists to screen passengers prior to boarding. The agency's Office of Intelligence (formerly called the Transportation

Security Intelligence Service) provides assistance to airlines in determining whether passengers are a match with persons on the lists.¹⁰

- **U.S. Customs and Border Protection’s Interagency Border Inspection System:** U.S. Customs and Border Protection officers use the Interagency Border Inspection System to screen travelers entering the United States at ports of entry, which include land border crossings along the Canadian and Mexican borders, sea ports, and U.S. airports for international flight arrivals. This system includes not only the applicable records exported by the Terrorist Screening Center, but also additional information on people with prior criminal histories, immigration violations, or other activities of concern that U.S. Customs and Border Protection wants to identify and screen at ports of entry.
- **State Department’s Consular Lookout and Support System:** This system is the primary sensitive but unclassified database used by consular officers abroad to screen the names of visa applicants to identify terrorists and other aliens who are potentially ineligible for visas based on criminal histories or other reasons specified by federal statute. According to the State Department, all visa-issuing posts have direct access to the system and must use it to check each applicant’s name before issuing a visa.

Also, the Terrorist Screening Center makes applicable records in the consolidated database available to support the terrorist-screening activities of other federal agencies—such as U.S. Immigration and Customs Enforcement, which is the largest investigative component of the Department of Homeland Security—as well as state and local law enforcement agencies. For example, the FBI’s National Crime Information Center has a file—the Violent Gang and Terrorist Organization File—which is accessible by federal, state, and local law enforcement officers for screening in conjunction with arrests, detentions, or other criminal

¹⁰The Transportation Security Administration is developing a new passenger prescreening program, known as Secure Flight. Under the Secure Flight program, the agency plans to take over, from commercial airlines, the responsibility to compare identifying information on airline passengers against information on known or suspected terrorists. The agency expects that Secure Flight will improve passenger prescreening as compared with the current airline-operated process. In June 2006, we reported that the Transportation Security Administration still faces significant challenges in developing and implementing the Secure Flight program. See, GAO, *Aviation Security: Management Challenges Remain for the Transportation Security Administration’s Secure Flight Program*, GAO-06-864T (Washington, D.C.: June 14, 2006).

justice purposes.¹¹ A subset of this file consists of the Terrorist Screening Center's records to be used to screen for possible terrorist links.

Figure 1 presents a general overview of the name-matching process typically used by frontline-screening agencies and airlines to screen individuals against applicable records exported by the Terrorist Screening Center, which has an important role in verifying identities. When the computerized name-matching system of a frontline-screening agency or, in the case of air travel, an airline generates a "hit" (a potential name match) against a terrorist database record, the agency or airline is to review each potential name-match. Any obvious mismatches (misidentifications) are to be resolved by the frontline agency or airline.

Conversely, clearly positive or exact matches generally are to be referred to the applicable screening agency's intelligence center and to the Terrorist Screening Center to provide law enforcement an opportunity for a counterterrorism response.¹² Similarly, hits involving inconclusive matches—that is, uncertain and other hard-to-verify potential matches—typically are to be referred to the applicable screening agency's intelligence center. In turn, if the intelligence center cannot conclusively determine whether a hit is an exact match, the Terrorist Screening Center is to be contacted.¹³ Referring inconclusive matches to the Terrorist Screening Center for resolution or confirmation is important because the possible consequences of not identifying a known or suspected terrorist could be worse than the inconveniences associated with

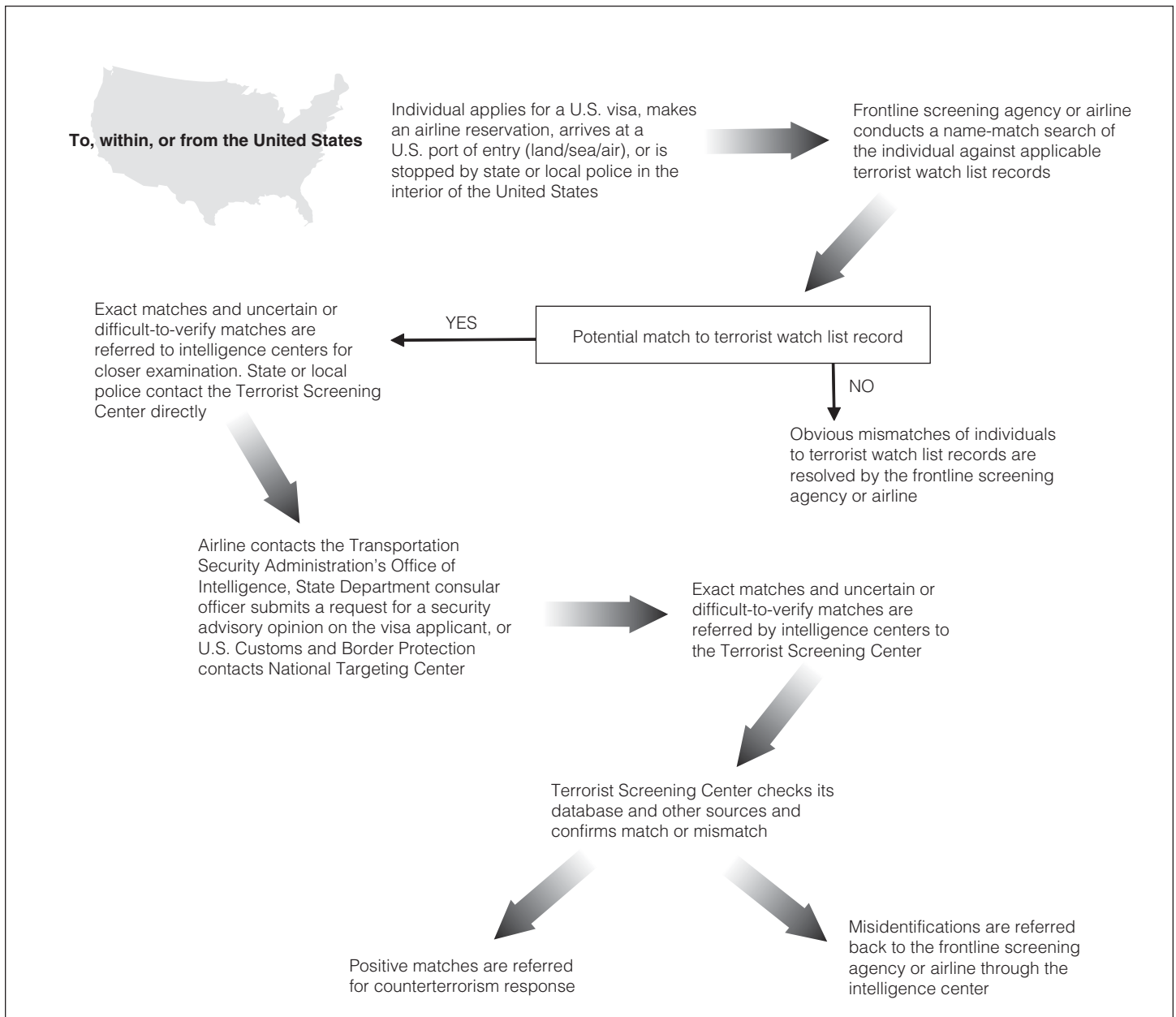
¹¹Also, the FBI and designated state and local criminal justice agencies access the Violent Gang and Terrorist Organization File in conducting background checks on individuals seeking to purchase firearms or obtain permits to possess, acquire, or carry firearms. See GAO, *Gun Control and Terrorism: FBI Could Better Manage Firearm-Related Background Checks Involving Terrorist Watch List Records*, GAO-05-127 (Washington, D.C.: Jan. 19, 2005).

¹²Airlines are to contact the Transportation Security Administration, which may then contact the Terrorist Screening Center, as necessary.

¹³In commenting on a draft of this report, the State Department noted that the general overview presented in figure 1 is not fully reflective of the process for screening nonimmigrant visa applicants against the terrorist watch list. Specifically, the department emphasized that for any hit that clearly is not a mismatch, consular officers are required to obtain a security advisory opinion. That is, the consular post must ask Department of State headquarters to initiate a process of requesting that the Terrorist Screening Center and other relevant agencies check their respective databases or systems for the existence of any investigative or intelligence information regarding the individual and pass the results back to the department for use in recommending a course of action to the post.

misidentifications. In conducting its research, the Terrorist Screening Center has access to classified data systems that may contain additional information not available to the referring agency. Once the Terrorist Screening Center has confirmed the individual as either a positive match or a misidentification, the frontline-screening agency is to be informed.

Figure 1: General Overview of the Name-Matching Process Used to Screen Individuals against the Terrorist Watch List



Source: GAO.

Homeland security-related screening processes entail some level of inconvenience for all travelers. Also, in an operational context, people can be and frequently are screened for reasons not related to the terrorist watch list but rather for reasons related to an agency's mission. For example, U.S. Customs and Border Protection screens travelers for any conditions that may make them inadmissible to the country, including past violations of immigration, drug, customs, or other laws. The agency also randomly selects certain individuals for more thorough screening. Similarly, prospective airline passengers may be randomly selected for additional screening, and others may be selected if they exhibit unusual behavior.¹⁴ Generally, screening agencies and airlines are not to disclose the reason they select an individual for more thorough screening measures, so persons may mistakenly assume it is because they are on a terrorist watch list.

Although Likely a Small Percentage of All People Screened, the Thousands of Persons Misidentified to the Terrorist Watch List Can Experience Additional Questioning, Delays, and Other Effects

Annually, hundreds of millions of individuals—international travelers, airline passengers, and visa applicants—are screened against relevant portions of the Terrorist Screening Center's consolidated watch list. The number of persons misidentified during terrorist watch list screening may be substantial in absolute terms but likely represents a small fraction of the total screenings. Nonetheless, misidentifications resulting from terrorist watch list screening can affect the respective individuals in various ways, with perhaps the most common situation involving delays and related inconveniences experienced by travelers.

¹⁴Since the late 1990s, airline passenger prescreening has been conducted using the Computer-Assisted Passenger Prescreening System (CAPPS I)—in which data related to a passenger's reservation and travel itinerary are compared against characteristics (known as CAPPS I rules) used to select passengers who require additional scrutiny—and through the matching of passenger names to terrorist watch lists. See, GAO, *Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*, GAO-05-356 (Washington, D.C.: Mar. 28, 2005), which reported that approximately 99 percent of all passengers on domestic flights are screened under the air carrier-operated, automated CAPPS I system, and the remaining 1 percent of passengers are screened by air carriers who do not have an automated system.

Although a Substantial Number, Misidentified Persons Likely Constitute a Small Percentage of All People Screened

Although the full universe of persons misidentified by terrorist watch list screening may be substantial in absolute terms, the total number likely represents a small fraction of all persons who are screened. **During the 26-month period we studied—from December 2003 (when the Terrorist Screening Center began operations) to January 2006—the center received tens of thousands of screening-encounter referrals from frontline-screening agencies and determined that approximately half involved misidentified persons with names the same as or similar to someone whose name was contained on the terrorist watch list.** The number of referrals to the Terrorist Screening Center does not constitute the universe of all persons initially misidentified by terrorist watch list screening because the names of many persons initially misidentified are not forwarded to the Terrorist Screening Center. Rather, by comparing birth dates or other data, the frontline- screening agencies (e.g., U.S. Customs and Border Protection) are able to resolve many initial misidentifications without contacting the Terrorist Screening Center. Additionally, for air passengers, the airlines often are able to resolve initial misidentifications without contacting the Transportation Security Administration.¹⁵ The screening agencies and airlines generally do not maintain readily available statistics on these resolutions.

Nonetheless, although the full universe of such misidentifications may be substantial in absolute terms, the total number likely represents a small fraction of all persons who are subject to terrorist watch list screening procedures, as in the following examples:

- U.S. Customs and Border Protection reported that its officers managed a total of 431 million border crossings into the United States at land, air, and sea ports of entry in fiscal year 2005.
- Domestic airline flights—flights within the United States—carried 658 million passengers during the 12 months ending January 2006, according to Department of Transportation statistics.¹⁶

¹⁵The Transportation Security Administration provides security directives and implementing guidance to foreign and domestic aircraft operators for use in ensuring that individuals who pose a threat to civil aviation are denied boarding passes or are subjected to additional screening, as appropriate.

¹⁶Also, terrorist-watch-list-screening procedures are applicable to international flights—of foreign and domestic air carriers—into or from the United States.

- The State Department reported that it processed about 7.4 million nonimmigrant visa applications in fiscal year 2005.¹⁷

In addition to these international travelers, domestic flight passengers, and visa applicants, any other person can be subject to terrorist watch list screening in conjunction with routine law enforcement activities. For instance, in stopping a motorist for a traffic violation, a state or local law enforcement officer can check the motorist's name against the National Crime Information Center's various files, which include terrorist watch list records exported by the Terrorist Screening Center. The National Crime Information Center, according to the FBI, is available to virtually every law enforcement agency nationwide, 24 hours a day, 365 days a year.

Misidentified Individuals Can Experience Delays and Other Effects

People who are misidentified to the terrorist watch list can be affected in various ways, most commonly experiencing delays and related inconveniences, including being subjected to more intensive questioning and searches. Generally, the extent of the effects of terrorist watch-list-related misidentification can vary by individual circumstances and the operational nature of the screening agency's mission. For example, an individual with a name similar to someone who is on the Transportation Security Administration's No Fly list likely will be unable to utilize the convenience of Internet, curbside, and airport kiosk check-in options. This effect of misidentifications is reflected in a sample of 24 complaint letters to the Transportation Security Administration that we reviewed.¹⁸ Many of the complainants described their frustrations with not being able to use alternative check-in options such as the Internet or airport kiosks. Similarly, in a survey conducted in June 2006 by the National Business Travel Association, many companies' travel managers responded that their

¹⁷A nonimmigrant is a person, not a citizen or national of the United States, seeking to enter the United States temporarily for a specific purpose, such as business or pleasure.

¹⁸As discussed in appendix I, the Transportation Security Administration provided us a selection of 24 terrorist watch-list-related complaint letters that the agency received from December 1, 2003 (when the Terrorist Screening Center became operational) to April 20, 2006. The agency attempted to select letters from different weeks throughout this time period; however, because a statistically projectable methodology was not used for the selections, the 24 letters are not representative of all complaints or inquiries (an unspecified total) that the Transportation Security Administration received during this time period.

employees have expressed frustration about repeatedly having to go to the airline ticket counter to obtain a boarding pass.¹⁹

Also, misidentifications can cause other effects, such as missed airline flights by either leisure travelers or business travelers, which could have economic and other consequences, although we found no readily available data on how frequently these effects occurred. However, according to Transportation Security Administration data, two international flights—one in December 2004 and another in May 2005—were diverted from landing at their scheduled destinations in the United States due to potential matches to the No Fly list. In each instance, following the diversions of the flights and further investigation after the airplanes landed, federal authorities determined that the respective passengers were misidentified and not true matches to the No Fly list. Nonetheless, the diversions resulted in delays and related inconveniences for all passengers on these flights.

The Transportation Security Administration has acknowledged that misidentifications can be embarrassing and time consuming for individuals and also potentially can erode the public's confidence in the agency's security efforts. Similarly, a recent Department of Homeland Security report recognized that "individuals who are mistakenly put on watch lists or who are misidentified as being on these lists can potentially face consequences ranging from inconvenience and delay to loss of liberty."²⁰

Also, an individual can experience an immediate delay at a port of entry when U.S. Customs and Border Protection's automated search of the Interagency Border Inspection System database returns a potential match to a terrorist watch list record. For such potential matches, U.S. Customs

¹⁹According to its Web site (www.nbta.org), the National Business Travel Association represents over 2,500 corporate travel managers and travel service providers who collectively manage and direct more than \$170 billion of expenditures within the business travel industry, primarily for Fortune 1,000 companies. In June 2006, the association conducted a survey of 1,316 corporate travel managers, and 444 responded to the survey. Of the responding travel managers, 107 reported that they have employees who repeatedly have had to go to the airline ticket counter to obtain a boarding pass. (Accessed August 2006.)

²⁰Department of Homeland Security, *Report on Effects on Privacy & Civil Liberties—DHS Privacy Office Report Assessing the Impact of the Automatic Selectee and No Fly Lists on Privacy and Civil Liberties as Required under Section 4012(b) of the Intelligence Reform and Terrorism Prevention Act of 2004* (Washington, D.C.: Apr. 27, 2006).

and Border Protection's operating protocol is to escort the person to another screening area for further questioning and inspection (a process referred to as secondary screening). The length of time the person spends in secondary screening can be several hours, depending partly on the difficulty or ease of verifying whether the person is or is not the individual on the watch list. In the four states we visited—California, Michigan, New York, and Texas—U.S. Customs and Border Protection officers told us that given the importance of the homeland security mission, their practice is to err on the side of caution by conducting very thorough screenings.²¹

The effects of such misidentifications and the related secondary screenings can be emotional as well as physical, as reflected in complaint letters to U.S. Customs and Border Protection. A sample of 28 complaint letters to U.S. Customs and Border Protection that we reviewed alleged a range of effects, such as experiencing travel delays, which resulted in missing airline flights and incurring additional travel costs; being subjected to extensive questioning and searches, while not being allowed to contact family members, friends, or business associates to inform them about the delays; and feeling embarrassed and frustrated.²²

The State Department's screening of nonimmigrant visa applicants against the terrorist watch list may not affect individuals in the same way as does screening by the Transportation Security Administration and U.S. Customs and Border Protection. Generally, the State Department's screening differs from other screening agencies because there is more time to search records and make decisions. According to State Department officials, the average time for processing a nonimmigrant visa application is about 2 days. However, additional processing time may be needed if initial screening of the applicant shows a possible link to terrorism—that is, the

²¹As discussed in appendix I, besides conducting work at U.S. Customs and Border Protection headquarters in Washington, D.C., we visited various land and air ports of entry in four states—California, Michigan, New York, and Texas. We judgmentally selected these four states because each has major land and air ports of entry, and the states collectively have ports of entry on both the northern and southern borders of the United States.

²²As discussed in appendix I, U.S. Customs and Border Protection provided us a selection of complaint letters submitted by 28 individuals. The dates of the 28 complaint letters encompassed an 11-month period, ranging from June 2005 to April 2006. The 28 letters were not selected based on a statistically projectable methodology. Thus, the 28 letters are not representative of the approximately 220 complaints or inquiries—regarding watch-list-related secondary screening at ports of entry—that U.S. Customs and Border Protection's Customer Satisfaction Unit received during the 11-month time period and forwarded for research to the agency's National Targeting Center.

applicant's name possibly matches that of a person whose name is on the terrorist watch list. The officials explained that this additional processing time is needed because a decision on the visa applicant cannot be made until a security advisory opinion is obtained. That is, the consular post must ask the Department of State headquarters in Washington, D.C., to initiate a process of requesting that various agencies check their respective databases or systems for the existence of any investigative or intelligence information regarding the individual and pass the results back to a central point. This interagency review process includes the FBI, the Drug Enforcement Administration, the Central Intelligence Agency, and others. According to State Department officials, visa applicants are routinely told not to buy tickets or incur other travel-related expenses until the clearance process has been completed and the application approved.

In acknowledging that the interagency review process may extend the processing time for a visa decision, the State Department provided us (in June 2006) the following contextual perspectives:

- In the last 2 years, the department and its interagency partners have worked to decrease the processing time in order to reduce the impact on the traveling public.
- Nevertheless, the department's position is that the time it takes to screen a visa applicant is a necessary part of the application procedure and, therefore, is not an adverse governmental action. At times, additional processing must be done in order to determine whether a visa applicant is eligible for a visa under the law, including for national security reasons. The additional processing is the inconvenient consequence of the proper functioning of the visa screening system.
- Moreover, the extended processing time generally is a one-time occurrence. Once an alien is cleared through the process, the clearance is noted in the department's consular visa database. Thus, this person may not be subject to the same processing delay when applying for another visa in the future, unless additional investigative or intelligence information arises after issuance of the first visa.²³

²³The extended or additional processing time is not always a one-time occurrence. In processing visa applications, consular posts may request security advisory opinions for a variety of reasons. Thus, even though an individual previously has been the subject of a security advisory opinion, a new visa application may present facts and circumstances that lead the consular post to request another security advisory opinion.

Screening by state and local law enforcement also differs from screening by the Transportation Security Administration, U.S. Customs and Border Protection, and the State Department. Essentially, federal agencies (or air carriers, as applicable) initiate screening when individuals make an airline reservation, arrive at a port of entry, or apply for a visa. In contrast, a state or local law enforcement agency may initiate screening by, for example, pulling over a motorist for speeding. Generally, a routine procedure for the law enforcement officer is to query the motorist's name against records in the National Crime Information Center, which contains criminal history records as well as terrorist watch list records. According to congressional testimony presented in March 2004 by the Director of Public Security for the State of New York, it takes about 12 to 15 minutes, on average, for a New York patrol officer to contact the Terrorist Screening Center and resolve a potential name match.²⁴ More recently, in July 2006, the Director of the Terrorist Screening Center told us that the average time nationally is now down to about 5 minutes—that is, the time period beginning with the center's receipt of the call from a state or local law enforcement officer and ending with the response to the officer regarding the potential name match.²⁵

²⁴Testimony of Mr. James W. McMahon, Director, Office of Public Security, State of New York, at a hearing before the Subcommittee on Crime, Terrorism, and Homeland Security, Committee on the Judiciary, and the Subcommittee on Intelligence and Counterterrorism of the Select Committee on Homeland Security, House of Representatives (Mar. 25, 2004).

²⁵The response to the state or local law enforcement officer may be provided by the Terrorist Screening Center or by the FBI's Counterterrorism Division (Terrorist Screening Operations Unit), as applicable.

Most Misidentifications Occur Because of Similarities to Names on the Terrorist Watch List; Agencies Are Attempting to Reduce the Incidence of Misidentifications or Otherwise Facilitate Individuals through the Screening Process

The most common cause of misidentifications is similarity of the names of persons being checked to names on the Terrorist Screening Center's consolidated watch list, for which there is no complete remedy, but agencies are taking actions to minimize the effect on frequently misidentified persons. The Terrorist Screening Center has formed an interagency group to improve the effectiveness of identity matching across agencies and also has ongoing initiatives regarding data quality. As a future enhancement, the Terrorist Screening Center's strategy is to develop the capability to link name-based watch list searches to relevant biometric systems maintained by other agencies, although this capability may be more useful for confirming positive matches than for reducing the incidence of misidentifications.

Misidentifications Result Because a Traveler's Name Is Similar to Someone with a Terrorist Watch List Record

Misidentifications occur most often because the names of some persons being screened are the same or similar to those in the consolidated terrorist watch list. To handle the large volumes of travelers and others who must be screened, federal agencies and most airlines use computer-driven algorithms to rapidly compare the names of individuals against the applicable terrorist watch list records. A primary factor in designing a computerized name-matching process is the need to minimize the possibility of generating false negatives—that is, failing to identify an individual whose name is on the terrorist watch list—without generating an unacceptable number of false positives (misidentifications). To help ensure that name-based screening does not miss detecting someone who is on the watch list, agencies and airlines may configure their algorithms in such a way that they return a broad set of possible matches for any given name input. For instance, the computerized algorithms may account for differences in names due to misspellings or transcription errors.

Operationally, for each name that is screened against the watch list, the computerized algorithm may return a list of possible matches. If applicable, screening agency or airline security personnel then review these results of possible matching records arrayed by probability scores to determine which, if any, is a positive match with the person being screened. To help ensure awareness of best practices among agencies, the Terrorist Screening Center has formed and chairs a working group—the

Federal Identity Match Search Engine Performance Standards Working Group—which met initially in December 2005.²⁶ An objective of the working group is to provide voluntary guidance for federal agencies that use identity-matching search engine technology. Essentially, the prospective guidance is intended to improve the effectiveness of identity matching across agencies by, among other means, assessing which algorithms or search engines are the most effective for screening specific types or categories of names. At the time of our review, a target date for completing the initiative to develop and provide voluntary guidance to screening agencies had not been set.

Some Misidentifications Can Result from Inaccurate or Incomplete Data

Some misidentifications can result from inaccurate or incomplete data in the consolidated terrorist watch list. Generally, the FBI and intelligence agencies are the original collectors of the information used to determine whether a given individual should be added to the terrorist watch list. The Terrorist Screening Center, in turn, is responsible for ensuring that information received from the intelligence community is accurately maintained in the consolidated watch list. One of the Terrorist Screening Center’s primary goals is to maintain accurate and complete information.

In June 2005, the Department of Justice’s Office of the Inspector General reported that its review of the Terrorist Screening Center’s consolidated watch list found several problems—such as inconsistent record counts and duplicate records, lack of data fields for some records, and unclear sources for some records.²⁷ Among other things, the Inspector General recommended that the Terrorist Screening Center develop procedures to regularly review and test the information contained in the consolidated terrorist watch list to ensure that the data are complete, accurate, and non-duplicative. The Terrorist Screening Center agreed and noted that it was taking steps to implement the recommendation. Also, the Terrorist Screening Center has quality-assurance initiatives ongoing to identify and correct troublesome records related to misidentifications.

²⁶The working group’s membership includes representatives from the departments of Homeland Security (including Transportation Security Administration and U.S. Customs and Border Protection), State, and Defense; FBI; and the intelligence community (including the National Counterterrorism Center, Central Intelligence Agency, National Security Agency, and Defense Intelligence Agency). Also, the National Institute of Standards and Technology acts as a special advisor to the working group.

²⁷Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27 (June 2005).

Moreover, the Terrorist Screening Center's director and principal deputy director stressed to us that quality of data is a high priority for the center and also is a continuing challenge, particularly given that the database is dynamic, changing frequently with additions, deletions, and modifications. The officials noted the equal importance of ensuring that (1) the names of known and appropriately suspected terrorists are included in the watch list and (2) the names of any mistakenly listed individuals are removed. In this regard, the officials explained that the center's standard operating practices include at least two opportunities to review records. First, Terrorist Screening Center staff—including subject matter experts detailed to the center from other agencies—review each incoming record submitted (nominated) to the center for inclusion in the consolidated watch list. Also, every time there is a screening encounter—for example, a port-of-entry screening of an individual that generates an actual or a potential match with a watch list record—that record is reviewed again.

In addition to the Terrorist Screening Center's quality-assurance initiatives, screening agencies also have been looking at ways to reduce misidentifications. One way that holds promise, where applicable, is to use additional personal-identifying information to enhance name-based searching. For example, as part of its efforts to develop the Secure Flight program, the Transportation Security Administration conducted tests between November 2004 and April 2005 to determine what combinations of names and associated personal-identifying attributes were most effective in matching airline passenger data against terrorist watch list records. According to the Transportation Security Administration, the testing indicated that searches using additional personal-identifying attributes could potentially result in decreasing the number of misidentifications. However, the Transportation Security Administration concluded that more testing was needed to determine, among other things, the point of diminishing returns in using combinations of personal-identifying information to enhance name-based watch list searches.

Agencies Are Taking a Number of Actions to Expedite Frequently Misidentified Persons through the Screening Process

In addition to initiatives aimed at reducing the number of misidentifications, screening agencies also are taking actions to expedite the screening of frequently misidentified persons.

Transportation Security Administration Maintains a Cleared List of Individuals to Expedite Screening and Mitigate Negative Effects

The Transportation Security Administration has instituted a process designed to help frequently misidentified air passengers obtain boarding passes more quickly and avoid prolonged delays. Under this process, an individual can voluntarily provide the Transportation Security Administration with additional personal-identifying information. Then, the Transportation Security Administration will use this information to decide whether the person's name should be put on a cleared list—that is, a list that contains the names and other personal-identifying information of individuals who have been checked and cleared as being persons not on the No Fly and Selectee lists. Airlines are to use the cleared list to more quickly determine that these passengers are not the persons whose names are on the No Fly and Selectee lists. As needed, the Transportation Security Administration provides the airlines with updates of the No Fly and Selectee lists and the cleared list. As discussed later in this report, the cleared list is integral to the Transportation Security Administration's redress process for watch-list-related complaints.

U.S. Customs and Border Protection Is Annotating Its Database to Help Frequently Misidentified Travelers Avoid Additional Screening and Delays

According to U.S. Customs and Border Protection officials, the agency has implemented procedures designed to help frequently misidentified travelers avoid additional screening and delays. Specifically, in February 2006, the agency began annotating its database regarding travelers who were inadvertently stopped because they have the same or similar name as a watch list record but are not the actual subject of the record. The officials explained that the agency uses the data routinely collected on a traveler during the initial inspection process, and no further action is necessary by the traveler. The officials noted that these travelers should no longer be stopped on subsequent visits because of the records in question. As of September 2006, according to U.S. Customs and Border Protection officials, the agency had annotated more than 10,300 such instances and had prevented more than 7,200 unnecessary inspections from occurring.²⁸

The Department of State Is Annotating Its Database to Avoid Future Delays for Visa Applicants

As mentioned previously, the State Department's processing of a visa application takes additional time if initial screening shows a possible link to terrorism, because a decision on the visa applicant cannot be made until a security advisory opinion request is forwarded to Washington, D.C., and a response is received. However, the State Department has taken steps to

²⁸Although a purpose is to expedite frequently misidentified persons through the screening process, the database-annotation initiative is not a "redress" process as defined in this report. Under the initiative, the agency is taking action proactively rather than responding to specific complaints or redress queries submitted by individuals.

help minimize visa-processing delays for any subsequent application filed by a previously screened person. Specifically, according to State Department officials, when a visa applicant is screened through the security advisory opinion process and is found to be a person who is not on the terrorist watch list, the State Department enters clarifying comments in its database or even on the visa itself. This information is available for review by consular officers in processing any subsequent visa applications filed by the individual. Thus, according to State Department officials, the individual's future applications should not incur any additional processing times, unless new information has been acquired in the interim period that would cast doubt on the applicant's eligibility for a visa.

As a Future Enhancement, the Terrorist Screening Center Plans to Have Links to Biometric Data; Various Traveler-Screening Programs Already Use Biometric Data

Within the law enforcement community, fingerprint identification has been used and accepted for decades and is the de facto international standard for positively identifying individuals. Thus, as is widely recognized throughout government, the use of biometric technologies based on fingerprint recognition, facial recognition, or other physiological characteristics offer opportunities for enhancing the key homeland security objective of preventing known or suspected terrorists from entering the country.²⁹

Conceptually, biometrics can be used to screen a traveler against a consolidated database, such as the terrorist watch list—a screening of one record against many records. However, the Terrorist Screening Center presently does not have this capability, although use of biometric information to supplement name-based screening is planned as a future enhancement. Specifically, the Terrorist Screening Center's strategy is not to replicate existing biometric data systems. Rather, the center's strategy, according to the director and principal deputy director, is to develop a "pointer" capability to facilitate the online linking of name-based searches to relevant biometric systems, such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS)—a computerized system for storing, comparing, and exchanging fingerprint data in a digital format, which contains the largest criminal biometric database in the world. Center officials recognize that even biometric systems have screening

²⁹In an earlier report, we assessed various biometric technologies. See, GAO, *Technology Assessment: Using Biometrics for Border Security*, GAO-03-174 (Washington, D.C.: Nov. 15, 2002).

limitations, such as relevant federal agencies may have no fingerprints or other biometrics to correlate with many of the biographical records in the center's consolidated database. For instance, watch list records may be based on intelligence gathered by electronic wire taps or other methods that involve no opportunity to obtain biometric data. Also, the availability of interoperable technology to facilitate online linking among agencies is a long-standing issue that presents challenges. Nonetheless, center officials anticipate that biometric information, if available, can be especially useful for confirming matches to watch list records when individuals use false identities or aliases.

On the other hand, the Terrorist Screening Center has no plans for trying to reduce the incidence of misidentifications by collecting or maintaining biometric information on persons who are not on the watch list. Center officials noted that collecting and using biometric information on innocent persons would raise significant privacy concerns, which would have to be thoroughly considered in interagency discussions and weighed against the possible benefits.

Presently, the Department of Homeland Security uses biometric data for operating various programs to screen travelers, one of which is a required-enrollment program for selected foreign nationals who travel to the United States and others are voluntary-enrollment or trusted-traveler programs. However, enrollment in these programs, whether required or voluntary, does not exempt individuals from being screened against the terrorist watch list. As mentioned previously, for instance, the watch list is dynamic, changing frequently with additions, deletions, and modifications.

The required-enrollment program that uses biometric data is the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which is an entry/exit tracking system designed to collect, maintain, and share information on selected foreign nationals who travel to the United States. The program uses a related system—the Automated Biometrics Identification System (IDENT), developed by the former Immigration and Naturalization Service—to collect two fingerprints (right and left index fingers) and a digital photograph to provide for the biometric identification of visitors.³⁰ Required enrollment in the US-VISIT program is conducted by the Department of State at visa-issuing consulates before the

³⁰In July 2005, the Secretary of Homeland Security announced that US-VISIT would be enhanced to collect 10-finger scans.

visitors depart or by U.S. Customs and Border Protection at ports of entry when the visitors arrive. American citizens, permanent legal residents, Canadian nationals, and Mexican nationals with border-crossing cards are not required to submit to US-VISIT screening at ports of entry. In July 2006, the Department of Justice’s Office of the Inspector General provided an update on progress toward achieving biometric interoperability between IDENT and IAFIS.³¹ The Inspector General’s progress report noted that the FBI and the Department of Homeland Security have formed a working group to make US-VISIT, IDENT, and IAFIS interoperable by December 2009.

Under the US-VISIT program, at each subsequent reentry into the United States, applicable individuals are biometrically screened against the fingerprints collected during the initial enrollment. Such biometric screening is for identity verification purposes—screening that involves a one-to-one matching of fingerprints to determine if the traveler is the person enrolled in the program. Enrollment in the U.S.-VISIT program does not exempt individuals from being screened against the terrorist watch list and generally may not reduce the possibility of the individuals being misidentified based on name similarities. As such, when there are potential matches to a name on the watch list, the individuals may still be subject to more extensive screening at ports of entry.

Another biometrics-based program—Registered Traveler—is being pilot tested by the Transportation Security Administration.³² The program, commonly categorized as a trusted-traveler program, collects biographical information and biometric data from airline passengers who volunteer to undergo a security threat assessment. The pilot program is being tested in partnership with selected airlines and airports across the country. Under the program, prior to boarding at airports, participants are to be screened using the biometric data.

³¹U.S. Department of Justice, Office of the Inspector General, Evaluation and Inspection Division, *Follow-up Review of the FBI’s Progress Toward Biometric Interoperability between IAFIS and IDENT* (Washington, D.C.: July 2006).

³²The Transportation Security Administration is authorized to “establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.” See Pub. L. No. 107-71, § 109(a)(3), 115 Stat. 597, 613 (2001).

In addition, U.S. Customs and Border Protection operates various trusted-traveler programs, which are intended to provide expedited processing for pre-approved, low risk travelers who frequently cross U.S. borders. For instance, a commuter program on the southern border is known as Secure Electronic Network for Travelers Rapid Inspection (SENTRI) and on the northern border as “NEXUS.” For these voluntary programs, the biometric component generally involves only the enrollment process, such as conducting fingerprint-based background checks using IDENT or IAFIS to ensure that applicants are eligible for expedited processing before allowing their participation.³³ Thereafter, cross-border commuting is facilitated by use of radio frequency identification (RFID) technology, whereby an embedded chip in each membership card transmits the person’s arrival to a reader-antenna at the port of entry.³⁴

While trusted-traveler programs are most commonly applicable to cross-border commuters, U.S. Customs and Border Protection officials told us that all persons who believe they are frequently misidentified with similar names on the terrorist watch list can apply and will be accepted if they are found to meet program requirements. Also, a benefit of these programs from a watch list perspective is that U.S. Customs and Border Protection has greater assurance of the identity of the enrollees and that these individuals are not persons on the watch list. Enrollment in a trusted-traveler program does not exempt individuals from being screened against the terrorist watch list; although, according to U.S. Customs and Border Protection officials, enrollment does mitigate the possibility of the individuals being misidentified and selected for more extensive screening at ports of entry. The officials also noted that the trusted-trusted traveler programs are not widely applicable to all ports of entry. Rather, the programs are helpful only to individuals eligible to use trusted-traveler lanes at the border, not at airports or seaports.

³³In the SENTRI program, for example, applicants must volunteer for (1) a biographical background check against criminal, law enforcement, customs, immigration, and terrorist databases; (2) a 10-fingerprint law enforcement check; and (3) a personal interview with a U.S. Customs and Border Protection officer.

³⁴RFID is a wireless technology that stores and retrieves data remotely from devices. For instance, the technology allows information to be written to tags, which can be scanned or read from a distance. See, GAO, *Information Security: Radio Frequency Identification Technology in the Federal Government*, GAO-05-551 (Washington, D.C.: May 27, 2005).

The Terrorist Screening Center and Frontline-Screening Agencies Are Addressing Concerns Related to Watch List Screening, and an Interagency Agreement Is Being Developed to Further Ensure an Effective Means for Seeking Redress

It is important that individuals who are inadvertently and adversely affected by watch list screening be provided an opportunity to seek redress. The Terrorist Screening Center, the Transportation Security Administration, and U.S. Customs and Border Protection have processes in place to address individuals' concerns involving watch-list-related screening and have reported some successes, such as removing from the watch list the names of several mistakenly listed persons. Most watch-list-related redress concerns usually involve misidentified persons—individuals who are not on the watch list but have name similarities with known or suspected terrorists. To help ensure that opportunities for redress are formally documented and that agency responsibilities are clear, the Department of Justice is leading an effort to develop an interagency memorandum of understanding. A final draft of the memorandum of understanding is expected to be ready for interagency clearances by fall 2006, according to Terrorist Screening Center officials.

The Terrorist Screening Center and the Federal Frontline-Screening Agencies Have a Role in Addressing the Concerns of Individuals Who are Adversely Affected by Watch List Screening

The Terrorist Screening Center, the Transportation Security Administration, and U.S. Customs and Border Protection have important responsibilities in providing individuals who are inadvertently and adversely affected by watch list screening with opportunities to seek redress. As mentioned previously, all aggrieved individuals may seek redress, including persons who express concerns or complaints that they are being misidentified and adversely affected because they have a name similar to someone whose name is on the terrorist watch list and persons who actually are on the terrorist watch list. Any such concern or complaint raised formally by an affected individual is what the Terrorist Screening Center calls a redress query. Specifically, the Terrorist Screening Center defines a "redress query" as communication from individuals or their representatives inquiring or complaining about an adverse experience during a terrorist watch-list-related-screening process conducted or sponsored by a federal agency, including congressional inquiries to federal agencies on behalf of constituents.

According to the Terrorist Screening Center's standard operating procedures for redress matters, frontline-screening agencies, such as the Transportation Security Administration and U.S. Customs and Border Protection, have a key role in handling redress queries. Significantly, for example, the frontline-screening agencies—and not the Terrorist

Screening Center—are to receive and initially handle redress queries from the public. The operating procedure of having frontline agencies receive redress queries serves at least two purposes, according to the Terrorist Screening Center. First, the applicable frontline-screening agency is better positioned to know the details of the screening encounters and to respond appropriately. Second, many screening encounters may be based on factors other than terrorism—factors such as narcotics trafficking or incomplete currency or customs declarations—which are not within the mission of the Terrorist Screening Center and must be resolved by the frontline agencies. Also, as a practical matter, the frontline agencies are the entities visible to complainants or inconvenienced persons.

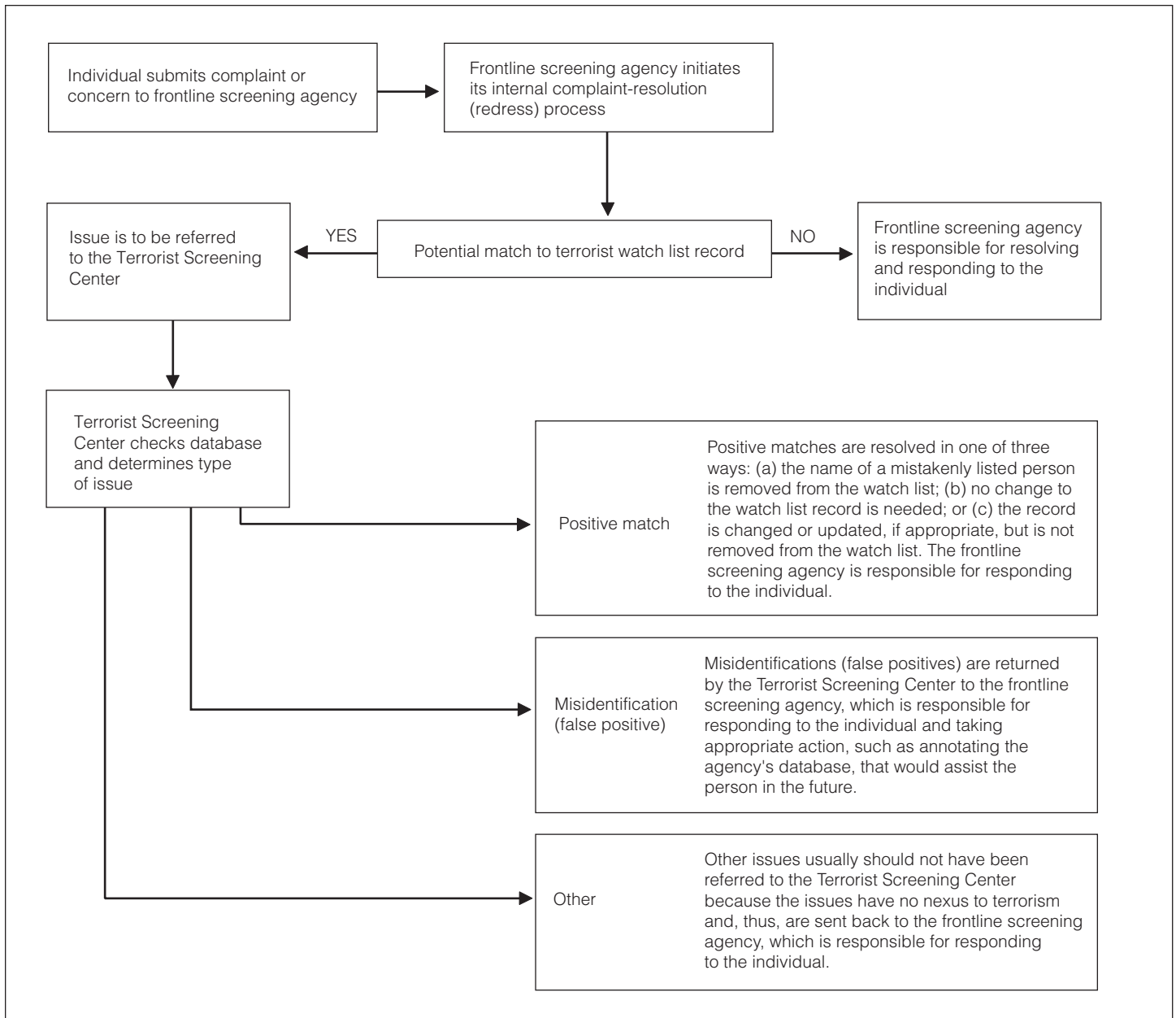
Further, after a frontline-screening agency receives a complaint or concern from an individual, the agency is to begin its internal complaint-resolution or redress process. As part of this process, the agency is to determine whether the person’s complaint is related to a potential match to a terrorist watch list record. If the determination is “no”—that is, the person is not actually on the watch list but was misidentified because of a name similarity to someone who is on the terrorist watch list—the frontline-screening agency is responsible for resolving the complaint and responding to the misidentified individual.

If the frontline-screening agency’s determination is “yes”—which includes not only definite matches but also any potential or “maybe” matches that require additional research to confirm—the frontline agency is to refer the redress query to the Terrorist Screening Center. Then, the center is to check its database to determine whether the individual is indeed on the terrorist watch list or whether the person is misidentified with someone on the watch list. If the person is actually on the terrorist watch list, the Terrorist Screening Center is to consult with applicable intelligence community and law enforcement agencies to assess whether the person is appropriately listed and should remain on the watch list or is mistakenly listed and should be removed from the list. In either instance, the center is to inform the applicable frontline-screening agency, which is responsible for responding to the individual. If the complainant is a misidentified person, the Terrorist Screening Center is to send the redress query back to the applicable frontline-screening agency for that agency to resolve. Also, as part of its quality-assurance efforts, the center is to review the underlying watch list record that caused the person’s adverse experience to determine, for example, the record’s validity or whether a modification is needed, including possible removal of the record. Finally, any referrals received by the Terrorist Screening Center not related to its mission—that is, “other issues” with no nexus to terrorism such as complaints involving

employee misconduct or random screening—are to be sent back to the applicable frontline-screening agency, which is to provide a response to the individual.

In January 2005, the Terrorist Screening Center established its formal redress process. An overview of the redress process, including interaction between the center and the frontline-screening agencies, is illustrated in figure 2.

Figure 2: General Overview of the Terrorist Screening Center’s Process for Handling Concerns Involving Watch-List-Related Screening



Source: GAO.

Note: As a general overview, the figure does not reflect all ways that complaints or concerns can be resolved. For instance, regarding clearance difficulties experienced by an individual at a port of entry, U.S. Customs and Border Protection may determine that the person was selected for intensive screening based on information provided by another federal law enforcement agency. If so, U.S. Customs and Border Protection may refer the complainant's query to the applicable agency—which, in turn, would reply directly to the individual.

The Terrorist Screening Center does not directly provide final disposition letters to individuals who have submitted redress queries. Rather, the center works with the frontline-screening agencies—and, as applicable, any relevant intelligence or law enforcement agencies—to develop a written response. In providing a final response to an individual who submits a redress query, the frontline-screening agencies use a response letter that neither confirms nor denies the existence of any terrorist watch list records relating to the individual. For example, one of the Transportation Security Administration's standardized response letters states, in part, "Where it has been determined that a correction to records is warranted, these records have been modified to address any delay or denial of boarding that you may have experienced as a result of the watch list screening process."

Generally, this type of language reflects the Terrorist Screening Center's policy of neither confirming nor denying whether an individual is on the consolidated terrorist watch list because this information is derived from classified and sensitive law enforcement and intelligence sources. The policy of nondisclosure to the public is intended to protect the operational counterterrorism and intelligence collection objectives of the government and the personal safety of those involved in counterterrorism investigations.

The Terrorist Screening Center's Handling of Redress Referrals Has Resulted in Removing the Names of Several Mistakenly Listed Persons from the Terrorist Watch List

During calendar year 2005, the Terrorist Screening Center processed to completion 112 redress queries referred by frontline-screening agencies. Of this total, according to the Terrorist Screening Center, 31 were determined to be mistakenly listed individuals and their names were removed from the watch list (see table 1). The center reported that for another 54 queries the individuals were on the terrorist watch list and the center either did not change the watch list records (48) or made some updates (6).

Table 1: Number and Disposition of Redress Queries Referred to the Terrorist Screening Center, Calendar Year 2005

Disposition of redress query	Number
Positive match: The name of the mistakenly listed person was removed from the watch list	31 ^a
Positive match: No change to the watch list record was needed	48
Positive match: The record was changed or updated but not removed from the watch list	6
Misidentification: The redress query was referred back to the frontline-screening agency to process and provide a response to the individual	19
Other: These queries involved issues not relevant to the terrorist watch list and should not have been referred to the Terrorist Screening Center	8
Total	112

Source: Terrorist Screening Center data.

^aAccording to Terrorist Screening Center officials, the center was already in the process of removing a few of these names before the center received the respective redress queries. The officials explained that although the names were properly included on the watch list initially, subsequent events warranted removing the names.

Also, as table 1 indicates, 19 of the 112 referrals in calendar year 2005 involved misidentified persons—that is, the Terrorist Screening Center determined that these individuals were not on the terrorist watch list but have names similar to someone who is a known or suspected terrorist. The center referred each of these queries back to the applicable frontline-screening agency for processing under the respective agency’s redress procedures. These 19 misidentifications do not constitute the annual universe of all redress queries involving misidentifications. Rather, thousands of such queries from misidentified persons are handled by the frontline-screening agencies and are not referred to the Terrorist Screening Center.

To enhance public awareness of redress availability, the Web site of the FBI—the Terrorist Screening Center’s administering agency—presents an overview of applicable policy and procedures, provides answers to frequently asked questions, and gives contact information for three frontline-screening agencies—the Transportation Security Administration, U.S. Customs and Border Protection, and the State Department. This information is also presented in appendix II of this report.

Most Redress Queries Involve Misidentified Persons and Are Handled by Frontline-Screening Agencies

Most redress queries involve misidentified rather than mistakenly listed individuals. Therefore, inherently the disposition or resolution of a redress query involving a misidentification cannot be removal of the individual's name from a watch list because the individual is not the person on the list. Instead, an objective of the frontline-screening agencies is to address complaints of misidentified individuals by providing alternative relief—that is, by developing procedures and having sufficient information in screening databases to expedite the processing of frequently misidentified persons.

Transportation Security Administration: For Individuals Who Are Frequently Misidentified Due to Name Similarities with Known or Suspected Terrorists, the Agency Has Compiled a Cleared List

The Transportation Security Administration has a contact center that centrally receives nonmedia public inquiries and complaints. According to the agency, the contact center's customer service representatives and contact security specialists are trained to handle and analyze incoming calls, e-mails, correspondence, and facsimiles from the public, the Congress, and private industry. The functions of these representatives and specialists, as specified in the contact center's operating procedures, are to analyze letters and electronic messages, sort them by subject matter, and confer with appropriate offices throughout the agency (including field staff) to provide responses.

Generally, any inquiries and complaints regarding watch-list-related screening—that is, screening against the No Fly and Selectee lists—are to be handled by the agency's Office of Transportation Security Redress, which was established in November 2004.³⁵ As part of the redress process, an individual can voluntarily provide additional personal-identifying information to the Office of Transportation Security Redress. Specifically, the individual can submit a completed Traveler Identity Verification Form (reproduced in app. III), along with a copy of a U.S. passport or copies of three types of other identification documents, such as birth certificate, driver's license, military identification card, military discharge paper, voter registration card, and naturalization certificate or certificate of citizenship.³⁶ Then, the agency will use this information in deciding

³⁵Previously, the agency's Office of the Ombudsman handled all inquiries and complaints, including those regarding watch-list-related screening.

³⁶The Traveler Identity Verification Form (May 2006) replaced an earlier form, the Passenger Identity Verification Form. Regarding the latter, the Transportation Security Administration's instructions required the submission of notarized copies of three identification documents. Instructions for the new form do not require that the submitted documents be notarized.

whether the person's name should be put on a cleared list—which airlines are to use for distinguishing the individual from persons who are in fact on the No Fly or Selectee lists.³⁷ Along with as-needed updates of the No Fly and Selectee lists, the Transportation Security Administration transmits updated cleared list information to the airlines for the purpose of enabling the airlines to more quickly determine that these passengers are not the persons who are on the No Fly and Selectee lists. The purpose of the cleared list is to mitigate or minimize delays or other inconveniences by facilitating the check-in process for passengers who have names similar to known or suspected terrorists. An individual on the cleared list may still have to obtain a boarding pass at the ticket counter rather than using Internet, curbside, or airport kiosk check-in options. Nonetheless, the intent of the cleared list is to reduce the delay or wait time for applicable air passengers in obtaining a boarding pass at the ticket counter.

According to the Director of the Office of Transportation Security Redress, over 30,000 individuals had submitted identify verification forms and supporting documentation to the agency, as of December 2005, and the names of the overwhelming majority of these individuals were added to the cleared list. The director explained that although the agency requires air carriers to use the cleared list, responsibility for utilizing the list rests with the air carriers, and all carriers do not operate in the same way or have equal capabilities. Further, according to the director, some customers (air passengers) call and complain about having problems even though they have taken the necessary steps to be placed on the cleared list. The director said that his office forwards information regarding these complaints to another component of the agency—the Office of Transportation Sector Network Management—which is responsible for contacting the respective air carriers to address relevant issues.

According to Transportation Security Administration officials, the Secure Flight program is a prospective solution to current issues regarding inconsistent use of the cleared list by air carriers—as well as any inconsistent use of the No Fly and Selectee lists. Under the Secure Flight program, the Transportation Security Administration plans to take over, from commercial airlines, the responsibility for comparing identifying information of airline passengers against information on known or

³⁷The cleared list procedure began in May 2003 under the agency's Office of the Ombudsman.

U.S. Customs and Border
Protection Is Considering
Realigning Its Watch-List-
Related Redress
Responsibilities and Is
Updating Its Procedures

suspected terrorists.³⁸ We note, however, that the Transportation Security Administration has been in the process of developing a passenger prescreening system, presently known as the Secure Flight program, for more than 3 years. We have reported and the Transportation Security Administration has acknowledged significant challenges in developing and implementing the Secure Flight program.³⁹ Earlier this year, the Transportation Security Administration suspended Secure Flight's development to reassess, or rebaseline, the program. The rebaselining effort includes reassessing the program goals to be achieved, the expected benefits and capabilities, and the estimated schedules and costs. As of July 2006, the Transportation Security Administration had not publicly announced any decisions regarding the future of the Secure Flight program, although the agency anticipates that the rebaselining effort will be completed by the end of September 2006.

U.S. Customs and Border Protection headquarters has a Customer Satisfaction Unit that functions as a centralized source for recording, tracking, and reviewing all complaint information related to U.S. Customs and Border Protection interactions with travelers, the general public, industry, and government entities. This unit is responsible for responding to customer complaints, irrespective of the subject matter—that is, the unit focuses on all complaint topics, not just complaints involving terrorist watch-list-related screening. For instance, U.S. Customs and Border Protection routinely uses a comment card that allows travelers to express any complaint regarding the port-of-entry processing experience. U.S. Customs and Border Protection policy is to provide a comment card to (1) all air and sea travelers who are subjected to a secondary examination and (2) all air, land, and sea travelers who undergo a personal search.

³⁸In March 2003, the Transportation Security Administration began developing CAPPS II, a second-generation computer-assisted passenger prescreening program, to provide improvements over CAPPS I and to screen all passengers flying into, out of, and within the United States. CAPPS II was to perform different analyses and access more diverse data, including data from government and commercial databases, to classify passengers according to their level of risk (i.e., acceptable risk, unknown risk, or unacceptable risk), which would in turn be used to determine the level of security screening each passenger would receive. Because of a variety of challenges, the Department of Homeland Security cancelled the development of CAPPS II in August 2004 and announced that a new prescreening program, called Secure Flight, would be developed.

³⁹GAO, *Aviation Security: Management Challenges Remain for the Transportation Security Administration's Secure Flight Program*, GAO-06-864T (Washington, D.C.: June 14, 2006).

In June 2006, U.S. Customs and Border Protection officials explained that the agency was actively considering ways to enhance the capability of the Customer Satisfaction Unit to support redress efforts regarding terrorist watch-list-related concerns or complaints. For instance, a realignment being considered is to move the responsibility for handling certain categories of complaints—those not involving terrorist watch list screening—from the Customer Satisfaction Unit to the Office of Public Affairs. Also, the officials further noted that the agency’s Office of Regulations and Rulings was updating the Customer Satisfaction Unit’s standard operating procedures, including redress procedures regarding terrorist watch-list-related concerns or complaints.

Further, in commenting on a draft of this report in September 2006, U.S. Customs and Border Protection officials said that the agency is working with the Terrorist Screening Center to ensure that its process aligns with the center’s process. Also, another Department of Homeland Security component—U.S. Immigration and Customs Enforcement—commented that its Office of Intelligence serves as a point of contact and works closely with the Terrorist Screening Center’s redress team to ensure the removal or modification of records, as appropriate, from the terrorist-screening database and the Treasury Enforcement Communications System/Interagency Border Inspection System. For instance, U.S. Immigration and Customs Enforcement noted that if the Terrorist Screening Center determines that an individual should no longer be listed in the terrorist-screening database, the Office of Intelligence coordinates with U.S. Customs and Border Protection to have the record expunged from the Treasury Enforcement Communications System/Interagency Border Inspection System.

As part of our study, we reviewed the Federal Bureau of Investigation’s Web site for the Terrorist Screening Center to determine what overview information regarding watch-list-related redress was publicly available (see app. II). In turn, from the FBI’s overview Web site, we followed up on any references or online links to the redress processes of key frontline-screening agencies—the Transportation Security Administration and U.S. Customs and Border Protection.

In contrast to the online link to the Transportation Security Administration’s redress guidance (see app. III), we found limited usefulness in the online link to U.S. Customs and Border Protection’s redress guidance. The FBI’s overview Web site lists the Customer Satisfaction Unit as the redress-related contact point for U.S. Customs and Border Protection. Also, the overview Web site provides an online link to a

fact sheet describing the Interagency Border Inspection System—a system that provides U.S. Customs and Border Protection and other law enforcement entities with access to computer-based information. However, the fact sheet (reproduced in app. IV) has no specific guidance regarding terrorist-watch-list-related redress. Rather, the fact sheet answers basic questions regarding the Interagency Border Inspection System, such as who uses the system and what information is in the system. Moreover, the overview Web site provides no references or online links to U.S. Customs and Border Protection’s trusted-traveler programs—such as SENTRI and NEXUS. As mentioned previously, agency officials told us that persons who believe they are frequently misidentified with the terrorist watch list or who continuously experience delays and other inconveniences during screening could apply to one of these programs and, if accepted, receive expedited processing at applicable ports of entry.

Based on our observations regarding the limited usefulness of the online links from the FBI’s overview Web site, U.S. Customs and Border Protection officials acknowledged a need to coordinate with the FBI and the Terrorist Screening Center to provide more appropriate online links regarding redress guidance. The officials noted, for example, that U.S. Customs and Border Protection’s Web site does provide information regarding the Customer Satisfaction Unit and how complaints are handled as well as information on trusted-traveler programs.

Department of State:
Applicants Who Are Denied a
Visa Have No Legal Basis to
Appeal, but an Agency-Initiated
Process Is Used to Remove
Erroneous or Outdated Entries
from the Consular Lookout and
Support System

The term “redress,” according to the State Department, is not applicable to complaints about visa denials, which are final decisions not subject to appeal or judicial review. However, the State Department has an agency-initiated process for removing erroneous or outdated entries from the Consular Lookout and Support System, which contains applicable terrorist watch list records. As mentioned previously, the system is used by consular officers abroad to screen the names of visa applicants to identify terrorists and other aliens who are potentially ineligible for visas based on criminal histories or other reasons specified by federal statute. All visa-issuing posts have direct access to the system and are required to use it to check each applicant’s name before issuing a visa, according to the State Department.

The Immigration and Nationality Act of 1952, as amended, gives Department of State consular officers at overseas posts exclusive authority for adjudicating applications submitted by foreign citizens for

visas to enter the United States.⁴⁰ The process for determining who will be issued or refused a visa consists of several steps—including checking or cross-referencing each applicant’s name against the Consular Lookout and Support System, which contains applicable names and biographical data exported from the Terrorist Screening Center’s database. According to the State Department, no applicant is denied a visa simply because the person’s name appears in the Consular Lookout and Support System, which is only a flag or tool to help the consular officer know if further screening may be required. Rather, visa denials are by law based either on statutory grounds of ineligibility, which are specifically set out in the Immigration and Nationality Act, as amended,⁴¹ or on the applicant’s failure to present evidence to establish eligibility for the type of visa requested. In addition to security and terrorism concerns, statutory grounds of ineligibility include, for example, criminal history reasons, previous violations of immigration law, and health-related grounds.

According to State Department instructions provided to consular offices worldwide, visa denials are to be reviewed by the consular officer’s supervisor. If an error has been made or a question exists about interpreting immigration law in reference to the facts surrounding the applicant, the consular officer can request a legal advisory opinion. Also, if there are misunderstandings about the application process, individuals can correspond with the overseas consular section and the Public Inquiries Division of the Visa Office in Washington, D.C.

However, federal courts have consistently held that a consular officer’s final decision to issue or deny a visa is not subject to a formal appeal or to judicial review.⁴² That is, there is no way to directly appeal the visa denial,

⁴⁰Pub. L. No. 82-414, 66 Stat. 182 (codified as amended at 8 U.S.C. § 1101, *et seq.*). However, obtaining a visa from an American consul does not guarantee an alien’s entry into the United States. Rather, a visa authorizes the alien to arrive at a port of entry, at which point a U.S. Customs and Border Protection officer will independently examine the alien’s eligibility for admission.

⁴¹See 8 U.S.C. § 1182(a).

⁴²Courts have long held that a consular officer’s decision to grant or deny a visa is not subject to judicial review. *See, e.g., Saavedra Bruno v. Albright*, 197 F.3d 1153 (D.C. Cir. 1999); *Centeno v. Schultz*, 817 F.2d 1212 (5th Cir. 1987); *Li Hing of Hong Kong, Inc. v. Levin*, 800 F.2d 970 (9th Cir. 1986); *Ventura-Escamilla v. I.N.S.*, 647 F.2d 28 (9th Cir. 1981); *Rivera de Gomez v. Kissinger*, 534 F.2d 518 (2d Cir. 1976); *U.S. ex rel. Ulrich v. Kellogg*, 30 F.2d 984 (D.C. Cir. 1929). *See also, Kleindienst v. Mandel*, 408 U.S. 752 (1972) (holding that courts may not look behind the exercise of an official’s discretionary authority to deny admission to an alien).

nor is there a way to directly overturn the consular officer's denial decision because it is not subject to judicial review. Thus, in explaining why it would be incorrect and legally misleading to use the term "redress" in reference to any complaint about a visa denial, officials in the State Department's Bureau of Consular Affairs commented that a visa refusal (denial) is a final decision in which the consular officer makes a legal determination that the applicant is not eligible for a visa based on a statutory ground. The State Department officials reiterated that the consular officer's decision is a final governmental adjudication, for which there is no appeal or judicial review, and the only recourse for the person is to submit a new application with sufficient information to "overcome" the grounds for ineligibility.

Consular officers are required to provide each applicant an explanation of the legal basis for denying the visa.⁴³ However, if the basis for ineligibility is terrorism—under section 212(a)(3)(B) of the Immigration and Nationality Act, as amended⁴⁴—the consular officer normally would not be able to explain the reasons behind the denial because of national security grounds.

According to Bureau of Consular Affairs officials, the State Department does have an agency-initiated process for removing erroneous or outdated information from the Consular Lookout and Support System. In explaining why the correction-of-records process is initiated by the agency and not the visa applicant, the officials commented substantially as follows:

- Visa applicants usually would not even know whether their names are on the terrorist watch list. If a visa application results in the overseas post's requesting a security advisory opinion and additional screening, the applicant might think that any processing delay is due to a record entry in the Consular Lookout and Support System. However, the additional screening could be due to reasons other than terrorism, such as a criminal record, a contagious disease, or simply an overstay on a previous visa.
- Thus, any deletion of entries from the Consular Lookout and Support System normally would be initiated by the consular officer in the field. That is, if the consular officer determines—based on evidence presented

⁴³Secretary of State cable to all diplomatic and consular posts, *Subject: Reminder Regarding Visa Refusal Procedures* (June 12, 2001).

⁴⁴See 8 U.S.C. § 1182(a)(3)(B).

during the course of a visa application—that an entry in the Consular Lookout and Support System is incorrect or has been overtaken by events, the officer is to initiate action to have the entry deleted from the system.

Also, the Bureau of Consular Affairs officials noted that there has been an occasional complaint that despite the issuance of a visa, the alien experienced difficulties at a U.S. port of entry because, for example, screening by U.S. Customs and Border Protection showed a potential match with a terrorist watch list record. Regarding these instances, the officials said that based on an interest in data integrity and customer service, the department works with the Terrorist Screening Center to review relevant records and determine an appropriate course of action, which could consist of a watch list message or annotation specifying that the alien is not a person on the watch list. In addition, as discussed previously, the State Department is taking steps to annotate its database when it screens individuals and finds that they are not on the watch list. Such annotations are intended to expedite visa processing in the future and limit the incidence of misidentifications.

The Department of Justice Is Leading an Effort to Finalize an Interagency Agreement to Help Ensure That Effective Redress Is Available

The Terrorist Screening Center and the frontline-screening agencies have interdependent responsibilities in providing redress for individuals who are inadvertently and adversely affected by watch list screening. The availability of redress is important for all affected persons, including persons who are misidentified because of name similarities and to persons who contend that they are mistakenly included on the terrorist watch list. For any given watch-list-related complaint or redress query, providing relief can necessitate interaction among several governmental agencies. For instance, if the query involves a person who is mistakenly listed, relevant redress participants could include the Terrorist Screening Center and a frontline-screening agency as well as the agency that originally submitted or nominated the person's name for inclusion in the consolidated terrorist watch list. Nominating agencies include the FBI and various agencies within the intelligence community, such as the Central Intelligence Agency, the Defense Intelligence Agency, and the National Security Agency.

To help ensure that opportunities for terrorist-watch-list-related redress are implemented effectively, the Department of Justice is leading an effort—which has been ongoing since fall 2005—to develop and finalize an interagency memorandum of understanding. Key purposes of the final memorandum of understanding include ensuring that opportunities for redress are formally documented and that agency responsibilities are

clear, with designated officials accountable for supporting the continued success of the processes. The Department of Justice has a lead role in developing the memorandum of understanding because the Terrorist Screening Center has primary responsibility for the consolidated terrorist-screening database. Interagency partners in the effort to develop the memorandum of understanding include the Department of Homeland Security, the Department of State, and the National Counterterrorism Center.

Also, another entity involved in developing the memorandum of understanding is the Privacy and Civil Liberties Oversight Board, which is part of the Executive Office of the President and consists of five members appointed by the president.⁴⁵ According to the board's executive director, the terrorist watch list redress process is a top priority for the board. The executive director noted that since June 2006 board staff have attended all meetings of the interagency partners engaged in developing the memorandum of understanding. This official opined that the board's participation has helped reprioritize this matter among the constituent agencies and that the board is committed to continuing its involvement.

According to Department of Justice officials, a final draft of the memorandum of understanding is expected to be ready for interagency clearances by fall 2006. Terrorist Screening Center officials emphasized that the interagency memorandum of understanding was definitely needed, particularly as a mechanism for ensuring the accuracy of the watch list. The center officials noted, for instance, that there have been disagreements at times between agencies over nominations to the watch list. Thus, in handling watch-list-related complaints, the center officials explained that the interagency memorandum of understanding could help by clearly outlining a process for coordinating with the National Counterterrorism Center and nominating agencies to validate the accuracy and appropriateness of watch list records.

⁴⁵The board was established by section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004. Pub. L. No. 108-458, 118 Stat. 3638, 3684-88. The board advises the president and other senior executive branch officials as to whether privacy and civil liberties protections are appropriately considered in the development and implementation of laws, regulations, and executive branch policies related to efforts to protect the nation against terrorism. The five board members were sworn in and had their first meeting on March 15, 2006. Additional information about the role of the board and its operations is available at www.privacyboard.gov.

Moreover, the Terrorist Screening Center officials explained that the interagency memorandum of understanding could help resolve significant watch-list-related redress differences among the frontline-screening agencies. Examples regarding Department of Homeland Security components are as follows:

- The Transportation Security Administration has an office specifically designated for redress issues, with an accountable official—the Director, Office of Transportation Security Redress. Also, the office has followed consistent procedures in referring appropriate watch-list-related complaints to the Terrorist Screening Center.
- In contrast, U.S. Customs and Border Protection does not have a clearly designated official accountable for redress, and the agency has not always followed consistent procedures in referring appropriate watch-list-related complaints to the Terrorist Screening Center.

Additionally, regarding the State Department, the Terrorist Screening Center officials stressed the importance of having clearly established procedures and responsibilities. The center officials noted that even though the State Department’s operational context is somewhat different than that of other frontline-screening agencies, the department nonetheless has a substantial volume of interactions with the Terrorist Screening Center. State Department Bureau of Consular Affairs officials acknowledged to us the value of having an interagency memorandum of understanding that specifies standard operating procedures for redress and designates points of contact. In this regard, the State Department officials commented that they have been participating in meetings with the Terrorist Screening Center and other interagency partners to discuss the proposed memorandum of understanding. According to the officials, a benefit to the State Department expected from the interagency agreement would be clearly established and coordinated procedures for removing—from the department’s Consular Lookout and Support System and the Terrorist Screening Center’s consolidated watch list—any name that is mistakenly listed or has been overtaken by subsequent events.

Concluding Observations

Homeland security measures affect all travelers to some extent. Thus, it may be argued that travel delays and other inconveniences resulting from terrorist watch-list-related screening can be viewed as regrettable but inevitable consequences of enhanced security. However, name-based screening and its inherent limitations—even full names, in most cases, are hardly unique identifiers—may result in disproportionate impact on

individuals who repeatedly are singled out for additional screening for no other reason than the similarity of their names to someone on the watch list.

The Terrorist Screening Center and its interagency partners are undertaking a number of efforts, including data-quality initiatives, to reduce the occurrence and/or impact of watch list screening on U.S. citizens and visitors who do not necessarily merit additional scrutiny and the associated inconveniences. A continuing challenge for the center will be ensuring that the consolidated watch list contains accurate data, particularly given that the database is dynamic, changing frequently with additions, deletions, and modifications. The efforts of an interagency working group to improve the effectiveness of name-matching computer algorithms may offer some promise for reducing the number of people who experience unintended, adverse effects. However, any policy trade-off considerations regarding use of algorithms likely will favor ensuring homeland security over minimizing inconveniences to travelers. Regarding future operations, the Terrorist Screening Center is actively considering approaches for using biometric data to supplement name-based searches, although the availability of appropriate technology is an issue that has long confronted the interagency screening community.

In any event, despite the best efforts of the interagency community to maintain a fully accurate watch list and to conduct screening efficiently, there likely will be continuing unintended consequences. Thus, it is appropriate for the Terrorist Screening Center and its interagency partners to continue their efforts to provide effective redress for both mistakenly listed persons and misidentified persons. Indeed, redress queries have already resulted in the removal of several mistakenly listed names from the watch list. Comparatively, however, the issue of redress arises more commonly regarding the thousands of persons who are not on the watch list but are misidentified and adversely affected because of a name similarity. Whether appropriate relief is being afforded these individuals is still an open question, for several reasons. For example, although a core element of the redress provided by the Transportation Security Administration is the maintenance of a cleared list, there are some indications that the cleared list is not working as intended to reduce delays for air passengers in obtaining boarding passes. Prospectively, the Transportation Security Administration expects that development and implementation of the Secure Flight program will help ensure consistent and effective use of the cleared list among air carriers, although the agency has not publicly disclosed its future plans for the program.

Another frontline-screening agency's initiative, U.S. Customs and Border Protection's database-annotation initiative, may prove to be an even more efficient approach for assisting frequently misidentified individuals. Unlike the Transportation Security Administration's cleared list procedures, the U.S. Customs and Border Protection's initiative is based on records in the agency's database and does not necessitate any filing of forms and other documentation by travelers. At the time of our review, U.S. Customs and Border Protection was planning to develop a capability to monitor the effectiveness of the initiative. This planning effort is particularly important, given that the initiative may eventually prove to be a model for a proactive solution if it functions as intended.

Finally, an overarching factor regarding whether appropriate relief is being afforded to persons inadvertently and adversely affected by terrorist watch-list-related screening is the absence of an interagency agreement to help ensure that, among other matters, redress procedures and responsibilities are clearly documented and implemented effectively. The Terrorist Screening Center and its interagency partners are working to address this fundamental deficiency and have indicated their intent to provide the public with updated information on the availability of redress, after finalization of an agreement.

We are not making recommendations at this time because the agencies have ongoing efforts to improve data quality and otherwise either reduce the number of misidentifications or mitigate their effects and to provide more effective redress.

Agency Comments

We provided a draft of this report for comments to the departments of Homeland Security, State, and Justice. We received written responses from each agency.

In its response, the Department of Homeland Security acknowledged that it currently is undertaking actions to enhance terrorist-screening and redress efforts. Also, the response noted that in January 2006, the departments of State and Homeland Security announced an initiative on "Secure Borders and Open Doors in the Information Age," otherwise known as the Rice-Chertoff Initiative. One purpose of the initiative is to establish a governmentwide redress process to address perceived problems in international and domestic traveler prescreening. According to the Department of Homeland Security, a goal is to establish a one-stop redress process for travelers by the end of calendar year 2006. The department explained that this initiative, which will supplement terrorist

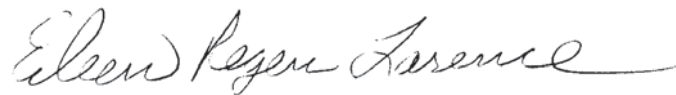
watch-list-related redress, focuses on a larger set of travel-screening redress issues. The full text of the Department of Homeland Security's written comments is reprinted in appendix V. The department also provided technical comments, which we incorporated in this report where appropriate.

The Department of State commented that the report accurately describes the visa process and the department's position that the administrative processing time required to screen a visa applicant—including, if required, the processing of a security advisory opinion review—is a necessary part of the visa application procedure rather than an adverse governmental action. Also, the department noted that—in its use of the terrorist watch list as a screening tool for visa adjudication—a “misidentification” is not an adverse result for the visa applicant. Rather, according to the department, this type of response helps to determine that the visa applicant is not associated with terrorism. In its written response, the department also provided a technical comment regarding the security advisory opinion process, which we incorporated in this report where appropriate. The full text of the Department of State's written comments is reprinted in appendix VI.

The Department of Justice provided technical comments only, which we incorporated in this report where appropriate.

As arranged with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days after the date of this report. At that time, we will send copies of this report to interested congressional committees and subcommittees. We will also make copies available to others on request. In addition, this report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report or wish to discuss the matter further, please contact me at (202) 512-8777 or larencee@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Other key contributors to this report were Ronald J. Salo, Eric W. Clemons, R. Eric Erdman, Susan L. Conlon, Michele C. Fejfar, Kathryn E. Godfrey, Richard B. Hung, Thomas F. Lombardi, Jan B. Montgomery, and Danny R. Burton.



Eileen Larence
Director, Homeland Security and Justice Issues

Appendix I: Objectives, Scope, and Methodology

Objectives

In response to a request from the Chairman of the House Judiciary Committee and the Ranking Member of the House Committee on Homeland Security, we addressed the following questions:

- To what extent are the numbers of terrorist watch list misidentifications known, and generally, how could misidentified persons be affected?¹
- What are the major reasons that misidentifications occur, and what actions are the Terrorist Screening Center and frontline-screening agencies taking to reduce the number of misidentified persons or expedite them through the screening process?
- To address concerns from misidentified and mistakenly listed persons, what opportunities for redress have the Terrorist Screening Center and frontline-screening agencies established?²

Scope and Methodology

Our work generally focused on the screening of travelers, although the terrorist watch list is used for a variety of other screening purposes, such as conducting background checks of workers who have access to secure areas of the national transportation system. In performing our work, we focused on the Terrorist Screening Center and three frontline-screening agencies—the Transportation Security Administration, U.S. Customs and Border Protection, and the Department of State—whose missions most frequently and directly involve interactions with travelers. At the Terrorist Screening Center, we interviewed key officials—including the director, principal deputy director, chief information officer, and privacy officer—and reviewed standard operating procedures and other relevant documentation.

Regarding the screening of air passengers against the No Fly and Selectee lists prior to boarding, in addition to contacting the Transportation Security Administration to broadly discuss the procedures of air carriers,

¹For purposes of this report, the term “misidentification” refers to a person initially matched by a screening agency to a name on the watch list, but upon closer examination, the person is found to not match any watch list record.

²As used in this report, the term “mistakenly listed persons” includes two categories of individuals—(1) persons who never should have been included on the watch list but were due to some type of error and (2) persons who were appropriately included on the watch list at one time but no longer warrant inclusion on the terrorist watch list due to subsequent events.

Appendix I: Objectives, Scope, and Methodology

we interviewed security officials at five major, domestic air carriers. At their request, the air carriers are not identified in this report. Regarding U.S. Customs and Border Protection's screening of travelers entering the United States, besides conducting work at the agency's headquarters in Washington, D.C., we visited various land and air ports of entry in four states—California, Michigan, New York, and Texas (see table 2). We judgmentally selected these four states because each has major land and air ports of entry. Also, the four states are geographically dispersed and collectively have ports of entry on both the northern and southern borders of the United States.

Table 2: U.S. Customs and Border Protection Ports of Entry Visited by GAO

State	Land ports of entry	Air ports of entry
California	San Ysidro	Los Angeles International Airport
Michigan	Detroit Port Huron	Detroit Metropolitan Airport
New York	Niagara Falls	John F. Kennedy International Airport
Texas	Laredo	Dallas/Fort Worth International Airport

Source: GAO.

Regarding the State Department, we focused on screening of applicants for nonimmigrant visas.³ We performed our work at State Department headquarters in Washington, D.C, and did not visit consular offices abroad.

More details about the scope and methodology of our work regarding each of the objectives are presented in the following sections, respectively.

Extent That the Numbers of Terrorist Watch List Misidentifications Are Known, and Generally, How Misidentified Persons Could Be Affected

From the Terrorist Screening Center, we obtained statistical information on misidentifications covering a 26-month time period—December 2003 (when the center began operations) to January 2006. These statistics are based on screening encounters that were referred for identity verification to the center by the frontline-screening agencies, particularly U.S. Customs and Border Protection, which conducts screening at ports of entry, and the Transportation Security Administration, which provides guidance to air

³A nonimmigrant is a person, not a citizen or national of the United States, seeking to enter the United States temporarily for a specific purpose, such as business or pleasure.

Appendix I: Objectives, Scope, and Methodology

carriers, receives encounter inquiries from them, and makes applicable referrals to the center. Frontline-screening agencies are able to resolve some misidentifications on their own without having to refer them to the center. Similarly, in following federal guidance, airlines may also resolve some misidentifications without involving the Transportation Security Administration or necessitating subsequent referrals to the Terrorist Screening Center. However, the agencies and airlines generally do not maintain readily available statistics on how often they do so. Thus, we were unable to quantify the universe of terrorist watch-list-related misidentifications. However, to provide a contextual perspective, we obtained national statistics on the numbers of persons who were subject to terrorist watch list screening procedures conducted, for example, in fiscal year 2005 at ports of entry.

To determine how misidentified persons could be affected, we interviewed officials at the principal frontline-screening agencies—the Transportation Security Administration, U.S. Customs and Border Protection, and the Department of State—whose missions most frequently and directly involve interactions with travelers. Also, as indicated in table 2, we made on-site observations of U.S. Customs and Border Protection screening operations at various ports of entry in California, Michigan, New York, and Texas. Our observations at these locations helped us better understand how the name-match screening process can affect misidentified persons, but these observations are not projectable to other locations.

To obtain additional information on ways that misidentified individuals could be affected by terrorist-watch-list-related screening, we asked the Transportation Security Administration and U.S. Customs and Border Protection to provide us examples of actual complaint letters to review:

- The Transportation Security Administration provided us a selection of 24 terrorist watch-list-related complaint letters that the agency received during December 1, 2003 (when the Terrorist Screening Center became operational) to April 20, 2006. The agency attempted to select letters from different weeks throughout this time period; however, because a statistically projectable methodology was not used for the selections, the 24 letters are not representative of all complaints or inquiries (an unspecified total) that the Transportation Security Administration received during this time period.
- U.S. Customs and Border Protection’s National Targeting Center provided us a selection of complaint letters submitted by 28 individuals. The dates of the 28 complaint letters encompassed an 11-month period, ranging from

Appendix I: Objectives, Scope, and Methodology

June 2005 to April 2006. The 28 letters were not selected based on a statistically projectable methodology. Thus, the 28 letters are not representative of all complaints or inquiries—regarding watch-list-related secondary screening at ports of entry—that U.S. Customs and Border Protection’s Customer Satisfaction Unit received during the 11-month time period and forwarded for research to the agency’s National Targeting Center.⁴

The scope of our work did not include contacting or interviewing any of the individuals who submitted complaint letters to the Transportation Security Administration or U.S. Customs and Border Protection.

To further identify ways that misidentified persons could be affected by watch-list-related screening, we contacted various associations that represent air carriers, travel agencies, and business travelers. Specifically, we contacted (1) the Air Transport Association, a trade organization of the principal U.S. airlines; (2) the American Society of Travel Agents; and (3) the National Business Travel Association, which represents corporate travel management professionals and the travel industry.

Also, we reviewed the results of a survey that the National Business Travel Association conducted in June 2006. According to its Web site (www.nbta.org), the association represents over 2,500 corporate travel managers and travel service providers who collectively manage and direct more than \$170 billion of expenditures within the business travel industry, primarily for Fortune 1,000 companies. In June 2006, the association conducted a survey of 1,316 corporate travel managers; the survey posed a range of questions that addressed how terrorist watch list screening by the Transportation Security Administration and air carriers affected travelers. A total of 444 corporate travel managers responded to the survey. The responses may not be representative of all of the association’s corporate travel managers.

⁴According to Customer Satisfaction Unit managers, all complaints regarding the terrorist watch list are forwarded to the agency’s National Targeting Center, which has access to classified information that may be needed to determine if the incidents cited by complainants involved individuals who either are on the watch list or were misidentified. National Targeting Center managers told us that if research indicates that the substance of the complaint does involve watch-list-related screening conducted by U.S. Customs and Border Protection, the National Targeting Center will draft a response letter, which is to be signed by the Customer Satisfaction Unit and mailed to the individual.

Appendix I: Objectives, Scope, and Methodology

Major Reasons That Misidentifications Occur, and Actions the Terrorist Screening Center and Frontline-Screening Agencies Are Taking to Reduce the Number of Misidentified Persons or Expedite Them through the Screening Process

Major Reasons That Misidentifications Occur

Regarding why misidentifications occur, our work focused on interviewing officials at and reviewing documentation obtained from the Terrorist Screening Center and three frontline-screening agencies—the Transportation Security Administration, U.S. Customs and Border Protection, and the Department of State. We also interviewed security officers at five major domestic air carriers about their role in name-match screening against the No Fly and Selectee lists and obtained their views on the causes of misidentifications. Further, we reviewed the work of two groups regarding factors they have identified that contribute to misidentifications—the Terrorist Screening Center’s Search Engine Standardization Working Group⁵ and the Department of Homeland Security’s Data Privacy and Integrity Advisory Committee.⁶

Actions to Reduce the Number of Misidentified Persons or Expedite Them through the Screening Process

At the Terrorist Screening Center, we interviewed the director, principal deputy director, chief information officer, and other senior managers and staff regarding data-quality initiatives, including efforts to identify and correct troublesome records related to misidentifications. Additionally, we inquired about the status of the center’s efforts to implement recommendations made by the Department of Justice’s Office of the

⁵The working group’s membership includes representatives from the departments of Homeland Security (including Transportation Security Administration and U.S. Customs and Border Protection), State, and Defense; FBI; and the intelligence community (e.g., the National Counterterrorism Center, Central Intelligence Agency, National Security Agency, and Defense Intelligence Agency). Also, the National Institute of Standards and Technology acts as a special advisor to the working group.

⁶The charter of the committee is to advise the Secretary of Homeland Security and the Department of Homeland Security’s chief privacy officer on programmatic, policy, operational, administrative, and technological issues within the department’s areas of responsibility that affect individual privacy, data integrity, data interoperability, and other privacy-related matters.

Appendix I: Objectives, Scope, and Methodology

Inspector General in its June 2005 report.⁷ Among other things, the Inspector General recommended that the Terrorist Screening Center develop procedures to regularly review and test the information contained in the consolidated terrorist watch list to ensure that the data are complete, accurate, and nonduplicative.

At the three frontline-screening agencies, we interviewed applicable program managers regarding initiatives being taken to expedite frequently misidentified persons through the screening process. We inquired particularly about any computer-based initiatives that use applicable databases to help ensure that travelers who have been frequently misidentified in the past are no longer subjected to intensive screening, unless warranted by new data.

In further reference to potential initiatives for minimizing misidentifications as well as better confirming the identities of terrorists, we reviewed the Terrorist Screening Center's strategic plan and discussed with center officials the outlook for using biometric data—such as fingerprints—to supplement name-based screening. Similarly, in our interviews with officials of the frontline-screening agencies, we discussed programs that currently use biometric data, such as the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which is an entry-exit tracking system designed to collect, maintain, and share information on selected foreign nationals who travel to the United States.

Redress Opportunities Established by the Terrorist Screening Center and Frontline-Screening Agencies to Address Concerns from Misidentified and Mistakenly Listed Persons

As used in this report, the term “redress” generally refers to an agency’s complaint-resolution process, whereby individuals may seek resolution of their concerns about an agency action. We identified elements of the opportunities for redress offered by the Terrorist Screening Center and the three frontline-screening agencies, and we generally analyzed their respective policies and procedures. However, we did not address the relation between agency redress and other possible remedies, such as judicial review, which involves invoking the legal system through a civil action. Rather, the scope of our work focused on means for redress made available by agencies for inconvenienced persons.

⁷Department of Justice, Office of the Inspector General, *Review of the Terrorist Screening Center*, Audit Report 05-27 (June 2005).

Appendix I: Objectives, Scope, and Methodology

We reviewed the Terrorist Screening Center's standard operating procedures for redress and interviewed the center official (privacy officer) principally responsible for watch-list-related redress. Also, we obtained and reviewed statistics and general disposition or outcome information regarding redress queries that the center received and processed to completion in calendar year 2005.⁸

Further, at the three frontline-screening agencies, we reviewed redress-related documentation, including standard operating procedures and training materials, and we interviewed the officials responsible for redress. Specifically, we interviewed the Director of the Transportation Security Administration's Office of Transportation Security Redress, the head of U.S. Customs and Border Protection's Customer Satisfaction Unit, and program managers at the State Department's Bureau of Consular Affairs responsible for processing nonimmigrant visa applications.

Also, to generally determine what watch-list-related redress information was publicly available, we reviewed the Federal Bureau of Investigation's Web site for the Terrorist Screening Center. In turn, from that overview Web site (see app. II), we followed up on any online links or references to the redress processes of the Transportation Security Administration (see app. III), U.S. Customs and Border Protection (see app. IV), and the State Department.

In addition, we contacted the Department of Justice's Office of Legal Policy, which has a lead role in ongoing efforts to develop an interagency memorandum of understanding to help ensure that redress processes are formally documented, with clearly established responsibilities for the Terrorist Screening Center and all interagency partners. Also, we contacted the executive director of the Privacy and Civil Liberties Oversight Board to discuss its role in facilitating development of the

⁸The Terrorist Screening Center defines a "redress query" as communication from individuals or their representatives inquiring or complaining about an adverse experience during a terrorist watch-list-related-screening process conducted or sponsored by a federal agency, including congressional inquiries to federal agencies on behalf of their constituents.

Appendix I: Objectives, Scope, and Methodology

interagency memorandum of understanding.⁹ However, because the memorandum of understanding was in draft form at the time of our study, we have not had an opportunity to review it.

Data Reliability

In addressing our objectives, we obtained the following statistics from the Terrorist Screening Center:

- The number of watch-list-related screening encounters referred to the center by frontline-screening agencies during the period December 2003 to January 2006.
- The number and general dispositions of redress queries that the center received and processed to completion in calendar year 2005.

We discussed the sources of the data with Terrorist Screening Center officials, including the chief information officer, and we reviewed documentation regarding the compilation of the statistics. We determined that the statistics were sufficiently reliable for the purposes of presenting overall patterns and trends.

⁹The five-member board, which is part of the Executive Office of the President, was established by section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004. Pub. L. No. 108-458, 118 Stat. 3638, 3684-88. The board advises the president and other senior executive branch officials as to whether privacy and civil liberties protections are appropriately considered in the development and implementation of laws, regulations, and executive branch policies related to efforts to protect the nation against terrorism. The five board members were sworn in and had their first meeting on March 15, 2006. Additional information about the role of the board and its operations is available at www.privacyboard.gov.

Appendix II: Terrorist Screening Center: Terrorist-Watch-List Redress Process

This appendix, which consists of two sections, presents publicly available information that we copied from the Web site of the Federal Bureau of Investigation:

- The first section of the appendix is an overview of the Terrorist Screening Center’s watch-list-related redress process and also presents contact information for three frontline-screening agencies—the Transportation Security Administration, U.S. Customs and Border Protection, and the Department of State.
- The second section covers frequently asked questions.

Overview and Contact Information

[Copied from the FBI’s Web site, www.fbi.gov. Accessed August 2006.]

“The Terrorist Screening Center cannot confirm or deny whether an individual is on the consolidated terrorist watch list, because this information is derived from classified and sensitive law enforcement and intelligence. The nondisclosure of the contents of the watch list protects the operational counterterrorism and intelligence collection objectives of the government, as well as the personal safety of those involved in counterterrorism investigations. The watch list remains an effective tool in the government’s counterterrorism efforts because its contents are not disclosed.

“The Terrorist Screening Center works with other agencies on a daily basis to resolve complaints from individuals who are experiencing repeated delays or difficulties during a screening process that may be related to the terrorist watch list. Because individuals may experience problems during screening for any number of reasons, and not just because of the terrorist watch list, individuals should contact the agency that is conducting the screening process in question. The screening agency is in the best position to resolve issues.

“Contact information:

“The Terrorist Screening Center does not accept redress inquiries directly from the public. Members of the public should contact the relevant screening agency with complaints about a negative screening experience.

“Please direct the public to contact the following screening agencies to submit a complaint about a negative screening experience.

**Appendix II: Terrorist Screening Center:
Terrorist-Watch-List Redress Process**

For air passenger screening:

Transportation Security Administration Ombudsman
Phone: (866) 289-9673
Email: tsa-contactcenter@dhs.gov
Online: TSA Traveler Identity Verification Program¹

For U.S. borders and ports of entry:

Customs and Border Protection
Customer Satisfaction Unit²
1300 Pennsylvania Ave., NW, Room 5.5C
Washington, DC 20229
Phone: (202) 344-1968
Fax: (202) 344-2791
Online: Interagency Border Inspection System Fact Sheet³

For visas:

Director, Information Management Liaison (CA/VO/I)
Bureau of Consular Affairs, SA-1
U.S. Department of State
Washington, D.C. 20520
FAX: (202) 663-3535
Online: Bureau of Consular Affairs³

“Frequently Asked Questions”

[Copied from the FBI’s Web site, www.fbi.gov. Accessed August 2006.]

¹See appendix III.

²On September 12, 2006, in providing technical comments on a draft of this report, U.S. Customs and Border Protection officials noted that the contact information given on the FBI’s Web site should be as follows: U.S. Customs and Border Protection, Freedom of Information Act/Privacy Act Branch. Also, the comments noted that the telephone number should be removed. We suggested to the U.S. Customs and Border Protection officials that they coordinate with the FBI to ensure that appropriate contact information is available to the public.

³See appendix IV for a copy of the fact sheet.

**Appendix II: Terrorist Screening Center:
Terrorist-Watch-List Redress Process**

“Why was the Terrorist Screening Database created?”

Prior to the creation of the terrorist-screening database, information about known or suspected terrorists was dispersed throughout the U.S. government and no one agency was charged with consolidating it and making it available for use in terrorist screening. Under Homeland Security Presidential Directive-6, the Terrorist Screening Center now provides “one-stop shopping” so that every government screener is using the same terrorist watch list—whether it is an airport screener, an embassy official issuing visas overseas, or a state or local law enforcement officer on the street. The Terrorist Screening Center allows government agencies to run name checks against the same comprehensive list with the most accurate, up-to-date information about known and suspected terrorists.

Who gets included in the terrorist-screening database?

Per Homeland Security Presidential Directive-6, only individuals who are known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism are included in the terrorist-screening database.

Does the terrorist screening database contain information on domestic terrorists, like Timothy McVeigh?

Yes. The terrorist-screening database contains information on both international and domestic terrorists.

Does the terrorist-screening database contain information on people who have been convicted of a crime?

The purpose of the terrorist-screening database is not to hold information on individuals who have been convicted of a crime; however, an individual appropriately included in the terrorist-screening database may also have a criminal history. None of the information pertaining to the criminal history is contained or referenced in the terrorist-screening database.

Are there U.S. citizens in the terrorist-screening database?

Yes, U.S. citizens are included in terrorist-screening database if they meet the Homeland Security Presidential Directive-6 terrorism nexus criteria.

**Appendix II: Terrorist Screening Center:
Terrorist-Watch-List Redress Process**

Can I find out if I am in the terrorism screening database?

The Terrorist Screening Center cannot reveal whether a particular person is in the terrorist-screening database. The terrorist-screening database remains an effective tool in the government's counterterrorism efforts because its contents are not disclosed. If the Terrorist Screening Center revealed who was in the terrorist-screening database, terrorist organizations would be able to circumvent the purpose of the terrorist watch list by determining in advance which of their members are likely to be questioned or detained.

I am having trouble when I try to fly or cross the border into the United States. Does this mean I am in the terrorist-screening database?

No. At security checkpoints like our nation's borders, there are many law enforcement or security reasons that an individual may be singled out for additional screening. Most agencies have redress offices (e.g., Ombudsman) where individuals who are experiencing repeated problems can seek help. If an individual is experiencing these kinds of difficulties, he/she should cooperate with the agency screeners and explain the recurring problems. The screeners can supply instructions on how to raise concerns to the appropriate agency redress office.

I have been told that I am on a terrorist watch list by an airline employee and I frequently have difficulty when I fly. Does this mean I am in the terrorist-screening database?

No; however, an individual may be a "misidentified person." A misidentified person is someone who is experiencing a delay during screening because they have a similar name to a person in the terrorist-screening database. Misidentified persons are sometimes delayed while the government works to distinguish them from the terrorist in the terrorist-screening database. Because these delays are frustrating and inconvenient, there are several initiatives in progress to help streamline the clearance process for misidentified persons. If an individual believes he/she is having a misidentification problem, he/she should contact the screening agency's redress office for assistance.

**Appendix II: Terrorist Screening Center:
Terrorist-Watch-List Redress Process**

Are individuals removed from the terrorist-screening database?

Yes. The Terrorist Screening Center works with partner agencies through a formal process to remove individuals who no longer meet the Homeland Security Presidential Directive-6 terrorism criteria.

How does the Terrorist Screening Center ensure that the terrorist-screening database is accurate?

The Terrorist Screening Center has a staff dedicated to redress and quality assurance that conducts comprehensive as well as case-specific reviews of terrorist-screening database records to ensure they are current, accurate, and thorough. The Terrorist Screening Center conducts research and coordinates with other federal agencies to ensure the terrorist record is as complete, accurate, and thorough as possible. The Terrorist Screening Center's redress and quality assurance process has resulted in the correction or removal of hundreds of records in the terrorist-screening database.

What are the Terrorist Screening Center's redress procedures?

See the TSC Redress Procedures webpage for details. [GAO note: The procedures are copied in the first section of this appendix.]

Does the Transportation Security Administration's Secure Flight program have anything to do with the terrorist-screening database?

Secure Flight is a congressionally mandated program that will check the names and dates of birth of passengers on domestic flights against the terrorist-screening database. As with all government programs that screen for terrorists, the Terrorist Screening Center provides this program support to ensure that terrorist identity matches are correct.

What prevents the Terrorist Screening Center from violating the civil liberties of Americans?

The Terrorist Screening Center only receives information collected by other government entities with pre-existing authority to do so. Each agency that contributes data to the Terrorist Screening Center must comply with legislation, as well as its own policies and procedures to protect privacy rights and civil liberties. The handling and use of information, including information about U.S. citizens and legal immigrants, is governed by the same statutory, regulatory, and

**Appendix II: Terrorist Screening Center:
Terrorist-Watch-List Redress Process**

constitutional requirements as if the information was not to be included in a Terrorist Screening Center managed database.”

Appendix III: Transportation Security Administration: Traveler Identity Verification Program

This appendix presents an overview of the Transportation Security Administration's (TSA) traveler identity verification program for air passengers who are affected by terrorist watch list screening. An individual can voluntarily provide TSA with additional personal-identifying information, which the agency will use to decide whether the person's name should be put on a cleared list—that is, a list that contains the names and other personal-identifying information of individuals who have been checked and cleared as being persons not on the No Fly and Selectee lists. Airlines are to use the cleared list to more quickly determine that these passengers are not the persons whose names are on the No Fly and Selectee lists. As needed, TSA provides the airlines with updates of the No Fly and Selectee lists and the cleared list.

Specific information about TSA's traveler identity verification program is publicly available on the agency's Web site (www.tsa.gov). The following sections of this appendix reproduce—as exhibits A and B—relevant information from TSA's Web site (accessed August 2006):

- Exhibit A: Our Traveler Identity Verification Program.
- Exhibit B: Traveler Identity Verification (TSA Form 2301, May 2006). Generally, to participate in the program, an individual must complete a traveler identity verification form and return the form and copies of specified identity documents to TSA.

Exhibit A: “Our Traveler Identity Verification Program”

“Told that you are on a Federal Government Watch List?

Problems printing your boarding pass at the kiosk or from home?

Experience other delays while checking-in for flights?

Our Office of Transportation Security Redress is here to help with our new Traveler Identity Verification Program.

Why am I having these problems?

TSA and the airlines are required to check and confirm that you are properly identified prior to your flight for safety and security. You may experience inconveniences when you present your identification during check-in due to mistaken identity or incorrect information. Our Traveler Identity Verification Program works with the relevant parties (including airlines) to resolve any inaccuracies or inconsistencies that may have resulted in misidentifications.

**Appendix III: Transportation Security
Administration: Traveler Identity Verification
Program**

Am I on the No-Fly List?!

If you receive a boarding pass, you are not on the No-Fly List. Most commonly, passengers who are told that they are on the No-Fly List have, in fact, a similar name to an individual on the Watch Lists.

What do I need to do?

You are invited to participate in the TSA Traveler Identity Verification Program by completing and returning the following information to TSA:

- Traveler Identity Verification Form (WORD 145 KB)
- A copy of your U.S. passport OR
- Copies of three of the following:
 - Driver's License
 - Birth Certificate
 - Voter Registration
 - Military ID Card
 - Visa
 - Naturalization Card
 - Government ID Card

How does TSA review my information?

Your submission is reviewed to determine if the delays are caused by mistaken identity or incorrect information. TSA will respond to you in writing and provide air carriers with your identifying information to help properly identify you at check-in and expedite your future travel.

I participated in the Traveler Identity Verification Program, but I'm still experiencing problems.

Airline check-in procedures must still be followed. We currently distribute the Watch Lists to the airlines, who compare your reservation information to the Watch Lists prior to your flight. The airlines use varying procedures and technology to conduct this comparison, which could inadvertently lead to continued delays.

We are developing a program called Secure Flight to enhance the security of air travel in the U.S. while reducing security-related delays for the traveling public. It will allow the federal government, instead of individual airlines, to compare passenger data against the Watch Lists prior to check-in at the airport, while fully protecting privacy and civil liberties.

**Appendix III: Transportation Security
Administration: Traveler Identity Verification
Program**


Our goal going forward is to ensure travelers' security with minimal disruptions.

Please note that you will be subject to screening procedures at the checkpoint. Every passenger will still walk through a metal detector, their carry-on bags will still be X-rayed, and every checked bag will still be screened for explosives. Additionally, you may be randomly selected at the airline counter or upon arrival at the checkpoint for secondary screening.

We will continue to work with travelers to minimize any unnecessary delays. We will continue to look at process and technology improvements to ensure a safe and efficient travel experience.”

Appendix III: Transportation Security Administration: Traveler Identity Verification Program

Exhibit B: Traveler Identity Verification (TSA Form 2301, May 2006)



Transportation Security Administration

Traveler Identity Verification

Instructions: Complete all fields and mail to the Office of Transportation Security Redress (address below)

Personal Information

Full Name: _____

First Middle Last

Social Security No.: _____ Birth Date: ____/____/____ Birthplace: _____

mm/dd/yy City or Town/Province/Country

Sex: Male Female Height: _____ Weight: _____ Hair Color: _____ Eye Color: _____

Contact Information

Current Address: _____

Street Number and Name Apt. no.

City or Town State or Province Zip Code

Home Telephone No.: (____) _____ - _____ Work Telephone No.: (____) _____ - _____

I. Required Documentation and Information


You must provide either a copy of a U.S. Passport (Passport No. must be clearly visible) or at least three (3) of the following documents in order for your request to be processed. Check the box next to the document(s) that you are submitting with this completed form and enter the requested information for each in the space provided.

Documentation	Information
<input type="checkbox"/> U.S. Passport	Registration No.: _____ Place of issuance: _____
OR	
<input type="checkbox"/> Birth Certificate	Registration No.: _____ Place of issuance: _____
<input type="checkbox"/> Certificate of Citizenship	Certificate No.: _____ Place of issuance: _____
<input type="checkbox"/> Certificate of Release or Discharge from Active Duty (DD Form 214)	Discharge date: _____ Check one: <input type="checkbox"/> Air Force <input type="checkbox"/> Army <input type="checkbox"/> Marines <input type="checkbox"/> Navy <input type="checkbox"/> Coast Guard
<input type="checkbox"/> Drivers License	License No.: _____ State of issuance: _____
<input type="checkbox"/> Government Identification Card	Badge No.: _____ Check one: <input type="checkbox"/> Federal <input type="checkbox"/> State <input type="checkbox"/> Local
<input type="checkbox"/> Immigrant/Nonimmigrant Visa	Control no.: _____
<input type="checkbox"/> Military Identification Card	Card No.: _____ Check one: <input type="checkbox"/> Air Force <input type="checkbox"/> Army <input type="checkbox"/> Marines <input type="checkbox"/> Navy <input type="checkbox"/> Coast Guard
<input type="checkbox"/> Naturalization Certificate	Certificate No.: _____ State of issuance: _____ Country of issuance: _____
<input type="checkbox"/> Non U.S. Passport	Registration No.: _____ Country of issuance: _____
<input type="checkbox"/> Voter Registration Card	Card No.: _____ State of issuance: _____

TSA Form 2301, May 2006

1 of 2

Appendix III: Transportation Security Administration: Traveler Identity Verification Program

	Transportation Security Administration	Traveler Identity Verification
<p>IV. Acknowledgement</p> <p>The information I have provided on this form is true, complete, and correct to the best of my knowledge and is provided in good faith. I understand that knowingly and willfully making any materially false statement, or omission of a material fact, on this form can be punished by fine or imprisonment or both (see section 1001 of Title 18 United States Code).</p> <p>I understand the above information and am voluntarily submitting this information to the Transportation Security Administration.</p>		
Print or Type Name	Signature	Date
<p>PRIVACY ACT STATEMENT: Authority: The authority for collecting this information is 49 U.S.C. § 114. Principal Purpose(s): This voluntary submission is provided to afford you the ability to confirm your identity as distinct from an individual on a Federal Watch List. Your Social Security Number (SSN) will be used to verify your identity. Furnishing this information, including your SSN, is voluntary; however, the Transportation Security Administration may not be able to confirm your identity without this information. Routine Uses: Routine uses of this information include disclosure to appropriate governmental agencies for law enforcement or security purposes, or to airports or air carriers to verify your identity for purposes of security screening.</p>		
<p>Mailing Instructions Please mail the completed form and copies of identity documents to:</p> <p style="margin-left: 40px;">Office of Transportation Security Redress Transportation Security Administration 601 South 12th Street, TSA-901 Arlington, VA 22202</p>		
<p>Faxing Instructions Please fax the completed form and copies of identity documents to:</p> <p style="margin-left: 40px;">(866) 672-8640 or (571) 227-1925</p>		
TSA Form 2301, May 2006		2 of 2

Appendix IV: U.S. Customs and Border Protection: Online Information

Background and Preliminary Observation

Appendix II provides an overview of the redress process used by the Terrorist Screening Center for addressing complaints or concerns resulting from the use of terrorist watch lists to screen individuals. As stated in appendix II, the Terrorist Screening Center is to work with frontline-screening agencies to resolve complaints from individuals who are experiencing repeated delays or difficulties during a screening process that may be related to a terrorist watch list. For instance, the Terrorist Screening Center's overview guidance notes that complainants experiencing such problems at U.S. borders and ports of entry should contact U.S. Customs and Border Protection. In further reference to the redress process for misidentifications of these individuals, the overview guidance provides an online link to the U.S. Customs and Border Protection's Interagency Border Inspection System Fact Sheet (reproduced below). The fact sheet does not specifically mention terrorist watch lists and the redress process.

However, U.S. Customs and Border Protection's Web site (www.cbp.gov), which can be directly accessed by the public, does provide information regarding the agency's Customer Satisfaction Unit and how complaints are handled as well as information on trusted-traveler programs.

Interagency Border Inspection System Fact Sheet

GAO note: The fact sheet consists solely of the following six questions and answers, which we copied from the Web site of U.S. Customs and Border Protection (accessed August 2006).

“What Is IBIS?”

“IBIS is the acronym for the Interagency Border Inspection System.”

“Who Uses IBIS?”

“In addition to U.S. Customs and Border Protection, law enforcement and regulatory personnel from 20 other federal agencies or bureaus use IBIS. Some of these agencies are the Federal Bureau of Investigation; U.S. National Central Bureau of the International Criminal Police Organization; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Internal Revenue Service; the Coast Guard; the Federal Aviation Administration; the Secret Service; and the Animal and Plant Health Inspection Service, just to name a few. Also, information from IBIS is shared with the Department of State for use by Consular Officers at U.S. Embassies and Consulates.”

**Appendix IV: U.S. Customs and Border
Protection: Online Information**

“What Does IBIS Provide?” “IBIS assists the majority of the traveling public with the expeditious clearance at ports of entry while allowing the border enforcement agencies to focus their limited resources on those potential non-compliant travelers. IBIS provides the law enforcement community with access to computer-based enforcement files of common interest. It also provides access to the FBI’s National Crime Information Center and allows its users to interface with all fifty states via the National Law Enforcement Telecommunications Systems.”

“Where Is IBIS?” “IBIS resides on the Treasury Enforcement Communications System at the U.S. Customs and Border Protection’s Data Center. Field level access is provided by an IBIS network with more than 24,000 computer terminals. These terminals are located at air, land, and sea ports of entry.”

“What Information Is in IBIS?” “IBIS keeps track of information on suspect individuals, businesses, vehicles, aircraft, and vessels. IBIS terminals can also be used to access National Crime Information Center records on wanted persons, stolen vehicles, vessels or firearms, license information, criminal histories, and previous Federal inspections. The information is used to assist law enforcement and regulatory personnel.”

“Additional Questions?” “Any concerns you may have as an international traveler or importer about the use or application of IBIS may be addressed to:

U.S. Customs and Border Protection
Freedom of Information Act/
Customer Satisfaction Unit
Room 5.5 C
1300 Pennsylvania Avenue, N.W.
Washington, D.C. 20229”

Appendix V: Comments from the Department of Homeland Security

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



**Homeland
Security**

September 15, 2006

Ms. Eileen Larence
Director
Homeland Security and Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Larence:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO's) draft report entitled, *TERRORIST WATCH LIST SCREENING: Efforts to Help Reduce Adverse Effects on the Public* (GAO-06-1031). Technical comments have been provided under separate cover.

The Department of Homeland Security appreciates your report and findings as well as your recognition of the many efforts we are currently undertaking to enhance terrorist screening and our redress efforts.

We do have one suggestion for an additional paragraph in your report, perhaps in your Results in Brief and Concluding Observations sections.

The Department of Homeland Security is working with the Departments of Justice, State and others on a larger set of travel screening redress issues, which the interagency memorandum of understanding, with its focus on redress related to the terrorist watch lists, will supplement. On January 17, 2006, the Departments of State and Homeland Security announced an initiative on "Secure Borders and Open Doors in the Information Age," otherwise known as the Rice-Chertoff Initiative. Part Three, "Smarter Screening," includes a "One Stop' Redress for Travelers." The purpose is to establish a government-wide redress process to address perceived problems in international and domestic traveler prescreening. Secretary Chertoff made it a goal to establish this process by the end of the calendar year so that those with complaints or legitimate issues can resolve them with greater efficiency. US-VISIT and the Office for Civil Rights and Civil Liberties (CRCL) within DHS have been tasked with initiating from within the relevant DHS components and the Department of State a governance board and working group for this project. The new director of DHS's Screening Coordination Office now chairs the governance board with CRCL and US-VISIT as co-chairs. Representatives from State, the Terrorist Screening Center, and

www.dhs.gov

**Appendix V: Comments from the Department
of Homeland Security**

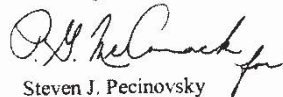
Appendix V: Comments from the Department
of Homeland Security

2

DHS's U.S. Customs and Border Protection, Transportation Security Administration, U.S. Immigration and Customs Enforcement, US-VISIT, CRCL and Office of Policy are all involved with the working group.

Thank you again for the opportunity to comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,



Steven J. Pecinovsky
Director
Departmental GAO/OIG Liaison Office

Appendix VI: Comments from the State Department



United States Department of State

*Assistant Secretary for Resource Management
and Chief Financial Officer*

Washington, D.C. 20520

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

SEP 14 2006

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "TERRORIST WATCH LIST SCREENING: Efforts to Help Reduce Adverse Effects on the Public," GAO Job Code 440374.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Timothy Smith, Chief, Coordination Division, Bureau of Consular Affairs at (202) 663-1246.

Sincerely,

A handwritten signature in black ink, appearing to read "Bradford R. Higgins".

Bradford R. Higgins

cc: GAO – Dan Burton
CA – Maura Harty
State/OIG – Mark Duda

Appendix VI: Comments from the State
Department

Department of State Comments on GAO Draft Report

**Terrorist Watch List Screening: Efforts to Help Reduce
Adverse Effects on the Public**
(GAO-06-1031, GAO Code 440374)

Thank you for allowing the Department of State the opportunity to comment on the draft report *Terrorist Watch List Screening: Efforts to Help Reduce Adverse Effects on the Public*.

The report accurately describes the visa process and the Department of State's position that the administrative processing time required to screen a visa applicant, including, if required, the processing of a Security Advisory Opinion (SAO) review, is a necessary part of the visa application procedure rather than an adverse governmental action. The report also acknowledges the Department's interest in data integrity and taking steps to minimize the impact of the SAO process on the traveling public. (Note: the SAO process is the means through which Department of State Consular Officers screen visa applicants against the Terrorist Watch List.)

The Department has the following comments:

1. The GAO notes, first on the page immediately following the report cover sheet and several times throughout the document, that of the tens of thousands of names sent to the Terrorist Screening Center (TSC) by the frontline screening agencies, about half were "misidentifications." From the perspective of the State Department, which uses the Terrorist Watch List primarily as a screening tool for visa adjudication, a "misidentification" is not an adverse result for the visa applicant. Rather, a negative response would clear a visa applicant of an association with a terrorist identity (though subject to a second review upon seeking admission at a U.S. port of entry.)
2. The description of the Department's visa name check process in the body of the report is accurate. However, the general overview description and chart on pages 11-13 are not accurate as descriptions of the visa SAO process. The description and chart state that "inconclusive ... uncertain and other hard-to-verify potential matches..." are to be referred to the applicable screening agency. If that agency is unable to conclusively determine whether a hit is an exact match, then it contacts the Terrorist

Appendix VI: Comments from the State
Department

2

Screening Center. In describing visa operations, it is more accurate to say (and depict on a chart) that consular officers are required to submit to the Department for a Security Advisory Opinion *all hits that cannot positively be labeled a mismatch*. That SAO request is automatically routed to the TSC and other screening agencies, and the Department will not recommend a course of action to a post until the TSC and other screening agencies have advised us that either the hit is a mismatch, or that derogatory information exists and must be reviewed to determine whether a legal basis for a visa denial exists.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

EXHIBIT 93
FILED UNDER SEAL

EXHIBIT 94
FILED UNDER SEAL

EXHIBIT 95



AUDIT OF THE U.S. DEPARTMENT OF JUSTICE TERRORIST WATCHLIST NOMINATION PROCESSES

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 08-16
March 2008

Audit of the Department of Justice's Terrorist Watchlist Nomination Processes

The U.S. government maintains a consolidated terrorist watchlist as a key component of its counterterrorism efforts. This list, maintained by the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC), was created by merging previously separate watchlists maintained by different agencies throughout the federal government. The consolidated terrorist watchlist is updated daily with new or revised information on known or suspected terrorists. This information is obtained by a variety of government agencies, including law enforcement agencies in the Department of Justice (DOJ).

As part of a coordinated review by other Offices of Inspector General (OIG) in the Intelligence Community, this DOJ OIG audit examined the DOJ's nomination of known or suspected terrorists to the consolidated terrorist watchlist. The objectives of this audit were to determine whether: (1) DOJ's processes and standards for nominating individuals to the consolidated watchlist are consistent, are articulated in policy or other guidance, and are understood by nominators; (2) DOJ components have quality control processes to help ensure nominations are accurate, understandable, updated with new information, and include all individuals who should be placed on the watchlist based on information available to the agencies; (3) the responsibility for watchlist nominations is clear, effective, and understood; (4) nominators receive adequate training, guidance, or information on the nominations process; (5) DOJ components maintain records of their nominations, including the source of the nomination and what information was provided; and (6) DOJ organizations with terrorism, counterterrorism, and domestic counterterrorism information in their possession, custody, or control appropriately participate in the nominations process.

Our audit was conducted in conjunction with other OIGs who examined similar issues at other agencies in the Intelligence Community. This interagency effort, led by the OIG for the Office of the Director for National Intelligence (ODNI), sought to examine watchlist nomination activities throughout the Intelligence Community. Among the other OIGs who participated in this coordinated effort were the OIGs from the Departments of State, Treasury, Energy, and Homeland Security; and the Central Intelligence, Defense Intelligence, National Geospatial-Intelligence, and National Security Agencies. We reviewed the nomination process within DOJ, while these other OIGs reviewed the processes within their respective agencies. The ODNI OIG coordinated this review and compiled the results of the separate reviews.

To accomplish the objectives of our review within DOJ, we interviewed over 100 DOJ employees and officials at both the headquarters and field office levels of various DOJ components.¹ These components included the FBI; Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA); Federal Bureau of Prisons (BOP); U.S. Marshals Service (USMS); DOJ National Security Division (NSD); and United States National Central Bureau (USNCB) – the U.S. liaison with the International Criminal Police Organization (INTERPOL). We also interviewed personnel at the TSC and the National Counterterrorism Center (NCTC), which is a component of the ODNI. In addition to these interviews, we reviewed the policies and processes concerning terrorist watchlisting at the various components and we performed testing of FBI watchlist nomination packages.

We performed our audit in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States, and accordingly, included such tests of the records and procedures that we considered necessary. Our audit covered policies, procedures, and practices in place at the time of our field work, June 27, 2007, through October 23, 2007.

OIG Results in Brief

Overall, our review determined that the FBI is the only DOJ component that formally nominates known or suspected terrorists for inclusion on the consolidated terrorist watchlist. The FBI processed 3,417 standard watchlist nominations in calendar year 2005, 2,568 nominations in 2006, and 2,255 in 2007, as of November 29, 2007. Our review found that FBI personnel understood the FBI's responsibilities regarding the watchlisting process, and the FBI had developed and articulated in policy formal processes for nominating known or suspected terrorists to the watchlist, had instituted sound record management procedures for its standard watchlist nominations, and had provided basic training on the watchlist nomination process to its staff.

We also determined that the FBI established criteria and quality controls to assist in developing proper and accurate watchlist nominations. However, we found that the FBI was not always providing updated nominations when new information became known about a nominated individual. We also found that the FBI was not always removing records from the watchlist when it was appropriate to do so. Moreover, FBI

¹ We visited field offices in Charlotte and Raleigh, North Carolina; Chicago, Illinois; and San Francisco and Dublin, California.

headquarters officials reported that watchlist nomination submissions from field offices were often incomplete or contained inaccuracies, which caused delays in the processing of nominations. We concluded that the FBI should require its Supervisory Special Agents (SSA) to review all nominations submitted by their case agents for accuracy and completeness. These individuals should also be responsible for helping to ensure that case agents create nominations for all individuals who meet the FBI's threshold for nomination. Such action would improve the accuracy and timeliness of watchlist nomination submissions and help prevent the omission of an appropriate nomination.

Additionally, we were informed that FBI field offices had, at times, bypassed FBI headquarters and submitted nominations directly to NCTC. This could result in the watchlisting of individuals without an FBI quality review and could also affect the completeness of the FBI's records that are maintained to support its watchlist nominations.

In addition to its watchlist nomination activities, the FBI prepares terrorist-related intelligence reports that it disseminates throughout the Intelligence Community. Although the FBI did not intend for these reports to be official nominations, NCTC officials informed us that they considered this information from the FBI to constitute official watchlist nominations. As a result, NCTC created watchlist records from these reports and sourced them to the FBI. However, because the FBI was not aware of this NCTC practice, the FBI was not monitoring the records to ensure that they were updated or removed when necessary.

Although the FBI is the only DOJ component that officially nominates individuals for inclusion on the consolidated terrorist watchlist, other DOJ components – such as the ATF, BOP, DEA, USMS, and USNCB – have the potential to obtain terrorist-related information through their day-to-day operations. These DOJ components are required to share terrorism information with the FBI. Our review found that these DOJ components have established processes to share such information with the FBI. However, with the exception of the USNCB and certain sharing processes at the DEA, these DOJ components were generally sharing information in an informal manner, and not all had documented their policies requiring information sharing. In addition, at least one component (ATF) did not categorize criminal activity as being terrorism-related in a manner similar to the FBI, most notably in cases of domestic terrorism. As a result, the potential exists for terrorism information to not be shared with the FBI and for terrorists to not be watchlisted.

In addition to sharing terrorist information with the FBI, the DEA and USNCB were participating in some information sharing initiatives within the Intelligence Community, including with NCTC, that were being interpreted by NCTC as watchlist nomination requests. As a result, NCTC's database included watchlist records that were sourced to the DEA and USNCB. However, neither the DEA nor the USNCB were aware that this was occurring or that watchlist records had been sourced to them. Therefore, the DEA and USNCB were not performing any activities to ensure that the watchlist records were updated or removed when necessary. As a result, these records have the potential to become outdated. Both the DEA and USNCB officials told us when we brought this issue to their attention that they would coordinate with NCTC to ensure proper handling of these records.

Finally, we found that although DOJ components are heavily involved in watchlisting and actively share terrorist information, these activities have been developed independently and are not coordinated by DOJ. We believe that DOJ should consider promulgating policy related to nominations to the consolidated terrorist watchlist and the sharing of information that might result in such a nomination. Although each DOJ component could continue its current initiatives to share information related to known or suspected terrorists and the FBI could continue to make its nominations, such a policy would provide a standardized framework within which all DOJ components would operate. Further, if all Department components operated within a standardized framework, others in the Intelligence Community, such as NCTC, would have a better ability to understand the intent of, and act appropriately upon, the information received from DOJ components.

As a result of our review, we have made seven recommendations to DOJ and to individual components to help improve the watchlist nomination policies, processes, and practices. These recommendations include establishing DOJ-wide watchlisting guidance, enhancing FBI watchlisting policies, and ensuring the correct sourcing of watchlist records that result from information shared by DOJ components.

Our findings are discussed in more detail in the following sections. First, we provide a brief background of DOJ nomination activities, then discuss the FBI's nomination of known or suspected terrorists to the consolidated terrorist watchlist. Our discussion on DOJ terrorist information-sharing practices follows.

Overview of DOJ Watchlist Nomination Activities

Homeland Security Presidential Directive-6 (HSPD-6) mandated the U.S. government to develop the consolidated terrorist watchlist. This

directive requires law enforcement and intelligence agencies with terrorist information in their possession, custody, or control to appropriately share such information for purposes related to the consolidated watchlist of known or suspected terrorists. A subsequent Memorandum of Understanding signed by the Attorney General, the Director of Central Intelligence, and the Secretaries of Homeland Security and State requires information on international terrorists to be shared with NCTC and purely domestic terrorism information to be shared with the FBI.² The procedure for submitting information on individuals for inclusion on the watchlist is referred to as the “nomination process.”

According to the Code of Federal Regulations, the FBI shall “exercise lead agency responsibility in investigating all crimes for which it has primary or concurrent jurisdiction and which involve terrorist activities or acts in preparation of terrorist activities within the statutory jurisdiction of the United States.” The Code of Federal Regulations also states, “if another [non-FBI] federal agency identifies an individual who is engaged in terrorist activities or in acts in preparation of terrorist activities, that agency is requested to promptly notify the FBI.”³ Therefore, DOJ components such as the ATF, BOP, DEA, USMS, and USNCB that have the potential to acquire terrorist information through their operations are required to share with the FBI information related to domestic or international terrorists with a nexus to the United States.⁴

² International Terrorism is defined by the U.S. Criminal Code as activities that (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended (i) to intimidate or coerce a civilian population, (ii) to influence the policy of a government by intimidation or coercion, or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum. The U.S. Criminal Code defines domestic terrorism as activities that (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended (i) to intimidate or coerce a civilian population, (ii) to influence the policy of a government by intimidation or coercion, or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States. 18 U.S.C. 2331 (2007).

³ 28 C.F.R. § 0.85 (2007).

⁴ The U.S. Criminal Code does not differentiate between international and domestic terrorism based solely on the geographic location of an individual. The distinction is made based on the types and origins of the terrorist activities involved. An example of a purely domestic terrorist event is Timothy McVeigh’s bombing of the Oklahoma City Federal Building. The events of September 11, 2001, represent an international terrorist event.

FBI Watchlist Nominations Processes

The FBI is the only DOJ component that officially nominates known or suspected terrorists to the consolidated terrorist watchlist. The FBI has formal processes and policies that document the FBI criteria for watchlist nominations, the methods for effecting nominations, requirements for updating watchlist records when new information is obtained, and removing watchlist records when it is determined that an individual should not be watchlisted. The FBI's watchlisting policies were developed internally and pertain only to the FBI, not to other DOJ components or any external agencies that are involved in watchlisting matters. The FBI uses several different methods to accomplish its nominations depending on the source and type of terrorist information involved.

Nominations of Investigative Subjects

In general, individuals who are subjects of ongoing FBI counterterrorism investigations are nominated to TSC for inclusion on the watchlist, including persons who are being preliminarily investigated to determine if they have links to terrorism. FBI policy requires the responsible case agent to forward a complete nomination package to the Terrorist Review and Examination Unit (TREX) in FBI headquarters. This package should include an initial case opening electronic communication, a copy of a notice of initiation that is directed to DOJ headquarters, and an FBI watchlist nomination form.⁵

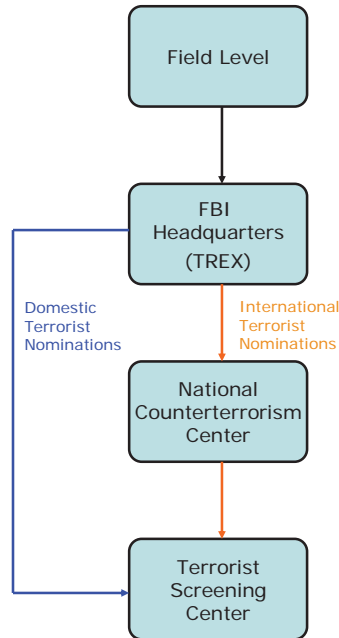
For international terrorist nominations, TREX is responsible for reviewing and approving the nomination. It then forwards the nomination to NCTC. NCTC performs its review of the nomination and submits it to the TSC for inclusion in the consolidated terrorist watchlist. In cases of domestic terrorist nominations, TREX will send the nomination directly to the TSC.

The following graphic provides a basic illustration of the FBI's watchlist nomination process for international and domestic terrorist nominations.

⁵ The FBI nomination form is called an FD-930. We refer to this document throughout the report as the nomination form.

Watchlist Nomination Process

FBI Investigative Subjects



Source: OIG analysis of FBI watchlist process

Quality Control Weaknesses

While the FBI has developed a process and criteria for nominating subjects of terrorism investigations to the consolidated terrorist watchlist, we concluded that the FBI could improve controls for ensuring the quality and timeliness of its watchlist nominations. We found that FBI policy did not require its field offices to perform reviews of the watchlist nomination form generated by case agents. As a result, a majority of the SSAs we interviewed were not reviewing the nomination forms created by their case agents. In addition, TREN officials reported that nomination packages from case agents were often incomplete and analysts were often required to follow-up with the agents to receive sufficient information, thus delaying the processing of nominations. In some instances we found that TREN had not received a nomination package for up to 4 months after the case was opened even though FBI policy requires the case agent to notify TREN within 10 days of the initiation of the investigation.

The Assistant Director of the FBI Counterterrorism Division, TREX management, and Assistant Special Agents in-Charge (ASAC) told us that field office SSAs should be reviewing the nomination forms for content and accuracy. They noted that a quality control review at that level helps ensure that watchlist nomination information is accurate and sufficient before leaving the field office, providing more accurate watchlist information to use in screening for terrorists. Additionally, FBI officials believed this control would help reduce processing delays caused by incorrect watchlist information identified by FBI personnel further along in the nomination process.

Moreover, until recently the FBI did not have procedures to ensure all subjects of terrorism investigations were nominated to the watchlist as required by FBI policy. FBI headquarters recently instituted procedures to review information in the FBI's Automated Case Support (ACS) system to identify any open terrorist cases for which it did not receive a nomination package. In addition to this practice, we believe nomination omissions could be significantly reduced if FBI field offices were required to perform regular reviews to ensure that all terrorism subjects in cases under their control have been nominated in a timely fashion and in accordance with FBI policy.

Failure to Modify and Remove Watchlist Records

According to HSPD-6, each nominating agency involved in the watchlist process is responsible for, on an ongoing basis, providing terrorist information in its possession, custody, or control, thus ensuring watchlist information is current, accurate, and complete. Additionally, nominating agencies should generally provide information to remove an individual from the watchlist when it is determined that no nexus to terrorism exists. During the course of an investigation, the FBI may acquire additional identifying information on watchlisted subjects. FBI policy includes requirements for updating and removing watchlist records of investigative subjects and states that it is "essential" that this additional information be used to enrich an existing record. To accomplish watchlist record revisions, the FBI uses the same process for initially nominating an investigative subject to the terrorist watchlist.

However, several FBI personnel informed us that the modification of watchlist records is not being performed on a regular basis. NCTC personnel also stated that they see very few modification requests from the FBI. Moreover, many of the FBI employees with whom we spoke were not aware of the standards for determining when a modification of the watchlist record is necessary. As a result, certain watchlist records are likely missing useful information.

Additionally, TREX and TSC personnel stated that FBI field offices are not always requesting the removal of watchlisted individuals when closing an investigation. While there are circumstances allowing the FBI to maintain a watchlist record on individuals for whom it has closed an investigation, TREX and TSC officials believed that often individuals inappropriately remained watchlisted because the case agents did not file the paperwork necessary to effect their removal.

Processing Redundancy

The FBI's process for nominating known or suspected terrorists of FBI investigations involves manually entering watchlist information at multiple points in the process. For international terrorist nominations, an FBI case agent first manually enters the information into an electronic FBI watchlist nomination form. Second, FBI personnel at TREX enter the same basic watchlist information into the Violent Gang and Terrorist Organization File (VGTOF) of the National Crime Information Center system.⁶ Third, FBI personnel at NCTC enter watchlist information into the Terrorist Identities Datamart Environment (TIDE), which is then exported electronically to the terrorist screening database maintained by the TSC. Essentially, the FBI is entering the same basic watchlist data three times during this nominations process. Similarly, domestic terrorist nominations are manually entered twice. A case agent first enters the watchlist information on the watchlist nomination form, and then FBI personnel at the TSC enter the same basic information into the consolidated terrorist watchlist database.

FBI officials recognized that these multiple entries may lead to watchlisting errors and informed us that efforts are currently underway to address this issue. We agree that the risk of data-entry error increases with each entry and we recommend that the FBI determine whether its watchlist processes – both its international terrorist and domestic terrorist nominations – could be streamlined to reduce the number of times watchlist information must be manually entered.

⁶ VGTOF contains a relevant subset of the consolidated terrorist watchlist for law enforcement to use in daily screenings of persons of interest. In our September 2007 report on the Terrorist Screening Center we noted that entering international terrorist information into VGTOF before submitting the nomination to NCTC caused inaccuracies and inconsistencies in watchlist records. Department of Justice, Office of the Inspector General, *Follow-up Audit of the Terrorist Screening Center*, Audit Report 07-41, September 2007.

Nomination of Non-Investigative Subjects

In addition to nominating subjects of its terrorist investigations, the FBI has a formal process for nominating to the watchlist known or suspected international terrorists who are not subjects of FBI investigations. FBI policy states that an FBI entity wanting to nominate an individual must provide the FBI Counterterrorism Division a memorandum containing information to support nominating the individual for inclusion on the consolidated terrorist watchlist even though it is not formally investigating the individual. The Counterterrorism Division is then responsible for submitting a request to NCTC to nominate the individual for watchlisting.

However, the FBI policy governing the nomination of known or suspected international terrorists not under FBI investigation does not describe procedures or mechanisms for modifying or removing watchlist records created by this process. Additionally, the FBI policy does not define quality control procedures to help ensure the accuracy and completeness of the information submitted to NCTC for watchlist nominations. While the FBI policy describes the process for nominating non-investigative subjects to the consolidated terrorist watchlist, it does not identify entities or procedures to be used in conducting a review of the information. In contrast, the FBI's policies for nominating its investigative subjects include quality control procedures and mechanisms to help ensure watchlist records are modified and removed as appropriate. We believe the FBI needs to develop quality control procedures and describe mechanisms or procedures to modify or remove watchlist records for non-investigative subject nominations.

In addition, although the FBI has a formal process for nominating non-investigative subjects to the watchlist, when we discussed this process with a Counterterrorism Division section manager responsible for receiving such information and forwarding nomination requests to NCTC, we were informed that the section had not received any such nomination requests. When we discussed this issue with an NCTC official, we learned that NCTC is receiving nominations for non-investigative subjects directly from FBI field personnel. Because this nomination practice is not covered in FBI policy, there are no requirements for FBI personnel to ensure that any resulting watchlist records are updated or removed as appropriate. There is likewise no mechanism to ensure that the nominations directly passed to NCTC by field personnel are appropriate and that the information is complete and accurate.

The weaknesses described above indicate that the potential exists for the watchlist nominations to be inappropriate, inaccurate, or outdated because watchlist records are not appropriately generated, updated or removed as required by FBI policy. Accurate and current identifying

information is critical for identifying suspected terrorists during screening practices, lowering the risk to frontline screening personnel, and reducing misidentifications of innocent individuals who are not suspected terrorists. Moreover, watchlist records on individuals determined to have no nexus to terrorism should be removed from the database to improve the accuracy of the list and to reduce the risk that innocent individuals will be stopped or detained as a result of outdated watchlist records.

FBI Terrorist Watchlist Training

The FBI provides formal training on the watchlist nominations process to various FBI personnel, and it includes instructions on the FBI watchlist protocols on the TREX website on the FBI Intranet. New FBI agents receive comprehensive instruction on the FBI's watchlist process and nomination requirements during the standard New Agent Training course. The FBI also informed us that it was providing further instruction on the consolidated terrorist watchlist during its newly implemented agent refresher course, which is provided to agents who have been employed with the FBI between 6 months and 3 years. Additionally, newly appointed Special Agents in Charge receive a tutorial on the watchlist process before reporting to their new assignment. FBI Legal Attachés receive instruction on the watchlist process during FBI Legal Attaché conferences. Further, field office personnel told us during interviews that the TREX Intranet site is a good reference source for agents to use when completing and submitting a watchlist nomination to TREX. Other FBI personnel noted that agents and task force officers regularly receive on-the-job training from experienced FBI agents, which can include instruction on the FBI's watchlist nomination procedures.

Through its counterterrorism training program, the FBI has also provided instruction on the watchlist nomination process to experienced FBI agents and non-FBI Joint Terrorism Task Force (JTTF) members.⁷ However, several veteran FBI field agents informed us that they still had not received formal training on the watchlist process. Similarly, non-FBI JTTF personnel we interviewed told us that they had not received any formal training on the nomination process even though they may be given lead agent responsibility for or be assigned to a JTTF terrorism case. Also, as previously noted, despite the training some field personnel did not follow FBI watchlist nomination procedures. For example, some FBI personnel failed to modify or remove watchlist records when appropriate, while others bypassed FBI

⁷ The Joint Terrorism Task Forces (JTTF) are FBI-led multi-agency task forces. The JTTFs are located in more than 100 cities in the United States and are made up of FBI Special Agents, state and local law enforcement, and representatives from other government agencies. The JTTFs' responsibilities are to prevent, detect, deter, and investigate attacks perpetrated by domestic and international terrorists in that JTTF's region.

headquarters and submitted nominations directly to NCTC. Therefore, we believe more formalized instruction on the watchlist nomination process is warranted.

Several FBI personnel we interviewed believed that more regular refresher training on the nomination process would be beneficial. FBI management at TREX stated that such training would help reduce the number of errors that TREX personnel find on watchlist nomination forms. Formalized training on the nomination process could also help heighten the awareness that watchlist records must be modified and removed when necessary.

FBI Watchlist Record Retention

To determine if the FBI retained records of its watchlist nominations, including the source of the nomination and the information contained in the nomination, we reviewed FBI policy and documentation maintained by the FBI. We found that the FBI has sound procedures for maintaining records on terrorist watchlist nominations for its investigative subjects. According to FBI officials, TREX retains records of all of its terrorist watchlist nominations in hardcopy and electronic formats. These files should include the watchlist nomination form, approved internal communication from the field office justifying and authorizing the case opening, and the notice of initiation memorandum.

We reviewed a sample of watchlist nomination hardcopy and electronic files, including those in the FBI's Automated Case Support system and confirmed that these documents were included. Additionally, we observed that FBI field office hardcopy case files included some or all of these documents. Therefore, we concluded that the FBI was adequately retaining records of its watchlist nominations for its investigative subjects, including the source of the nomination and the information contained in the nomination.

However, we were told by a TREX supervisor that sometimes TREX processes nominations without all of the required documents. Therefore, watchlist records maintained at TREX for these nominations may not contain all the documents outlined in FBI policy.

In addition, as described above, the FBI's policies and practices for nominating non-investigative subjects to the watchlist are less structured and centralized than those for investigative subjects. Therefore, we are concerned that the FBI's maintenance of documents supporting watchlist

records for non-investigative subjects is decentralized and not being maintained.

DOJ Terrorist Information Sharing

In October 2005, the President issued Executive Order 13388, which requires agencies possessing or acquiring terrorism information to promptly provide access to that information to agencies with counterterrorism functions.⁸ Additionally, in 2003 a Memorandum of Understanding signed by the Attorney General, the Director of Central Intelligence, and the Secretaries of Homeland Security and State required that information on international terrorists be shared with NCTC and purely domestic terrorism information be shared with the FBI. As a result, DOJ components such as the ATF, BOP, DEA, FBI, USMS, and USNCB that have the potential to acquire terrorist information through their operations are required to share such information with other agencies for purposes related to the consolidated terrorist watchlist.

To examine DOJ's involvement in terrorist watchlisting, we interviewed officials at the FBI, DEA, ATF, NSD, USMS, USNCB, and BOP. NCTC and FBI officials informed us that in addition to the FBI's watchlist nomination practices, the FBI also has processes to share terrorist information with appropriate agencies. Officials at each of the other DOJ components reported that they have not been formally involved in any watchlist nominations. However, as described below, each of these components reported that they share terrorist information with other agencies with a counterterrorism mission.⁹ Through the sharing of terrorism information with the FBI, DOJ components also allow the FBI the opportunity to assess potential terrorist threats and to nominate known or suspected terrorists to the U.S. government's consolidated terrorist watchlist.

FBI Terrorist Information Sharing

FBI domestic field offices have intelligence groups that generate Intelligence Information Reports to share terrorism information within the FBI and with agencies in the Intelligence Community, including NCTC. However, NCTC officials told us that NCTC treated these documents as official watchlist nomination requests. Moreover, the resulting records created by NCTC identify the FBI as the source of the nomination. When we

⁸ Executive Order 13388 on Further Strengthening the Sharing of Terrorism Information to Protect Americans. (E.O. 13388).

⁹ Officials from the NSD informed us that the NSD is not involved in the watchlist nomination process.

raised this issue with FBI officials, they stated that they were not aware of this NCTC practice. Because the FBI was not aware that such watchlist records were created, it was not modifying or removing these watchlist records as necessary. Additionally, because the FBI did not consider these reports to be watchlist nominations, they were not reviewing them to ensure that all nomination-related information was complete and accurate. Therefore, we believe that there is a significant potential for records created in this manner to be inaccurate or become outdated.

The FBI has developed procedures to assist the Department of Defense (DOD) in the sharing of information related to military detainees in Afghanistan and Iraq. According to FBI officials, the DOD did not have the capability of incorporating fingerprints for these detainees into a system used in the watchlisting process. Therefore, the FBI's Criminal Justice Information Services Division (CJIS) Intelligence Group processes DOD-obtained fingerprints and then passes the related information on the individual to NCTC.¹⁰ According to CJIS officials, the FBI considers itself a conduit in processing a DOD watchlist nomination and does not consider itself to be the nominating agency for these subjects. However, NCTC officials informed us that when it receives such records, they are sourced to the FBI. If these records have enough information to qualify for watchlisting, NCTC processes the FBI-sourced record as a nomination. Therefore, these records also have the potential to become stale because the FBI – identified as the source agency – is not in a position to, and does not monitor the records to ensure that they are accurate and current. We believe that the FBI, NCTC, and DOD should coordinate their actions to ensure that watchlist records created through this process are sourced to the correct agency.

Other DOJ Information Sharing

As previously noted, the FBI is the lead agency responsible for investigating terrorist activities within the statutory jurisdiction of the United States. Other federal agencies that identify terrorists or terrorist activities are required to promptly notify the FBI. Through the sharing of terrorism information, DOJ components allow the FBI to assess potential terrorist threats and nominate known or suspected terrorists to the U.S. government's consolidated terrorist watchlist.

¹⁰ CJIS serves as the FBI's focal point and central repository for criminal justice information, such as fingerprints and criminal history information, in the FBI.

Drug Enforcement Administration

The DEA is responsible for “the development and implementation of a concentrated program throughout the federal government for the enforcement of Federal drug laws and for cooperation with State and local governments in the enforcement of their drug abuse laws.”¹¹ The DEA notes that, while not having a formal counterterrorism mission, there is often a nexus between drugs and terrorism. For example, in November 2005 the DEA reported in an internal communication that almost half of the 41 foreign terrorist organizations identified by the State Department had ties to some aspect of drug trafficking.

Although the DEA acknowledges a nexus between drugs and terrorism, DEA officials informed us that the agency does not officially nominate individuals for inclusion on the consolidated terrorist watchlist. According to DEA officials, they had not received any guidance directing the DEA to formally nominate to the watchlist all individuals who the DEA had identified as being associated with drug trafficking activities carried out by foreign terrorist organizations on the State Department’s list of foreign terrorist organizations.

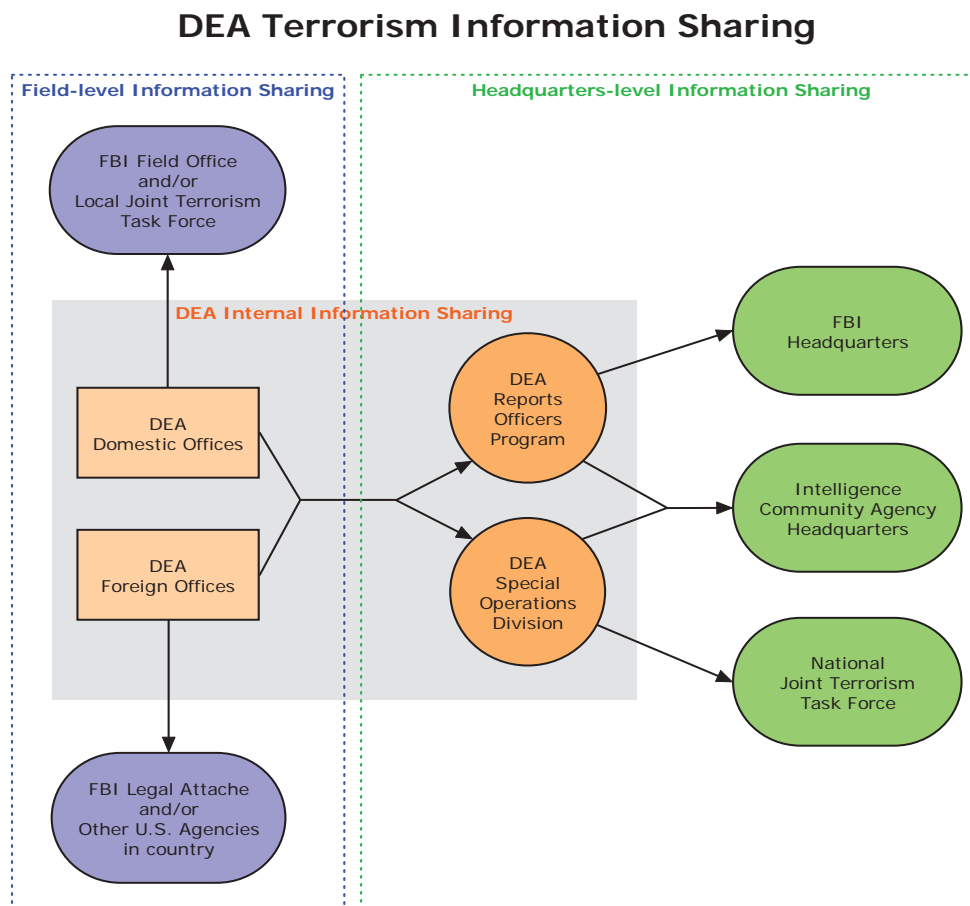
The DEA has developed policies and processes for sharing terrorism information with other agencies. DEA policy requires all terrorism information to be shared with the DEA’s Special Operations Division (SOD), the local JTTF, and the local FBI field office. DEA’s foreign offices are also instructed to immediately pass terrorism information in country to the FBI and other U.S. agencies when appropriate. In addition, the DEA has established a program at its headquarters designed to gather information from DEA activities for sharing with the U.S. Intelligence Community. The DEA Reports Officer Program was designed to review DEA investigative reports and intelligence communications developed by DEA field personnel and to develop summary reports of useful information for dissemination to appropriate Intelligence Community agencies, including the FBI and NCTC.

Our discussions with DEA field office personnel found that the process for sharing terrorism-related information was well understood by DEA domestic field office management. In each DEA field office we visited, DEA personnel informed us that they passed terrorism information to the local FBI office and the JTTF, as well as to the DEA’s SOD. We reviewed documents from the Reports Officer Program that indicated that the DEA was formally sharing terrorism-related information with the Intelligence Community. Although the SOD and Reports Officer Program share

¹¹ 28 C.F.R. § 0.101 (a) & (b) (2007).

information in a formal manner – usually through cables sent to agencies in the Intelligence Community or through the DEA’s participation on the National Joint Terrorism Task Force (NJTTF) – the terrorism information relayed to the local FBI offices and JTTFs is shared in a less formal manner.¹² According to DEA personnel in the field offices we visited, terrorism-related information may be shared through telephone calls or through face-to-face conversations. We were also informed that DEA personnel did not maintain records of information shared in this manner.

The following diagram demonstrates the basic DEA process for reporting and sharing terrorism information.



Source: OIG analysis of the DEA information sharing process

¹² The National Joint Terrorism Task Force (NJTTF) is a multi-agency task force led by the FBI. It includes representatives from ATF, BOP, DEA, USMS and 37 other government agencies and critical industries. The NJTTF coordinates the sharing of terrorism threats and intelligence, coordinates special information and intelligence gathering initiatives, and provides logistical and training support to the JTTFs. NJTTF task force members receive and review information from their agencies and items of interest are shared with other member agencies as appropriate.

DEA-Sourced Watchlist Nominations – DEA headquarters and field personnel stated that the DEA was not involved in the watchlist nomination process. However, despite DEA’s belief that it was not involved in the watchlist nomination process, we found that NCTC is creating watchlist nominations from DEA intelligence documents that contain information on known or suspected terrorists. Further, NCTC is sourcing such nominations to the DEA. As of October 2007, NCTC reported that 40 records in its database were sourced to the DEA. DEA officials were not aware that this was occurring and believed that the agency had no formal role in the watchlist nomination processes. When we discussed this with senior DEA officials, they informed us that they would coordinate with NCTC to ensure that NCTC officials understood that the DEA’s activities were intended as information sharing efforts and not intended as formal nominations to the watchlist.

Moreover, because it did not know that it “owned” watchlist records, the DEA had not been submitting information to modify or remove these watchlist records when necessary. We believe the DEA and NCTC need to coordinate responsibility for modifying and removing the DEA-sourced nominations from the consolidated terrorist watchlist.

Bureau of Alcohol, Tobacco, Firearms and Explosives

The mission of ATF is to “investigate, administer, and enforce the laws related to alcohol, tobacco, firearms, explosives, and arson.” In addition to those specific functions, ATF can perform any other function “related to the investigation of violent crime or domestic terrorism” as may be delegated by the Attorney General.¹³ Though ATF does not have a specifically defined counterterrorism function, its investigations can involve, or lead to, the discovery of terrorist information.

According to ATF officials, they have not submitted any terrorist watchlist nominations. However, ATF officials stated that they share information that they deem to be terrorism-related with the local FBI field office or JTTF. At the field office level we were told that information was shared with the FBI in an informal manner, usually by telephone, e-mail, or face-to-face conversation. In addition, through its participation on the NJTTF, ATF shares information with, and receives information from, the various member agencies. ATF does not maintain documentation of the information that is shared in this manner.

¹³ 28 C.F.R. § 0.130(a) & (d) (2007).

However, ATF officials informed us that they often disagree with the FBI as to what constitutes domestic terrorism. These ATF officials stated that if ATF determines that an act is purely criminal and falls within ATF jurisdiction, ATF will independently investigate the matter regardless of whether the FBI would deem the case to be domestic terrorism. ATF officials suggested that there was a lack of clarity, consistency, and understanding of the definitions of terrorism and terrorist acts among law enforcement agencies.

Therefore, in some circumstances ATF is not sharing potential domestic terrorism information with the FBI. As a result, the possibility exists for individuals with a nexus to terrorism to not be placed on the consolidated terrorist watchlist.

We recommend that ATF and the FBI agree on sharing terrorism information for use in the consolidated terrorist watchlist, to include what activities would result in terrorism information sharing. Further, ATF should ensure that ATF personnel are trained in how to identify such activities.

United States Marshals Service

Two of the primary missions of the USMS are the protection of the federal judiciary and fugitive apprehension.¹⁴ USMS personnel told us that these responsibilities can lead to the discovery of terrorism-related information.

According to USMS officials, when the USMS encounters a credible threat during a threat investigation, USMS policy requires that such information – with or without a nexus to terrorism – be passed to the local FBI office. The USMS follows the same process if it obtains possible terrorism information during a fugitive investigation. Our interviews of USMS headquarters officials and field office staff indicated that the USMS is sharing information with the FBI and the process for sharing such information is understood by USMS personnel. However, although the USMS shares information at the national level through its participation on the NJTTF, similar to our findings at the DEA and ATF, we found that the USMS process for sharing information at the field level has not been formalized.

United States National Central Bureau

Unlike the other DOJ components discussed above, the USNCB is not an investigative law enforcement organization. The mission of the USNCB is

¹⁴ 28 C.F.R § 0.111 (a) & (e) (2007).

to facilitate international law enforcement cooperation as the United States' representative to the International Criminal Police Organization (INTERPOL). The USNCB's major function is to transmit information between the United States and other INTERPOL member countries, including requests for assistance and information involving patterns and trends of criminal activities.

When we initially spoke with officials from the USNCB, they informed us that, although the USNCB currently has several initiatives through which it shares with the U.S. intelligence community potential terrorism information that it obtains, it had no formal role in the watchlist nomination process. However, as with the DEA, officials at NCTC informed us that nominations had been created from information provided by the USNCB and these nominations are being sourced to the USNCB without its knowledge. As a result, these records are not being monitored for modification and removal when necessary. When we informed USNCB officials that since December 2003 about 350 nominations had been created and sourced to the USNCB, USNCB officials responded that it was acceptable for NCTC to create watchlist nominations from information the USNCB provided. These officials also stated that they would follow up on the matter because they did not intend for their actions to be considered formal watchlist nominations originating from USNCB. Rather, they considered their efforts to be information sharing initiatives appropriate to their role as a liaison with INTERPOL. The USNCB officials also stated that their role as a liaison office – as opposed to an investigative law enforcement agency – dictated that their efforts be limited and not include any efforts to investigate the significance or credibility of the information received and disseminated. Accordingly, we recommend that the USNCB coordinate with NCTC to clarify the responsibility for modifying and removing these USNCB-sourced watchlist records.

Federal Bureau of Prisons

Like the USNCB, the BOP is not an investigative law enforcement agency. However, the BOP plays an important role in the collection, analysis, and sharing of terrorism-related information through its monitoring and analysis of inmate communications. In recent years, the BOP has developed several initiatives designed to contribute to the U.S. government's counterterrorism efforts. For example, through its participation on the NJTTF, the BOP has worked with the FBI in the establishment of the

Correctional Intelligence Initiative.¹⁵ In addition, the BOP created a Counter Terrorism Unit, which is responsible for tracking and monitoring the international and domestic terrorists within the BOP system, including analyzing inmate correspondence and financial transactions. Through this monitoring, the BOP Counter Terrorism Unit often obtains information or intelligence about terrorist organizations and activities. According to BOP officials, the BOP shares such information with the FBI through its contact with the NJTTF and with local FBI agents. In addition, an FBI agent has been detailed to the BOP Counter Terrorism Unit to facilitate information sharing.

In our discussions with BOP personnel, we found that they understood BOP processes and procedures for sharing terrorism-related information and that BOP personnel were sharing information with the FBI. However, as with the other DOJ information sharing components, we found that the process by which this information is shared has not been formalized. In addition, we found that the BOP's ability to identify inmates with potential ties to terrorism, particularly in instances of domestic terrorism and cases in which an inmate had been convicted of non-terrorism related charges, had not been fully developed.

DOJ Oversight of Watchlisting and Information Sharing

In general, while DOJ components share terrorist information and provide watchlist information, these activities have been developed independently and are not coordinated by the Department. DOJ's National Security Division (NSD), which was created in March 2006, is now responsible for overseeing the development, coordination, and implementation of Department policy with regard to intelligence, counterintelligence, and national security matters. Further, NSD is responsible for participating in the systematic collection and analysis of information relating to terrorism investigations and formulating legislative initiatives, policies, and guidelines relating to terrorism.¹⁶

We discussed DOJ watchlisting and information sharing activities with NSD officials. These officials stated that NSD has no formal role in the watchlist nomination process. Officials further stated that because NSD is primarily a consumer of information from other DOJ components, such as the FBI, they had not considered whether Department policy on the watchlist

¹⁵ The Correctional Intelligence Initiative is an FBI-led initiative, coordinated through the NJTTF, designed to deter, detect, and disrupt radicalization efforts within federal, state, local, and tribal prison systems in the United States.

¹⁶ 28 C.F.R. 0.72 § (a)(4) & (c)(1) (2007).

nomination process and related information sharing activities was necessary. These officials also noted that NSD does not have the authority to promulgate guidance or policy to other DOJ components without specific direction from the Office of the Deputy Attorney General. Therefore, they said that NSD had not become involved in matters related to terrorist watchlist nominations or related information sharing policies and practices.

In the absence of DOJ oversight and coordination, the FBI has developed policies and processes to nominate individuals to the consolidated terrorist watchlist and other DOJ components have developed processes concerning the sharing of terrorist information. Yet, none of the other components have formalized their information sharing practices and only some of them have documented their policies requiring information sharing. We believe that informal information sharing processes create a greater risk that terrorism information is not shared fully, accurately, and timely and that the information has not been acted upon in an appropriate manner.

We therefore recommend that DOJ consider promulgating general policy related to nominations to the consolidated terrorist watchlist and the sharing of information that might result in such a nomination. Such policy could identify nomination thresholds and information sharing criteria and require the formalization of watchlist nomination and information sharing activities. Although each DOJ component would continue its current initiatives to share information related to known or suspected terrorists and the FBI would continue to make its nominations, such a policy would provide an overall framework within which DOJ components would operate. Further, if all DOJ components operated within a standardized framework, others in the intelligence community, such as NCTC, would have a better ability to understand the intent of, and act appropriately upon, the information provided.

Conclusion

The FBI is the only DOJ component that formally nominates known or suspected terrorists for inclusion on the consolidated terrorist watchlist. We found that the FBI had established a formal watchlist nomination process with quality controls built into the process, FBI personnel understand their agency's role in the watchlist nomination process, the FBI provides formal training and basic instruction on its watchlist nomination process, and the FBI generally has sound record management procedures for its watchlist nominations.

However, we found weaknesses in the FBI's watchlist nomination policies, such as insufficient field office review of nomination packages for

investigative subjects. In addition, there is no requirement to modify and remove, when necessary, watchlist records of non-investigative subjects. Accordingly, we are recommending that the FBI improve its quality control structure by requiring field office review of watchlist nominations to ensure accuracy and timeliness as well as developing policy for modification and removal of watchlist nominations of non-investigative subjects.

Additionally, our review revealed deficiencies in the FBI's practices related to submitting, modifying, and removing watchlist nomination records. For example, we found that FBI field offices bypass FBI headquarters and submit nominations for non-investigative subjects directly to NCTC. This practice does not have sufficient controls to ensure the appropriateness or accuracy of the nomination. We also found significant delays in the processing of watchlist nomination packages. Further, we found that the FBI generally has sound record management procedures for its watchlist nominations, although we identified instances outside the FBI's standard nominations procedures that may cause FBI records to be incomplete.

We intend to continue our review of the FBI's watchlist nomination practices and perform more in-depth analysis of FBI files to further assess the identified quality control weaknesses. For example, we intend to determine if subjects of open FBI cases are appropriately and timely watchlisted and that these records are updated with new identifying information as required. We also plan to examine the extent to which the FBI is watchlisting individuals for which it does not have an open investigation and if subjects of closed FBI investigations are appropriately removed from the watchlist in a timely manner. In addition, we also plan to review watchlist nomination files and determine the extent and effect of nomination package delays and omissions.

In addition to its responsibilities as DOJ's only nominating component, the FBI also engages in intelligence sharing initiatives. However, unbeknownst to the FBI, when NCTC receives FBI reports generated through these initiatives, NCTC treats them as formal nominations. Because these records were sourced to the FBI without the FBI's knowledge, watchlist record modifications and removals were not being processed as required. We also found that the DEA and USNCB engaged in similar information sharing initiatives which resulted in the creation of watchlist records by NCTC. We believe that there is a significant potential for records created in this manner to be inaccurate and become stale. We therefore recommend that the FBI, DEA, and USNCB ensure the correct sourcing of watchlist records involving information shared by their agencies.

Although the FBI is the only DOJ component that officially nominates individuals to the terrorist watchlist, other DOJ components obtain terrorist-related information through their operations. Our review revealed that these components have established processes to share such information with the FBI. However, with the exception of the USNCB and certain processes at the DEA, all of the components were sharing information in an informal manner, and only some components had documented their policies requiring information sharing. In addition, the potential exists for terrorism information to not be shared with the FBI and for individuals to not be watchlisted because at least one component, ATF, did not categorize criminal activity as being terrorism-related in a manner similar to the FBI.

Finally, our review found that these nominating and information sharing initiatives have been developed independently and are not coordinated by DOJ. In the absence of DOJ coordination and oversight, the FBI had developed its own policies and processes to nominate individuals to the consolidated terrorist watchlist, and other components had developed their own processes concerning the sharing of terrorist information. However, with the exception of the USNCB, and certain sharing practices at the DEA, we found that none of the components had formalized their information sharing practices and only certain components had documented their policies regarding information sharing.

We believe that informal information sharing processes create a greater risk that terrorism information is not passed fully, accurately, and timely and that information is not acted upon in an appropriate manner. We therefore recommend that DOJ consider promulgating general policy related to watchlist nomination processes and the sharing of information that might result in a nomination. Such policy could identify nomination thresholds and information sharing criteria, or require formalization of watchlist nomination and information sharing activities. Although each DOJ component would continue its current initiatives to share information related to known or suspected terrorists and the FBI would continue to make its nominations, such a policy would provide an overall framework within which all DOJ components would operate. Further, if DOJ components operated within a standardized framework, others in the Intelligence Community, such as NCTC, would have a better understanding of the intent of, and act appropriately upon, information provided.

Recommendations

We recommend the Department of Justice:

1. Promulgate general policy related to nominations to the consolidated terrorist watchlist and the sharing of information among DOJ components that might result in such a nomination, potentially including identifying nomination thresholds and information sharing criteria, and requiring formalization of watchlist nomination and related information sharing activities.

We recommend the FBI:

2. Modify its written policy to require field office SSAs to review the nomination form for sufficient and accurate information prior to submission of the nomination form to FBI headquarters.
3. Determine whether its watchlist processes for both its international terrorist and domestic terrorist nominations could be streamlined to reduce the number of times watchlist information must be manually entered.
4. Improve the policies concerning non-investigative subjects that the FBI nominates to the consolidated terrorist watchlist, including adding a requirement for the modification and removal of non-investigative subjects from the watchlist.
5. Ensure that all appropriate individuals, including JTTF personnel and veteran FBI agents, receive adequate training related to the FBI's watchlist nominations process.

We recommend the FBI, DEA, and USNCB:

6. Ensure the correct sourcing of watchlist records involving information shared by their agencies and clarify responsibility for keeping these records accurate and up-to-date.

We recommend the FBI and ATF:

7. Reach agreement on sharing terrorism information for use in the consolidated terrorist watchlist, to include what activities would result in terrorism information sharing. Further, ATF should ensure that ATF personnel are trained in how to identify such activities.

DEPARTMENT OF JUSTICE
OFFICE OF THE DEPUTY ATTORNEY GENERAL RESPONSE



U.S. Department of Justice


Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

February 20, 2008

MEMORANDUM FOR THE INSPECTOR GENERAL, OFFICE OF INSPECTOR GENERAL

FROM: Craig Morford 
Acting Deputy Attorney General

SUBJECT: Inspector General's Report re DOJ Consolidated Terrorist Watchlist Nominations
Process

In connection with the above-referenced Report, below is DOJ's response to the Inspector General's recommendation relating to Department-wide policy.

Recommendation 1: We recommend that the Department of Justice promulgate general policy related to nominations to the consolidated terrorist watchlist and the sharing of information among DOJ components that might result in such a nomination

DOJ Response: DOJ agrees with the Inspector General's recommendation with respect to establishing a Department-wide watchlisting policy. We understand that the Director of National Intelligence (DNI) is also considering issuing guidance on watchlisting nominations to the entire Intelligence Community (IC). Accordingly, DOJ will coordinate issuance of Department-wide policy with the DNI's issuance of IC-wide guidance.

FEDERAL BUREAU OF INVESTIGATION RESPONSE

OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

Recommendation #1: Promulgate general policy related to nominations to the consolidated terrorist watchlist and the sharing of information among DOJ components *that might result in such a nomination, potentially including identifying nomination thresholds and information sharing criteria, and requiring formalization of watchlist nomination and related information sharing activities.*

FBI Response: FBI Concur: In collaboration with the Terrorist Screening Center and NCTC, develop uniform standards and protocols for watchlisting.

Recommendation #2: Modify its written policy to require field office SSAs to review the nomination form for sufficient and accurate information prior to submission of the nomination form to FBI headquarters.

FBI Response: FBI Concur: TREX will draft an Electronic Communication (EC) with updated watchlisting policies and will highlight the roles and responsibilities of field office SSAs. The EC will require that SSAs sign off on all FD-930s before the forms are submitted to TREX. The FBI will have the EC finalized in March 2008.

Recommendation #3: Determine whether its watchlist processes for both its international terrorist and domestic terrorist nominations could be streamlined to reduce the number of times watchlist information must be manually entered.

FBI Response: FBI Concur: TREX is currently working with NCTC and TSC to streamline the process. The TSC now enters all DT nominations. For FBI IT nominations, like it is for the rest of the watchlisting community, data will be entered into TIDE by NCTC-TIG for export to the TSDB, where it will in turn be exported to VGTOF and the other support systems. An EC describing the new process and outlining the responsibilities of TREX/TSC will be drafted by April 2008.

Recommendation #4: Improve the policies concerning non-investigative subjects that the FBI nominates to the consolidated terrorist watchlist, including adding a requirement for the modification and removal of non-investigative subjects from the watchlist.

FBI Response: FBI Concur: TREX will work with ITOS I/II, TSC and NCTC to ensure that all non-investigative subjects are nominated, modified, and removed from watchlisting in a consistent manner. An EC will be drafted highlighting the new policy and will be disseminated to all field offices and to Legal Attaché offices in March 2008.

APPENDIX II

Recommendation #5: Ensure that all appropriate individuals, including JTTF personnel and veteran FBI agents, receive adequate training related to the FBI's watchlist nominations process.

FBI Response: FBI Concur: TREX has provided watchlisting training at the annual NJTTF Conference. Further, TREX is currently scheduled to provide training to 18 New Agents Trainee (NAT) classes in FY2008. TREX will also coordinate with NJTTF Unit to develop training curriculum at various regional JTTF conferences. The FBI believes there will be significant progress by May 2008.

Recommendation #6: Ensure the correct sourcing of watchlist records involving information shared by their agencies and clarify responsibility for keeping these records accurate and up-to-date.

FBI Response: This is a joint FBI/DEA/USNCB Action Item.
FBI Concur: TREX will work with NJTTF, DEA, and USNCB points of contact to develop a Memorandum of Understanding that will clearly outline each agency's responsibilities for keeping accurate records. The FBI believes there will be significant progress by April 2008.

Recommendation #7: Reach agreement on sharing terrorism information for use in the consolidated terrorist watchlist, to include what activities would result in terrorism information sharing. Further, ATF should ensure that ATF personnel are trained in how to identify such activities.

FBI Response: This is a joint FBI/ATF Action Item
FBI Concur: TREX will work with NJTTF and ATF points of contact to develop an MOU that will clearly outline how terrorism information for use in the consolidated terrorist watchlist should be used. The FBI believes there will be significant progress by April 2008.

DRUG ENFORCEMENT ADMINISTRATION RESPONSE



U. S. Department of Justice
Drug Enforcement Administration

www.dea.gov

Washington, D.C. 20537

MEMORANDUM

TO: Raymond J. Beaudet
Assistant Inspector General
for Audit
Office of the Inspector General

FROM: Gary W. Oetjen
Deputy Chief Inspector
Office of Inspections
Inspection Division

A handwritten signature in black ink, appearing to read "Gary W. Oetjen", written over the typed name and title.

SUBJECT: DEA's Response to the OIG's Draft Report: *Department of Justice's Consolidated Terrorist Watchlist Nominations Processes, January 2008*

The Drug Enforcement Administration (DEA) has reviewed the Department of Justice (DOJ), Office of the Inspector General's (OIG) draft audit report, entitled: *Department of Justice's Consolidated Terrorist Watchlist Nominations Processes*. DEA appreciates OIG's efforts to conduct a thorough review of DOJ's terrorist watchlist nomination process. As a result of this review, DEA concurs with the one recommendation directed at DEA and will take the necessary steps to implement the recommendation.

Although OIG realizes the Federal Bureau of Investigation (FBI) is the only DOJ component that officially nominates individuals for inclusion onto the consolidated terrorist watchlist, OIG understands that DEA has established policies and processes for sharing terrorism information with the FBI, other agencies and the U.S. Intelligence Community. DEA also appreciates that OIG noted that the process for sharing terrorism-related information was well understood by DEA domestic field office management.

The following is DEA's response to the OIG's recommendation:

Recommendation: Ensure the correct sourcing of watchlist records involving information shared by their agencies and clarify responsibility for keeping these records accurate and up-to-date.

APPENDIX III

Raymond J. Beaudet, Assistant Inspector General for Audit

Page 2

DEA concurs with the recommendation. DEA has been in close coordination with National Counterterrorism Center (NCTC) Deputy Director Russ Travers concerning this issue. Deputy Director Travers understands that DEA intelligence documents that contain information on known suspected terrorists are not intended as nominations by DEA, and that DEA has no formal role in the nomination process. Deputy Director Travers' staff is working on removing references in the system to DEA nominations and clarifying that they are for information sharing purposes only. DEA will remain in contact with Mr. Travers on this issue.

In addition, DEA's Office of National Security Intelligence (NN) is in the final stages of negotiating a memorandum of understanding with NCTC to place an NN staff coordinator in NCTC whose responsibilities will include monitoring these information sharing efforts to ensure that they are not mistaken to be nominations.

Documentation detailing DEA's efforts to implement the attached action plan will be provided to the OIG on a quarterly basis, until such time that all corrective actions have been completed. If you have any questions regarding DEA's response to the OIG's recommendation, please contact Senior Inspector Michael Stanfill at 202-307-8769.

Attachment

cc: Michele M. Leonhart
Deputy Administrator

Richard P. Theis
Director, Audit Liaison Group
Management and Planning Staff

APPENDIX III

ACTION PLAN

Review of Department of Justice's Consolidated Terrorist Watchlist Nominations Processes

Recommendations	Action Planned	Projected Completion Date
<p>Ensure the correct sourcing of watchlist records involving information shared by their agencies and clarify responsibility for keeping these records accurate and up-to-date.</p>	<p>Concur. DEA has been in close coordination with National Counterterrorism Center (NCTC) Deputy Director Russ Travers concerning this issue. Deputy Director Travers understands that DEA intelligence documents that contain information on known suspected terrorists are not intended as nominations by DEA, and that DEA has no formal role in the nomination process. Deputy Director Travers has his staff working on removing references in the system to DEA nominations and clarifying that they are for information sharing purposes only. DEA will remain in contact with Mr. Travers on this issue. In addition, DEA's Office of National Security Intelligence (NN) is in the final stages of negotiating a Memorandum of Understanding with NCTC, to place an NN staff coordinator in NCTC whose responsibilities will include monitoring these information sharing efforts in the future to ensure that they are not mistaken to be nominations.</p>	

APPENDIX IV

U.S. NATIONAL CENTRAL BUREAU of INTERPOL RESPONSE



U.S. Department of Justice

INTERPOL - U.S. National Central Bureau

Washington, D.C. 20530

February 5, 2008

Ms. Carol S. Taraszka
Regional Audit Manager
Chicago Regional Audit Office
Office of the Inspector General
U.S. Department of Justice
500 West Madison Street, Suite 3510A
Chicago, Illinois 60661-2590

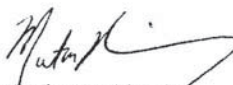
Dear Ms. Taraszka:

Re: Interpol-USNCB Response to Recommendation of the OIG Terrorism Watchlist
Audit

In response to the OIG Audit Report dated January 25, 2008, please be advised that the Interpol-U.S. National Central Bureau (USNCB) concurs with the recommendation of the report relating to the USNCB. In order to implement this recommendation, the USNCB will write to the appropriate officials at the National Counterterrorism Center (NCTC) for the purpose of discussing and agreeing upon a process for ensuring that INTERPOL information provided to the NCTC is accurate and updated as frequently as practicable. The USNCB intends to send the letter to the NCTC within two weeks of the date of this letter, and to establish an updating process with the NCTC within the three months of the date of this letter. We will keep you apprised of the status of these efforts.

Please call me at 202-616-8730 if you have any questions or require any additional information.

Sincerely,


Martin Renkiewicz
Director

BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES RESPONSE



U.S. Department of Justice

Bureau of Alcohol, Tobacco,
Firearms and Explosives

Office of the Director

FEB 20 2008

Washington, DC 20226

MEMORANDUM TO: Assistant Inspector General for Audit

FROM: Acting Director

SUBJECT: Draft Audit Report – The Department of Justice’s Consolidated
Terrorist Watchlist Nominations Process

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) appreciates the opportunity to comment on the Office of the Inspector General’s (OIG) draft audit report entitled “Audit of the Department of Justice’s Consolidated Terrorist Watchlist Nominations Processes.”

ATF has reviewed the OIG draft audit report and fully supports the effort to help improve the watchlist nomination policies, processes, and practices. ATF provides the following formal response to address the OIG’s recommendation to ATF and the Federal Bureau of Investigation (FBI) to reach an agreement on sharing terrorism information for use in the consolidated terrorist watchlist, to include what activities would result in this information sharing. Further, ATF should ensure that ATF personnel are trained in how to identify such activities.

While the OIG report found no specific incidents where ATF failed to properly share terrorism-related information with the FBI, thereby resulting in an omission from the consolidated terrorist watchlist, ATF continues to support the sharing of terrorism information with the FBI and proposes the following measures be taken to eliminate the possibility of an individual with a nexus to terrorism not being placed on the watchlist:

- ATF will meet with the FBI with the intention of reaching a clear and practical method of determining when criminal activity has an identifiable nexus to domestic terrorism.
- ATF will continue to exchange information related to suspected acts of domestic terrorism with the FBI through ATF special agents currently assigned full time to the National Joint Terrorism Task Force and the FBI’s Domestic Terrorism Operations Unit.


APPENDIX V

- 2 -

Assistant Inspector General for Audit

Further, ATF concurs with the OIG recommendation and will take necessary steps to implement the recommendation and ensure that ATF personnel are trained in how to identify such activities.

Should you have any questions regarding this response, please contact Richard E. Chase, Assistant Director, Office of Professional Responsibility and Security Operations, at (202) 648-7500.



Michael J. Sullivan

APPENDIX VI

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

We provided a draft audit report for review and comments to the Office of the Deputy Attorney General (ODAG); the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Drug Enforcement Administration (DEA); the Federal Bureau of Investigation (FBI); the Federal Bureau of Prisons (BOP); the National Security Division (NSD); the U.S. Marshals Service (USMS); and the U.S. National Central Bureau of Interpol (USNCB). Our report did not include any recommendations addressed to the BOP, NSD, or USMS and these components had no comments on our report. The comments that we received from the ODAG, ATF, DEA, FBI and USNCB, which detail the actions taken or plans for implementing our recommendations, have been incorporated in Appendices I through V of this report. Our analysis of these responses and a summary of the actions necessary to close each recommendation are found below.

Recommendation Number:

1. **Resolved.** The Office of the Deputy Attorney General agreed with this recommendation. According to the Office of the Deputy Attorney General, it understands that the Director of National Intelligence (DNI) is considering issuing watchlist nomination guidance to the entire Intelligence Community (IC) and DOJ will coordinate its issuance of Department-wide policy with the DNI's issuance of IC-wide guidance. Although this recommendation was not specifically directed to the FBI, the FBI also offered its comments and stated that, in collaboration with the Terrorist Screening Center (TSC) and National Counterterrorism Center (NCTC), it will develop uniform standards and protocols for watchlisting.

Therefore, this recommendation can be closed when we receive confirmation of the issuance of Department-wide policy addressing nominations and terrorist information sharing related to the consolidated terrorist watchlist.

2. **Resolved.** The FBI concurred with this recommendation and stated that its Terrorist Review and Examination Unit (TREX) will draft an electronic communication (EC) with updated watchlisting policies, including a requirement that a Supervisory Special Agent (SSA) sign off on all FD-930s before the forms are submitted from a field office to TREX. The FBI estimates that this EC will be finalized in March 2008. Therefore, this recommendation can be closed when we receive evidence that the aforementioned EC has been finalized and disseminated to all appropriate field office personnel.

APPENDIX VI

3. **Resolved.** The FBI concurred with this recommendation and stated that TREX is currently working with NCTC and TSC to streamline the process and reduce the number of times watchlist information must be manually entered. It proposes to have nomination data entered into TIDE by the NCTC Terrorist Identities Group. NCTC will then export the information to the TSC where it will be included in the consolidated terrorist watchlist and disseminated to all other appropriate support systems. The FBI expects that an EC describing the new process and outlining the responsibilities of TREX and TSC will be drafted by April 2008. Therefore, this recommendation can be closed when we receive the finalized version of this EC and evidence that the new process has been implemented.
4. **Resolved.** The FBI concurred with this recommendation and stated that TREX will work with other appropriate entities to ensure that all non-investigative subjects nominated to the watchlist are nominated, modified, and removed from the watchlist in a consistent manner. The FBI expects that an EC highlighting the new policy will be drafted and disseminated to all field and Legal Attaché offices in March 2008. Therefore, this recommendation can be closed when we receive the finalized EC.
5. **Resolved.** The FBI concurred with this recommendation and stated that TREX has provided watchlisting training at the annual National Joint Terrorism Task Force (NJTTF) Conference, is currently scheduled to provide training to 18 New Agents Trainee classes in FY 2008, and will coordinate with the NJTTF unit to develop training curriculum at various regional JTTF conferences. Although the FBI's response addresses training for JTTF personnel, it is unclear whether veteran agents not assigned to the JTTFs will receive any watchlisting training. This recommendation can be closed when we receive additional comments addressing watchlisting training that will be provided to veteran FBI agents. In addition, please provide the training curriculum that was developed for the regional JTTF conferences.
6. **Resolved.** The FBI, DEA, and the U.S. National Central Bureau (USNCB) concurred with this recommendation and each component offered additional comments that are addressed below.

The FBI stated that TREX will work with NJTTF, DEA, and USNCB points of contact to develop a Memorandum of Understanding that will clearly outline each agency's responsibilities for keeping accurate records. The FBI believes that significant progress will be made by April 2008.

APPENDIX VI

The DEA stated that it has been in close communication with the NCTC concerning this issue and that appropriate staff at NCTC are working to remove references to DEA nominations and clarifying to NCTC staff that DEA intelligence documents are for information sharing purposes only. In addition, the DEA's Office of National Security Intelligence (NN) is in the final stages of negotiating a Memorandum of Understanding with NCTC to place an NN staff coordinator in NCTC whose responsibilities will include monitoring these information sharing efforts to ensure that they are not mistaken for watchlist nominations.

The USNCB stated that it will coordinate with NCTC to develop a process for ensuring that information provided to NCTC is accurate and updated as frequently as practicable. However, the USNCB does not specifically state that it will address the correct sourcing of watchlist records resulting from USNCB information.

This recommendation can be closed when the FBI provides us with the Memorandum of Understanding signed by DEA, USNCB and the FBI. The FBI should also provide us with comments as to what action it is taking to ensure the correct sourcing of watchlist records that were incorrectly sourced to the FBI. The DEA needs to provide us with evidence that references to DEA nominations have been removed and that DEA and NCTC have agreed that DEA intelligence documents will no longer be considered DEA watchlist nominations. The USNCB needs to provide us with confirmation that officials at USNCB and NCTC have agreed upon a process for ensuring that information provided to NCTC is accurate, updated as frequently as practicable, and correctly sourced.

7. **Resolved.** The FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) concurred with this recommendation and both components offered additional comments that are addressed below.

The FBI concurred with this recommendation and stated that TREX will work with the NJTTF and ATF points of contact to develop a Memorandum of Understanding that will clearly outline how terrorism information for use in the consolidated terrorist watchlist should be used.

The ATF stated that it will take necessary steps to implement the recommendation and ensure that ATF personnel are trained in identifying matters that might relate to the terrorist watchlist. Specifically, ATF stated that it will meet with the FBI with the intention

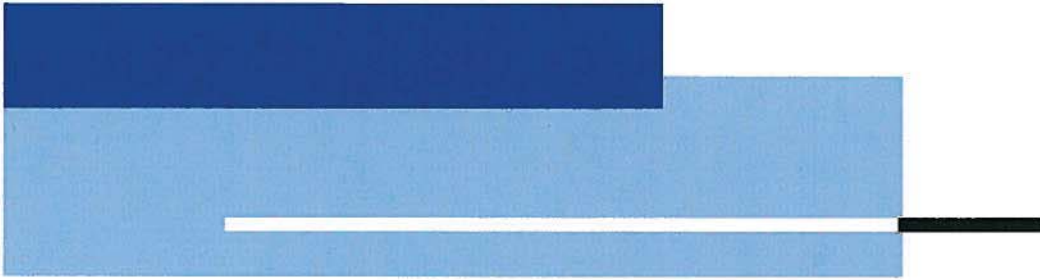
APPENDIX VI

of reaching a clear and practical method of determining when criminal activity has an identifiable nexus to domestic terrorism. In addition, the ATF plans to continue to exchange with the FBI information related to suspected acts of domestic terrorism. This information exchange will be accomplished through ATF Special Agents currently assigned full time to the National Joint Terrorism Task Force and the FBI's Domestic Terrorism Operations Unit.

This recommendation can be closed when we receive evidence that the ATF and FBI have reached an agreement on the sharing of all terrorism information for use in the consolidated watchlist, including what activities would result in terrorism information sharing, and evidence that ATF personnel are trained in how to identify such activities (including both domestic and international terrorism matters).

EXHIBIT 96

REDACTED – FOR PUBLIC RELEASE



THE FEDERAL BUREAU OF INVESTIGATION'S SECURITY CHECK PROCEDURES FOR IMMIGRATION APPLICATIONS AND PETITIONS

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 08-24
June 2008

REDACTED – FOR PUBLIC RELEASE

REDACTED – FOR PUBLIC RELEASE

This page left blank intentionally.

REDACTED – FOR PUBLIC RELEASE

REDACTED – FOR PUBLIC RELEASE

This page left blank intentionally.

REDACTED – FOR PUBLIC RELEASE

REDACTED – FOR PUBLIC RELEASE

**THE FEDERAL BUREAU OF INVESTIGATION’S
SECURITY CHECK PROCEDURES FOR
IMMIGRATION APPLICATIONS AND PETITIONS**

TABLE OF CONTENTS

	Page
INTRODUCTION	1
Name Check.....	2
Fingerprint Identification.....	5
OIG Audit Objectives and Approach.....	7
FINDINGS AND RECOMMENDATIONS	9
I. NAME CHECK TIMELINESS AND QUALITY	9
Name Check Timeliness and Backlog	9
Reasons for Delayed Name Check Processing	14
Conclusion	33
Recommendations.....	34
II. NAME CHECK MONITORING AND PROGRAM IMPROVEMENTS.....	36
Monitoring Workflow.....	36
NNCP Interaction with Customer Agencies.....	43
Cost Recovery	44
Long Term Plans for Improving NNCP Operations	47
Conclusion	50
Recommendations.....	51
III. FINGERPRINT IDENTIFICATION TIMELINESS AND ACCURACY	52
Automating Fingerprint Identification.....	52
Fingerprint Identification Workflow Process	53
Fingerprint Fee Structure	58
Personnel.....	60
Production Monitoring.....	62
Customer Interaction.....	65
Conclusion	66
Recommendations.....	66
STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS.....	67
APPENDIX I - OBJECTIVE, SCOPE, AND METHODOLOGY.....	68

REDACTED – FOR PUBLIC RELEASE

APPENDIX II - ACRONYMS71

APPENDIX III - FBI SECURITY CHECKS REQUIRED FOR
USCIS IMMIGRATION FORMS73

APPENDIX IV - SUMMARY OF NATIONAL NAME CHECK
PROGRAM ASSESSMENTS74

APPENDIX V - DATA REPORT RELIABILITY78

APPENDIX VI - QUALITY ASSURANCE REVIEWS BY
NAME CHECK PHASE79

APPENDIX VII - FBI RESPONSE TO THE DRAFT REPORT81

APPENDIX VIII - OFFICE OF THE INSPECTOR GENERAL ANALYSIS
AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT ..90

REDACTED – FOR PUBLIC RELEASE**INTRODUCTION**

The Federal Bureau of Investigation (FBI) conducts security check and identification services that involve an examination of its vast repositories of investigative records. The FBI offers the following two types of security checks for immigration and naturalization applications: name checks and fingerprint identifications.

TABLE 1: FBI Security Checks

Security Checks	Description
National Name Check Program (NNCP)	Managed by the FBI's Records Management Division, this partially automated security check searches the Universal Index, which references persons, places, and things in an estimated 100 million FBI case files. The files, maintained in the Automated Case Support system, the FBI's Alexandria, Virginia, Records Complex, or one of the FBI's 265 field locations around the world, document people who are the subjects of an FBI investigation (main file) or are associated with the main subject of an investigation (reference file). ¹
Integrated Automated Fingerprint Identification System (IAFIS) ²	Managed by the FBI's Criminal Justice Information Services Division (CJIS), IAFIS is a national fingerprint and criminal history system that provides automated fingerprint search capabilities, latent searching capabilities, electronic image storage, and electronic exchange of fingerprints and responses, 24 hours a day, 365 days a year. According to the FBI, IAFIS maintains the largest biometric database in the world, containing fingerprints and corresponding criminal history information for more than 50 million subjects.

Source: FBI

¹ Prior to fiscal year (FY) 2003, the NNCP searched only main files, which included perpetrators of crimes or those previously investigated by the FBI. In FY 2003, the FBI began searching name check requests against both FBI main and reference files. Reference files contain case file information that is associated with the main subject of an investigation. For example, a reference file may refer to subjects who were interviewed at the scene of a crime or subjects present during an FBI investigation. This FBI effort was designed to detect individuals who may not surface as the direct subject of an investigation during an FBI name check, but who are connected to subjects with criminal and investigative histories.

² IAFIS is composed of several systems: Automated Fingerprint Identification System (AFIS), Interstate Identification Index (III), Electronic Fingerprint Converter (EFCON), Identification Tasking and Networking (ITN), and the IAFIS Data Warehouse (IDWH). Each segment provides discrete capabilities and works in conjunction with the other segments to support FBI service providers. AFIS is a fingerprint comparison system.

REDACTED – FOR PUBLIC RELEASE

The FBI's largest fingerprint identification and name check customer is the U.S. Department of Homeland Security's (DHS) U.S. Citizenship and Immigration Services (USCIS). The USCIS is responsible for administering immigration and naturalization functions, and requests these services as part of its process of deciding whether to grant immigration benefits to applicants and petitioners.³ According to the USCIS, it relies upon information derived from these FBI security checks, along with questions concerning the applicant's background, English language proficiency, and civics testing to adjudicate immigration applications and petitions. However, the USCIS has reported that delays in the FBI's name check process have hindered its ability to adjudicate immigration or naturalization applications in a timely manner.

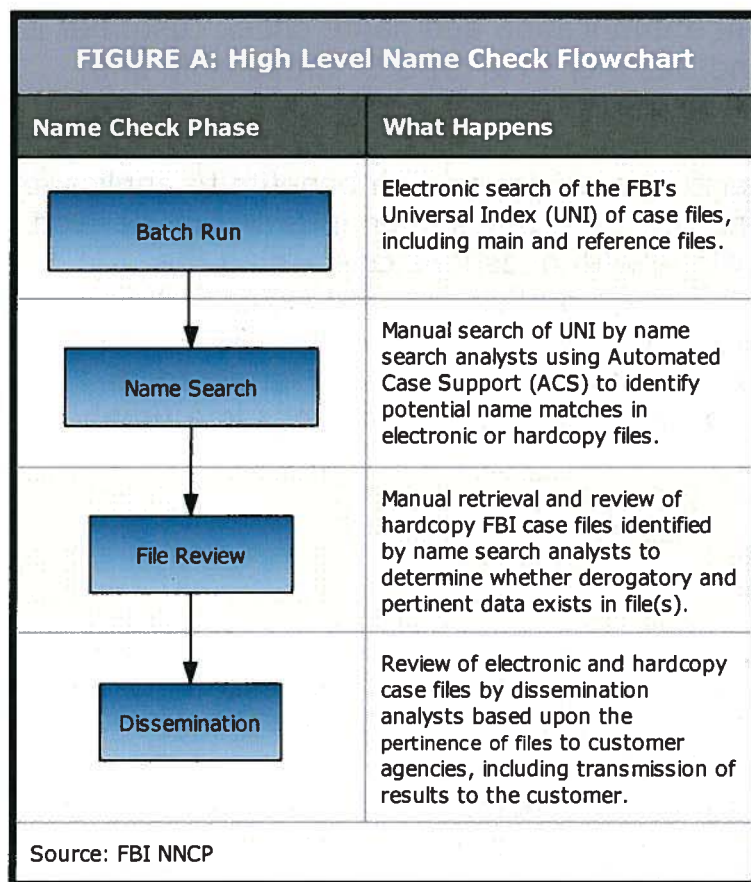
Name Check

The NNCP was established in 1953 to prescreen the names of federal job applicants applying for national security positions. Once located in the FBI's Information Management Section (IMS) of the Criminal Justice Information Services Division (CJIS), the NNCP was transferred to the Records Management Division's (RMD) Records/Information Dissemination Section (RIDS) in the 2001 reorganization of certain FBI headquarters functions. In 2005, the NNCP was integrated into an autonomous RMD section because of the increasing significance of the FBI's name check services.

The NNCP has the authority to disseminate information to authorized agencies when it is relevant to that agency's responsibility and is in the best interests of the U.S. government.⁴ The NNCP disseminates pertinent and derogatory information from FBI case files by means of the four distinct

³ Appendix III describes the USCIS immigration applications and petitions that receive FBI fingerprint identification or name check services.

⁴ 28 U.S.C. § 534 (2006).

REDACTED – FOR PUBLIC RELEASE

phases shown in Figure A.⁵ Each customer agency defines what information from the FBI case files is pertinent and derogatory for the requested name check. What may be considered pertinent and derogatory for one agency may not be pertinent and derogatory for another. According to the FBI, pertinent and derogatory information for USCIS means that the name search subject is a potential threat to national security, public safety, or may be ineligible for an immigration benefit. National security concerns include involvement in terrorist activity, espionage, sabotage, foreign

counterintelligence or the illegal export of technology or sensitive information among other activities. Public safety concerns include information regarding the subject's criminal history or criminal activity. These concerns can also involve information relating to the subject's health, such as a contagious disease, mental disorder, or drug abuse. In addition, an applicant may be ineligible for an immigration benefit due to an array of immigration violations such as presenting a fraudulent document, unlawful entry into the United States, or unlawful residence or employment in the United States.

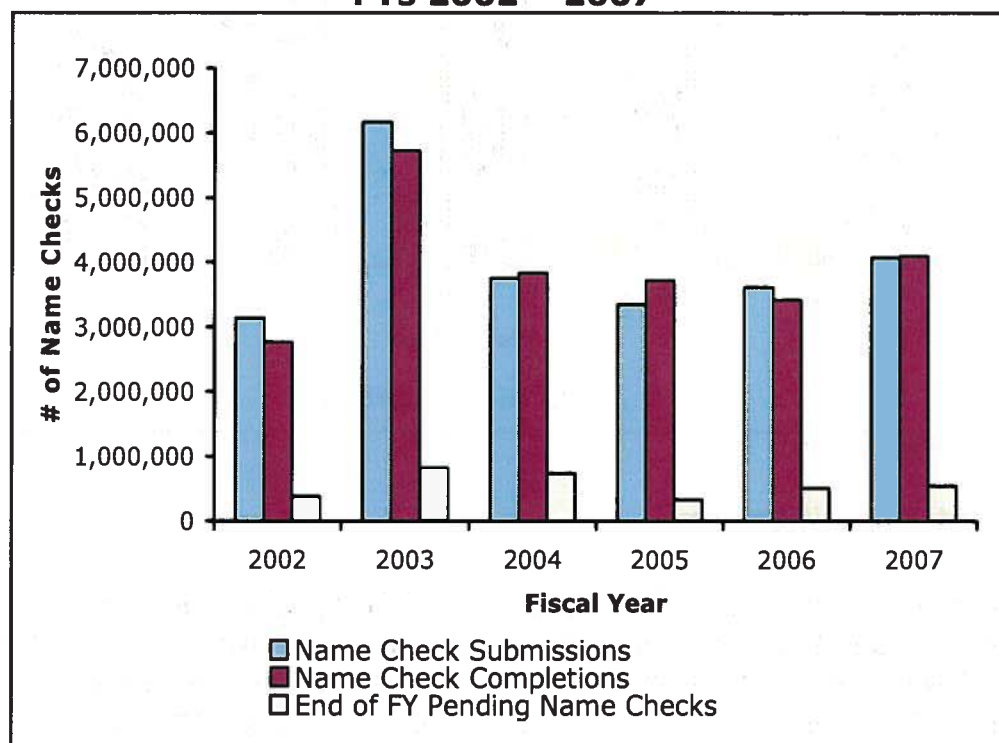
The use of NNCP's services surged following the terrorist attacks of September 11, 2001, with name check requests increasing from 2.7 million name checks in Fiscal Year (FY) 2001 to more than 4 million in FY 2007. Customers such as the DHS, the Department of State (DOS), and the Office of Personnel Management (OPM) routinely seek FBI case file information for

⁵ The NNCP modified the name check process in January 2008 to move name checks from the Name Search phase directly to the Dissemination phase, bypassing the File Review phase. Analysts in performing Dissemination work request file review services as needed. This transition was a significant adjustment to the name check workflow process because it allowed name checks that do not require any hardcopy documentation to progress directly to the Dissemination Phase.

REDACTED – FOR PUBLIC RELEASE

individuals seeking government employment or official appointment, a security clearance, U.S. travel visas, U.S. permanent residency or naturalization, attendance at White House functions, or employment at high-profile events such as a major sporting event. Table 2 depicts the total name check request volume by fiscal year (FY). Of the 4 million name check requests received in FY 2007, 2.2 million were from USCIS.

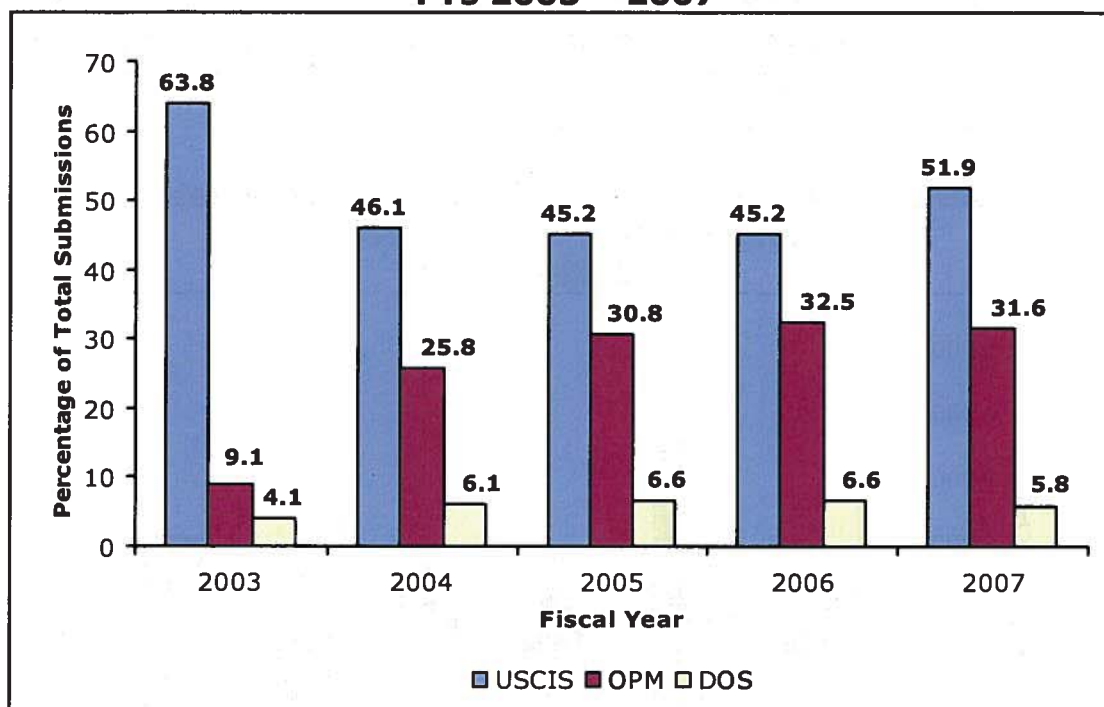
**TABLE 2: Total Volume of Submitted, Completed, and Pending Name Checks
FYs 2002 – 2007⁶**



Source: FBI NNCP

The bulk of NNCP's work is for federal agencies that make adjudications for benefits related to immigration, federal employment, and U.S. travel visas. The NNCP's three largest customers by volume are the (1) USCIS, (2) OPM, and (3) DOS. About 50 percent of all name checks performed by the NNCP originate from the USCIS. Table 3 below depicts the total name check request volume by FY for the USCIS, OPM, and DOS.

⁶ The surge of name check requests in 2003 resulted from the resubmission of 2.7 million name check requests from USCIS for more extensive searches.

REDACTED – FOR PUBLIC RELEASE**TABLE 3: Percentage of Total NNCP Volume
Top 3 Customer Agencies
FYs 2003 – 2007**

Source: FBI NNCP

Fingerprint Identification

The FBI has maintained a repository of fingerprint records since 1924. Prior to July 1999 when the Integrated Automated Fingerprint Identification System (IAFIS) was implemented, the FBI manually compared submitted fingerprints to fingerprint cards on file. Through IAFIS, the process for interpreting and comparing fingerprint data is mostly automated. Therefore, only a small portion of the fingerprint identification process requires human intervention to verify a subject's prints with the FBI repository.

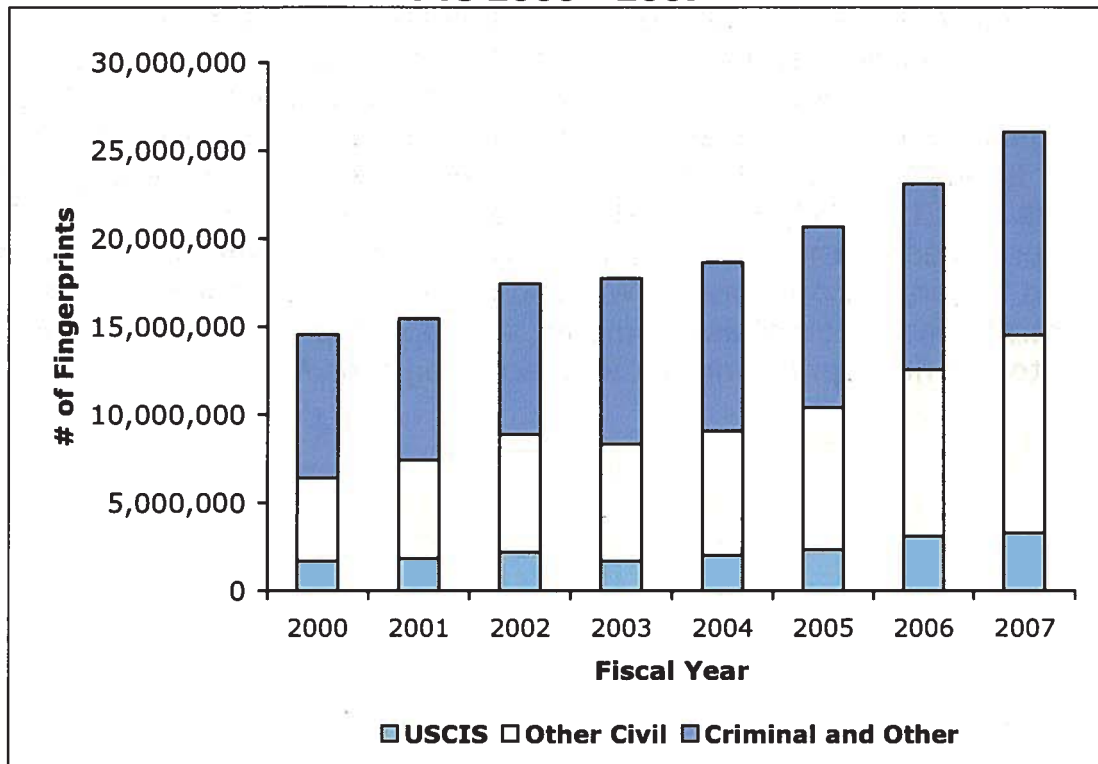
CJIS conducts fingerprint identifications for requesting agencies from a secure facility in Clarksburg, West Virginia. CJIS provides fingerprint identification services for law enforcement purposes (criminal), such as fingerprints taken from an arrestee upon booking into a police station, and non-law enforcement purposes (civil), such as fingerprints requested for employment or licensing purposes, including immigration and naturalization.⁷ On average, CJIS processes about 21 million fingerprint requests annually from approximately 80,000 customers.

⁷ Since FY 2005, 50 percent or more of the fingerprint requests were submitted for civil purposes.

REDACTED – FOR PUBLIC RELEASE

The USCIS is the largest single requestor of the FBI's fingerprint identification services. In FY 2007, USCIS requested over 3.2 million fingerprint identifications. Table 4 displays the total volume of customer agency fingerprint submissions and the annual volume of the USCIS submissions.

**TABLE 4: Total Fingerprint Volume by Submission Type⁸
FYs 2000 - 2007**



Source: FBI CJIS Division

Between 2000 and 2007, the FBI completed more than 153 million fingerprint identifications, including more than 18 million for the USCIS.

⁸ Through FY 2004, "Criminal and other" consisted almost entirely of fingerprints for criminal justice purposes but also included military fingerprints. Since FY 2005, all non-civil fingerprint requests have been for criminal justice purposes.

REDACTED – FOR PUBLIC RELEASE

OIG Audit Objectives and Approach

The Department of Justice Office of the Inspector General (OIG) initiated this audit to assess the timeliness and accuracy of the FBI's name and fingerprint checks that are requested by the USCIS when processing applications and petitions of individuals seeking an immigration benefit. For name and fingerprint checks, we reviewed the FBI's process, response times, fee structure, personnel resources allocated to each program, production monitoring, and communication with customers. We conducted field work and interviewed officials at FBI headquarters; CJIS in Clarksburg, West Virginia; and RMD in Washington, D.C, and Alexandria and Winchester, Virginia. In addition, we interviewed representatives from three large FBI customers (USCIS, OPM, and DOS) to obtain their assessments of the services provided by the FBI and any concerns they had with the FBI name check and fingerprint processes. We also reviewed historical performance data, internal and external assessments, and documentation for planned changes to the fingerprint and name check programs.⁹

⁹ Appendix I describes our scope and methodology as related to the audit objective, while Appendix II contains a list of acronyms.

REDACTED – FOR PUBLIC RELEASE

This page left blank intentionally.

REDACTED – FOR PUBLIC RELEASE

REDACTED – FOR PUBLIC RELEASE

FINDINGS AND RECOMMENDATIONS

I. NAME CHECK TIMELINESS AND QUALITY

The FBI received over 4 million name check requests in FY 2007 from federal agencies, the law enforcement community, and authorized non-criminal justice agencies. While we found that the FBI processed about 86 percent of name check requests within 60 days, name checks for the remaining 14 percent can take anywhere from several months to over a year. In addition, as of March 2008 the FBI had over 327,000 pending USCIS name check requests, with 90 percent over 30 days old and more than 110,000 requests (30 percent) pending for over 1 year.

Our audit found that the NNCP's methods for conducting name checks rely on outdated and ineffective technology, staff and contractors who have limited supervision and training, inadequate quality control measures, and inconsistent use of production goals for name check analysts. As a result, the NNCP's name check backlog causes delays in the DHS's efforts to assess potential national security threats residing in the United States and adjudicate applicants' requests for immigration benefits. In addition, NNCP's processes do not provide adequate assurance that necessary information is being retrieved and transmitted to customer agencies.

Name Check Timeliness and Backlog

Federal law requires the USCIS to grant or deny naturalization benefits to an applicant at the time of the initial examination or within 120-days after the date of the examination.¹⁰ If USCIS does not grant or deny the benefit within 120 days of the date of examination, an applicant may apply to the U.S. district court in the district in which the applicant resides for a hearing on the matter.

¹⁰ 8 C.F.R. § 335.3 (1993).

REDACTED – FOR PUBLIC RELEASE

The NNCP recently established production goals to complete USCIS name checks. The NNCP's goal is to process 98 percent of USCIS's name check requests within 30 days. As depicted in Table 5, as of March 2008 the NNCP reported that over 327,000 USCIS-requested name checks remain in its working queue, with over 300,000 (90 percent) over 30 days old and more than 111,000 (30 percent) over 1 year old.

**TABLE 5: Pending USCIS Name Check Submissions
(as of March 2008)¹¹**

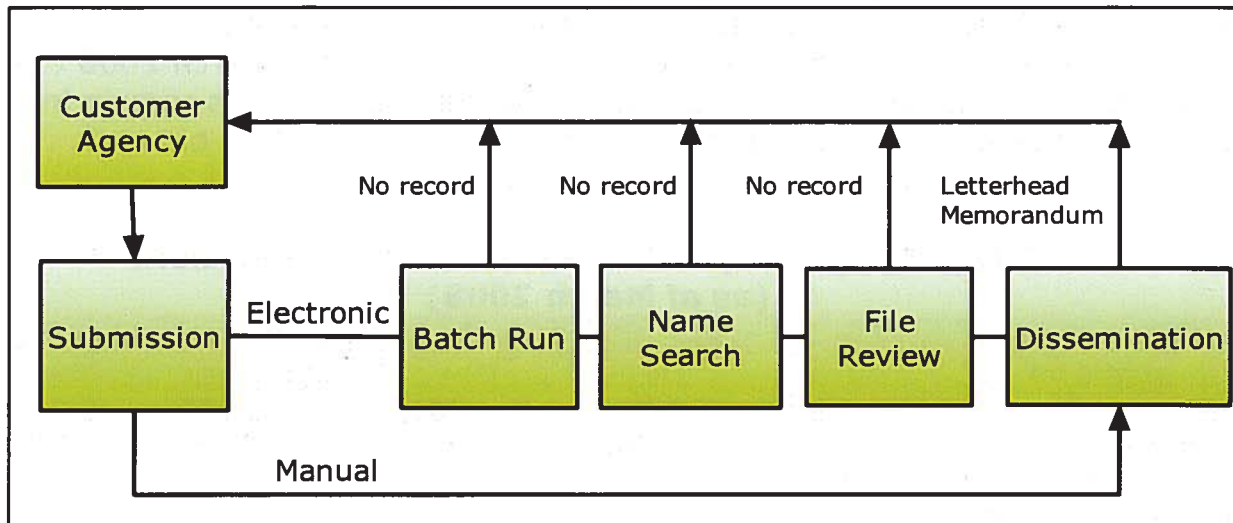
USCIS Submissions	0 – 30 Days	31 – 60 Days	61 – 120 Days	121 Days – One Year	> One Year
Asylum	2,199	1,286	861	2,150	5,613
Catch-All	703	797	1,090	3,705	7,390
Executive Office for Immigration Review	1,281	739	858	1,481	2,631
Naturalization	9,323	7,027	23,898	36,629	50,794
Adjustment of Status	11,232	7,303	8,182	95,342	45,260
Total	24,738	17,152	34,889	139,307	111,688

Source: FBI NNCP

The NNCP process, as illustrated in Figure B, involves four distinct phases: (1) an electronic Batch Run search of the FBI's Universal Index (UNI), (2) a customized Name Search of UNI, (3) a File Review which entails the collection and manual review of pertinent hardcopy records in FBI case files, and (4) Dissemination of pertinent and derogatory information via a letterhead memorandum (LHM) to the requesting customer agency.¹²

¹¹ The volume of pending USCIS name check submissions fluctuates. In October 2006, the USCIS pending volume totaled nearly 365,000 name checks. The USCIS volume exceeded 402,000 submissions as of September 2007, before dropping to the March 2008 volume of over 327,000 submissions.

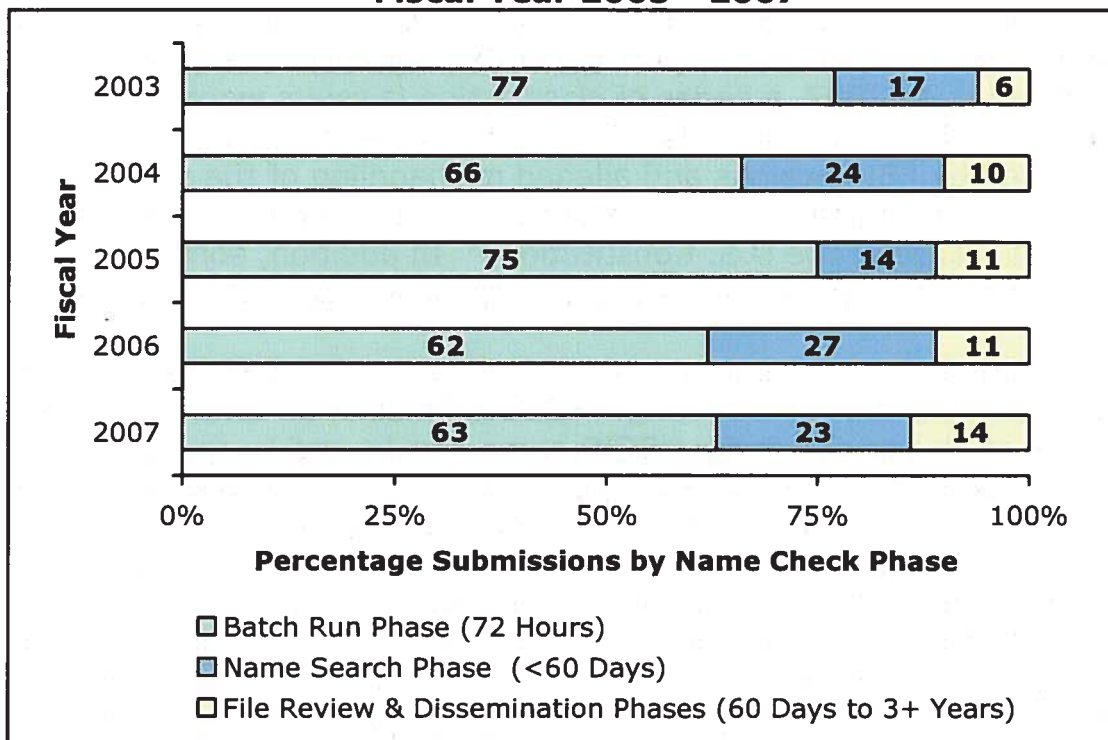
¹² Dissemination packages may communicate pertinent or derogatory information via a LHM, investigative report, or a third-party referral. The LHM is a term used by the FBI to describe a name check analyst's summary of the FBI's case file data.

REDACTED – FOR PUBLIC RELEASE**FIGURE B: NNCP Name Search Flow Process¹³**

Source: FBI NNCP

The automated Batch Run process electronically eliminates subject names that do not have a match in UNI. The processes following the Batch Run entail a greater degree of manual work, including requesting and scanning documentation, reviewing files, and obtaining permission from third-party agencies to disseminate derogatory information to the customer. As shown in Table 6 below, the percentage of name checks taking longer than 60 days to process has gradually increased since FY 2003. For example, in FY 2003 only 6 percent of all name checks took longer than 60 days to process; in FY 2007, approximately 14 percent of name check requests took longer than 60 days.

¹³ As noted in the Introduction, the NNCP modified the name check process in January 2008 to move name checks from the Name Search phase directly to the Dissemination phase, bypassing the File Review phase.

REDACTED – FOR PUBLIC RELEASE**TABLE 6: Percentage of Name Checks Received by Phase
Fiscal Year 2003 - 2007**

Source: FBI NNCP

A letterhead memorandum (LHM) is part of a dissemination package issued to a customer when the name check subject's case file contains pertinent and derogatory information. In FY 2007, the FBI issued 1,413 LHMs to USCIS. This means that for less than 1 percent of all USCIS name check submissions in that year, pertinent and derogatory information was found in FBI systems and transmitted to the USCIS.¹⁴

Effects of Delayed Name Checks

Delays in name checks affect immigration and naturalization applicants who seek to adjust their status and become citizens of the United States. Security check delays and backlogs can impact these individuals and can also have far-reaching implications for homeland security, commerce, and education. Delays in the naturalization process slow applicants' access to U.S. citizenship benefits. Delayed security checks may also slow the adjudication and deportation of national security threats residing in the United States, hinder the entry of foreign workers for domestic business operations, and impede academic study-abroad programs.

¹⁴ Due to delays in name check processing, some of the 1,413 LHMs could be related to submissions from previous years.

REDACTED – FOR PUBLIC RELEASE

The delays in security checks have generated lawsuits against the USCIS and the FBI. The FBI Office of the General Counsel reports that since 2005 more than 6,000 writs of mandamus have been filed by applicants and petitioners in federal courts compelling USCIS to grant or deny benefits without delay.¹⁵ In 2007, a series of class action lawsuits were initiated on behalf of naturalization applicants. The petitions claim that adjudication delays caused by FBI backlogs and alleged mishandling of the security check process violate the Administrative Procedure Act and the Fifth Amendment Due Process Clause of the U.S. Constitution.¹⁶ In addition, some judges have threatened to use their authority to adjudicate applications or petitions.

To address the delays, in September 2007 the FBI and USCIS entered into an agreement to filter out certain FBI case files in an effort to decrease the volume of files reviewed for USCIS name checks and to speed up the name check process. The filtering mechanism has two components. The first filter, termed Mega Filter, eliminates three file categories from the name check process for all pending and future USCIS name checks. The second filter, termed Super Filter, identifies or flags thousands of FBI files that the USCIS and NNCP agreed to eliminate from USCIS name searches. The flags indicate that name check analysts should disregard such files. However, according to name check supervisors and analysts we interviewed, these files may contain pertinent criminal history information or reference other files with information that the USCIS would consider pertinent and derogatory.

Furthermore, in response to the delays in the FBI name check process and in an effort to reduce the backlog of immigration applications, the USCIS decided in February 2008 to begin approving otherwise completed U.S. permanent residency (green card) applications that were at least 180 days old even if the FBI had not completed its name check review. If derogatory information on the green card recipient is later revealed by the FBI's name check process subsequent to granting a green card, the USCIS said it will

¹⁵ The mandamus writ commands the performance of a particular act or directing the restoration of the complainant to rights or privileges of which he has been illegally deprived. *Nebel v. Nebel*, 241 N.C. 491 85 S.E.2d 876, 882. The U.S. District Courts have original jurisdiction of any action in the nature of mandamus to compel an officer or employee of the United States or any agency thereof to perform a duty owed to a plaintiff. 28 U.S.C. § 1361 (1962).

¹⁶ The class action suits include *Bavi v. Mukasey* (2007), *Zhang v. Gonzales* (2007), and *Roshandel v. Chertoff* (2007), among several others. The Administrative Procedure Act, 5 U.S.C. § 555 (2007), in part requires administrative agencies to conclude matters presented to them "within a reasonable time." The Fifth Amendment Due Process Clause, U.S. Constitution, prohibits the government from depriving life, liberty, or property without due process of law.

REDACTED – FOR PUBLIC RELEASE

seek to deport the recipient. The USCIS stated that the change will not apply to naturalization applicants due to the difficulty in revoking citizenship as compared to the process for rescinding permanent residency.

Reasons for Delayed Name Check Processing

In the wake of the terrorist attacks on September 11, 2001, the FBI, in cooperation with the USCIS, altered its name check method, searching both main and reference investigative file data. As a result, the USCIS resubmitted 2.7 million name check requests in FY 2003. The NNCP stated that this resubmission of USCIS name check requests to obtain reference file data associated with the name check subjects initially created the backlog. In addition, the NNCP stated that the manual processes of locating and retrieving paper files worldwide coupled with inadequate funds to improve the program has contributed to the backlog.

A February 2002 Business Process and Staffing Study of name check operations, produced by Advanced Computing Technologies for the FBI, observed that the NNCP experienced processing delays during the study period of September 2000 and July 2001, and that the September 11 terrorist attacks had significantly increased the NNCP's workload.¹⁷ The study concluded that the number of NNCP staff on board was not sufficient to handle the name check information needed in the aftermath of the terrorist attacks.

The FBI acknowledged NNCP's current processes are inefficient and do not reflect a state-of-the-art system. In addition to the FY 2002 study, the FBI conducted assessments of the NNCP in FYs 2007 and 2008.¹⁸ Each assessment found the need to further automate the name check process. However, instead of implementing new search mechanisms and automated processes, the NNCP supplemented its antiquated processes by significantly increasing the number of personnel performing manual name check functions. In addition, the most significant technological enhancements we noted in the past several years include a user friendly interface to scanned documentation and efforts to implement a text recognition tool. One RMD official described the current approach as applying "small band-aids" to the legacy name check process in an attempt to meet the increased name check demand.

¹⁷ This study was commissioned by CJIS prior to the transfer of name check operations to RMD.

¹⁸ See Appendix IV for additional assessment and study details including scope and pertinent recommendations.

REDACTED – FOR PUBLIC RELEASE

In March and April 2008, the NNCP finalized customer-level operations plans with USCIS and OPM, respectively. The USCIS plan describes how the NNCP segmented the USCIS name check backlog into timeframes and instructed analysts to begin focusing on the oldest pending name checks first. According to the NNCP, the segmentation of work queues reduced the backlog of name checks older than 4 years from 12,000 to 3,000 between the inception of this initiative in November 2007 and March 2008. The NNCP and USCIS hope to have addressed all name checks pending more than 2 years by July 2008 and those pending more than 1 year by November 2008. The plan also outlines how the NNCP will meet their June 2009 goal of processing 98 percent of USCIS's name check requests within 30 days. Likewise, the OPM operations plan discusses eliminating all OPM name checks pending for over 40 days by April 2009. Both plans rely on using the NNCP's current processes and state that the FBI is issuing a statement of work designed to obtain the services of a contractor to reengineer the name check process with contemporary technology and business practices.

FBI officials said their long-term goal is to implement a largely automated name check process; however, we confirmed that NNCP's current automated processes, such as its name matching tools, have had few if any modifications or upgrades since their inception. Further, the current NNCP method for completing name checks is dependent upon a growing number of FBI and contract employees who are under-supervised and have limited training.

Integrating Technology into the Name Check Process

Technology and automation are critical for increasing name check process efficiency. However, we identified several weaknesses with how the FBI is integrating technology into the name check process.

FBI Name Matching Tools are Outdated and Incomplete

Despite the trio of assessments of the NNCP, the FBI did not conduct a technical assessment of perhaps the most important factor affecting the NNCP's ability to timely and accurately perform name checks: its phonetic name matching tools. Our review of the FBI search tools revealed that the FBI relies heavily on an outdated modified Soundex algorithm to return potentially close phonetic matches.¹⁹ The NNCP Batch Run phase uses two methods to search and find name matches, an Around the Clock Three Way search and a phonetic search developed by the FBI in the mid-1990s. The

¹⁹ Soundex is an English-based phonetic algorithm that was developed in 1918. The U.S. Census Bureau began using Soundex in the 1930s as a means for searching family names in genealogical research.

REDACTED – FOR PUBLIC RELEASE

Around the Clock Three Way search is actually two search techniques: an Around the Clock and a Three Way Search.

[REDACTED]

[REDACTED]

Source: FBI Information Technology Operations Division (ITOD)

[REDACTED]

[REDACTED]

REDACTED – FOR PUBLIC RELEASE

Deficiencies with Soundex Tools. One of the primary problems with using a Soundex phonetic algorithm for name checks stems from its initial development. Soundex algorithms are not culturally based search tools and do not attempt to adjust for the cultural permutations, transliteration issues, and culturally specific naming characteristics involved in modern name matching. Developed using English or Anglo names that are easily broken into name parts (i.e., first, middle, last), there are no transliteration issues. Although there may be multiple ways to spell Smith (Smyth or Smithe), the pronunciation and consonants do not change. Soundex algorithms used with other languages such as Arabic, which have not only different sounds and pronunciations but different cultural naming norms, may produce high levels of false positives and negatives.²⁰



Source: OIG

²⁰ A false positive occurs when the search tool indicates that a name check submission matches a name in UNI when in fact it does not match the name. A false negative occurs when the search tool indicates that a name check submission does not match a name in UNI when in fact the submission is a match.

REDACTED – FOR PUBLIC RELEASE



Similarly, Soundex algorithms are incapable of placing varied value on different name parts. When used to search against English names, this is not necessarily a significant deficiency. However, since approximately half of the NNCP workload comes from the USCIS, and many of the name check requests include names not generally associated with English-language origins, this can become a significant problem. The Western concept of naming parts and order – given, middle, and surname – is not applicable in many other cultures. Many Eastern cultures order their names with the family or surname first. For example, in China the family name often is written first, followed by the given name. In addition, 100 surnames account for 85 percent of the population in China. Therefore, by weighing a surname match the same as a given and surname match, the system would produce a high number of false positives. In addition, many Arabic names may include several names not easily broken into given, middle, and surname. Therefore, using a Soundex system that puts the same weight of a Western ordered surname match as a given name match may return a high level of false positives.

As noted below in Table 9, the top 10 places of birth for name check subjects submitted by USCIS are countries where English is not the native language.

REDACTED – FOR PUBLIC RELEASE

REDACTED – FOR PUBLIC RELEASE**TABLE 9: Top 10 Places of Birth of USCIS Name Check Subjects
FYs 2001-2007**

Name Check Subject Place of Birth (POB)	Checks Submitted to Batch Run
Mexico	1,472,666
India	596,299
Country Unknown	549,941
China	507,733
Philippines	421,340
Cuba	326,247
El Salvador	247,887
Colombia	233,564
Dominican Republic	229,785
Haiti	186,625
Total for Top 10 Places of Birth	4,772,087
Total for All Places of Birth	9,568,287

Source: FBI ITOD

While a majority of these countries use a Western order for naming, naming practices among these countries vary dramatically. For example, many of the most common places of birth are countries where Spanish is the primary language. In Spanish-speaking cultures, it is common for children to have multiple surnames: that of the father and mother. In this case, a Soundex algorithm is unable to put more value on a potential match of both surnames rather than a single surname. Depending on how the information is entered into the system, often incorrectly using Western naming norms, a high level of false positives or false negatives may occur.

The difficulties discussed with name matching, and specifically with Soundex, become even more significant when comparing the most common places of birth for all incoming and pending name checks. We noted that as of October 1, 2007, the places of birth most represented among pending USCIS name checks (at any stage of the name check process) relative to their share of all USCIS name checks since 2001 were Libya, Iraq, India, Saudi Arabia, China, Kuwait, United Arab Emirates, Yemen, South Korea, and Palestine. When compared to the most common places of birth for USCIS incoming name check submissions, it is apparent where the system has problems identifying potential matches. This data underscores the importance of improving upon the FBI's phonetic algorithm, especially with respect to countries where the primary spoken language is not written using a Latin alphabet and the countries do not traditionally use western naming norms.

REDACTED – FOR PUBLIC RELEASE

Quality Assurance. Our audit found that the FBI has not performed any quality assurance on its name matching search tools. In the 11 years since UNI was created, we found that only one comparison to another name searching tool had been completed. We reviewed the comparison completed in 2005 by the FBI's Information Technology Operations Division (ITOD) and determined that the FBI compared the systems based solely on system capabilities, not on accuracy or other performance metrics.²¹ While the FBI has reviewed other phonetic search tools for use in operational case management, no additional reviews or comparisons have been performed related to NNCP.

Further, we reviewed two Soundex studies. Both studies, performed in the 1990s, tested a Soundex algorithm on British names. In one study, researchers found a Soundex algorithm failed to match 60 percent of true match pairs.²² In the second study, the Soundex algorithm failed to identify 25 percent of actual matches and of the matches identified, 66 percent were incorrect.²³ Even without taking into account the transliteration, segmentation, dialect, and acoustic errors prevalent in foreign-language name searching, the results produced by these Soundex algorithms could not be viewed as complete and accurate.

In light of these findings, we spoke with officials at the Terrorist Screening Center (TSC) and DOS, organizations that rely on identity matching to help perform their duties. We found that at both the TSC and the DOS, phonetic algorithms were tested and updated to address specific cultural and linguistic variances. Both agencies used native foreign language speakers, metrics, and real data test sets to determine how to adjust their search engine results. This has not occurred at the FBI. In fact, we were told by ITOD officials that the UNI matching searches, including the phonetic tool, have not been updated since their creation in the mid 1990s.

²¹ The review determined whether the software provided six criterion, none of which reviewed the software for accuracy and not all of which are current FBI capabilities: (1) would search results include name variations; (2) is the search capable of supplying a phonetic search component; (3) does the search provide foreign name translation into English; (4) does the search rank results based on accuracy; (5) is it capable of searching names regardless of the order of name parts entered; (6) are searches for organization names processed identically to searches for individuals.

²² Lait, A.J and Randell, B. "An Assessment of Name Matching Algorithms," *University of Newcastle upon Tyne*, (1996) <http://homepages.cs.ncl.ac.uk/brian.randell/Genealogy/NameMatching.pdf> (accessed October 31, 2007).

²³ Stainer, Alan. "How Accurate is Soundex Matching?", *Computers in Genealogy*, March 1990: 286-288.

REDACTED – FOR PUBLIC RELEASE

In March 2007, at the request of Associate Deputy Director of FBI and with the sponsorship of Assistant Director of RMD, a review of the need for improvement in the automation of the NNCP was undertaken. An individual from the FBI's Special Technologies and Applications Office (STAO) reviewed the name check process and provided the results to RMD. The June 2007 internal FBI communication expressed concern regarding the accuracy of the Soundex-based name matching tool. The communication referenced one of the previously mentioned studies and concluded that:

The UNI system should be replaced by one which applies culture specific matching criterion, automatic application of linguistic rules based on culture/language context, be noise tolerant [typographical errors], recognize equivalent but dissimilar name variants, include statistical and probabilistic search aids, and support syntactic flexibility.

Given that no testing has been performed on the FBI's Soundex phonetic algorithm to determine its effectiveness, accuracy, and reliability, especially when matched against foreign names, we cannot determine if the FBI's modified phonetic Soundex tool accurately returns potential name matches. Based on the above-mentioned studies of other Soundex algorithms, we believe there is a high risk that the FBI's Soundex algorithm does not accurately return potential name matches. Consequently, we recommend that the FBI implement procedures to periodically test and update its name matching phonetic search tools at the same time it seeks to develop a new name check system.

Other Organizations Incorporating Name Search Automation. In the fall of 2007, the TSC began testing a combination of phonetic-based systems designed to address many of the transliteration and cultural permutation issues facing the identity matching community. The TSC approach contains three phonetic search tools, including one designed to match Arabic names. Once subject information is entered into the system, the subject is queried using all three tools. Each tool individually ranks the potential matches according to how close they match the input data. The potential matches are combined into one output that provides the user with a weighted ranking of potential matches that can be used to prioritize adjudications. In addition, each tool is tuned to only return results that meet a certain pre-determined threshold. This threshold can be tuned and updated depending on the agency's needs. For example, the agency may decide that results ranked below 75 percent are not accurate enough to warrant review. Therefore, the threshold may be set to not return matches below 75 percent.

REDACTED – FOR PUBLIC RELEASE

TSC officials and their contractors explained to us that the goal of this system was not to return all possible results, but only to return those most likely to be matches. In its initial testing of the system using a pre-determined set of data, the TSC was able to tune the system to produce results with the fewest false positives and false negatives, leaving the reviewer with less data to search. By searching a subject using three different tools instead of one, the TSC increases the likelihood that all potential matches will be captured.

After testing their system, TSC officials told us that it provides three times more effective search capability than its previous system for identifying potential true identity matches. Testing of the new system found that potential matches increased from 19 to 59. TSC analysts are currently using the mix of search engines to identify potential matches in the TSC Database. To build the most flexibility into its search system, the TSC designed the system to be a plug-in system, allowing the TSC to update, add, and change the search engine tools as necessary.

Since the mid-1990s, the DOS has developed several cultural and linguistic based algorithms to perform name searches. Like the TSC, DOS officials noted that their algorithms are constantly being updated and refined based on field-user experience and requests. The algorithms used by DOS are tested against a known real database before being implemented, allowing DOS to set parameters for returned results. DOS tested and updated its algorithms after the September 11 attacks using data from an Arabic phonebook to ensure the effectiveness of its Arabic name search tool.

When compared to other identity matching search tools on the market that address the cultural and linguistic issues noted above, the FBI's Soundex-based search tools are technologically outdated. The FBI's current tools can neither address the cultural and linguistic issues previously noted, nor be tuned to provide a ranking of results. This results in a heavy reliance on the individual analyst to identify cultural permutations or variations in order to obtain all potential matches. In addition, by not providing name search analysts with a ranked result of potential matches, name search analysts may be sorting through an unnecessary amount of false positives.

We believe that the FBI's reliance on its custom Soundex algorithm to find phonetic name matches, without any quality assurance testing, places the FBI at a high risk of not producing accurate search results. We recommend the FBI explore other available phonetic search tools to work in conjunction with or as a replacement to its current Soundex-based algorithm.

REDACTED – FOR PUBLIC RELEASE

Federal Identity Matching Working Group. The TSC helped charter a Federal Identity Matching Working Group in 2006 comprised of 14 agencies within the intelligence community to “establish a voluntary guideline for Federal agencies using identity matching search engine technology” and to “provide agencies with a guideline for establishing a performance metric indicating how effective the searching is being carried out.” Members of this working group, which include the Central Intelligence Agency (CIA) and the U.S. Department of Defense (DOD), are testing their own search tools to determine their capabilities in comparison to the rest of the federal identity matching community.

The FBI is represented on the working group by officials from its Counterterrorism Division (CTD), but there is no NNCP representation on the working group. We believe it is important that NNCP interact with other agencies in the federal identity matching community in order to stay current on the trends and developing technologies. As a section within the FBI using identity matching search technology and providing this service to other federal agencies, we recommend the NNCP participate fully in the work of the federal identity matching community.

Integrating the Name Check Process into Sentinel

In addition to upgrading its name matching tools, the FBI also needs to ensure that its development of a new case management system and search tools serve the needs of the NNCP. In December 2006, an OIG audit report noted that the implementation of the FBI’s new investigative case management system, Sentinel, will require changes to the FBI’s name check system and estimated the cost of updating the existing name check system to work with Sentinel would exceed \$10 million.²⁴ We reviewed a communication between the NNCP and the FBI’s Information and Technology Branch (ITB) that confirms Sentinel may provide multiple capabilities that benefit the NNCP. However, several NNCP functions will not be covered by Sentinel. Until the Sentinel project advances to the phase when the NNCP will be addressed, the ITB has directed the NNCP to move forward with an action plan for a new name check system that the ITB will review to separate requirements for a new NCP application and those met by other IT assets.

²⁴ U.S. Department of Justice Office of the Inspector General, *Sentinel Audit II: Status of the Federal Bureau of Investigation’s Case Management System*, Audit Report 07-03 (December 2006), 19.

REDACTED – FOR PUBLIC RELEASE

The ITB stated that it is developing a joint search engine to access data stored electronically throughout the FBI's repositories, including the UNI case file information searched by the NNCP. This new effort utilizes the FBI's Information Portal (IP), an enterprise class platform currently under development that may be capable of integration into Sentinel. As a major component of the FBI's information technology (IT) modernization project, Sentinel will replace the FBI's legacy Automated Case Support (ACS) system. The NNCP currently uses ACS to report all pertinent and derogatory information known to the FBI about a search subject. In addition, the Name Check Program (NCP) mainframe application is utilized by name check analysts to acquire name check subjects, search FBI databases, and close completed name checks residing in ACS.²⁵ The FBI anticipates piloting the IP in early FY 2009 with the objective of bringing a new federated search capability to the FBI. If this new technology meets expectations, the FBI believes that it may serve as a foundation for a new name search tool.

The NNCP's Business Operations Support Unit (BOSU) is concurrently reviewing the NNCP's needs for developing new technology for a "Next Generation NNCP." BOSU officials told us that while they are in contact with the ITB and are following the ITB's life-cycle management directives for developing new technology, they stated that the process of incorporating new technology is "painfully slow" and that they are not yet ready to discuss specifics with Sentinel program representatives. We discussed the impact of Sentinel with name check managers, but they could not explain how Sentinel will impact and improve the name check process. Therefore, we recommend that the FBI ITB and NNCP engage in close and continuing interaction to ensure that the interim and long-term technology efforts modernize the FBI's name matching capability.

Name Check Technological Enhancements

Due to the backlog of unprocessed name checks, the NNCP has been exploring automated solutions to speed up the ability of analysts to review and process name check requests. In FY 2004, the NNCP implemented a stand-alone database known as the Name Check Dissemination Database (NCDD) to manage all documentation compiled during the name check process so analysts do not have to recreate a name check if the name is resubmitted, and provide access to scanned FBI files that analysts identified as relating to a name check subject. These are functions that the NCP mainframe application cannot perform. In addition, the NNCP is exploring

²⁵ The FBI NCP mainframe application is the official application of record for the NNCP, and a component of the FBI's Automated Case Support (ACS) system. All incoming and closeout name checks must be processed through NCP for an official count.

REDACTED – FOR PUBLIC RELEASE

the use of Content Analyst software to assist in searching and sorting case file text. As discussed below, although the NNCP recognizes the need to automate name check processes these IT enhancements have not improved the NNCP's efficiency.

Name Check Dissemination Database (NCDD). FBI officials have promoted the NCDD as a critical tool for tracking the name check process. However, the NCDD is an autonomous application that does not automatically synchronize with the NCP mainframe application. In order to update work queues in NCDD for each analyst, an NCP mainframe data file must be loaded into the NCDD daily. However, the data synchronization is unidirectional; that is, any work conducted within the NCDD, such as a closeout on a completed and disseminated name check, is not fed back into the NCP automatically.²⁶ Because the NCDD is not a fully integrated application in the work flow, many analysts told us that the NCDD creates a duplicative work step in the name check process.

In addition, although the FBI issued an NCDD User Guide in November 2006, the guide does not include instructions regarding the use of NCDD for how documents should be recorded, retained, and tracked. Many analysts circumvent the NCDD's electronic inventory functions and establish their own method for tracking pending workload and retaining hardcopy files of all outgoing communications, including the LHMs sent to customer agencies and the Electronic Communications (EC)s and e-mails sent to FBI field divisions. The inconsistent use of NCDD raises the risk of procedural steps being missed, documentation being lost, and pending checks being delayed.

We also found access and inoperability issues between the NCDD and T Drive, which is the central repository for RMD's scanned documentation. Twenty-four percent of analysts we interviewed indicated that they often experience complications in locating scanned files on the T Drive, while 44 percent of analysts either did not have access to files stored on the T Drive at the time of our interview or were unsure whether they had access. We spoke with RMD personnel in both NNCP and Document Conversion Laboratory (DocLab), as well as FBI programmers responsible for NCDD.²⁷ They indicated that complications with the T Drive are caused by errors in

²⁶ The analyst must manually log back into the NCP application and close out the name check in the NCP. A name check that is completed through NCDD will remain open until the analyst marks the closeout in the NCP application.

²⁷ To provide analysts with electronic versions of files, and to facilitate the name check process, RMD provides document scanning services through the Document Conversion Laboratory (DocLab). Once documents are scanned, the files are uploaded to the T Drive.

REDACTED – FOR PUBLIC RELEASE

NCDD's mapping of the T Drive directory structure and improper training. Because it is preferred that analysts access the T Drive through the NCDD, such interoperability and training issues significantly impede an analyst's ability to access necessary FBI files, review the files for pertinent and derogatory information, and disseminate the information in a timely manner to the customer agency. We were told by NNCP that an NNCP technical team is attempting to resolve the T Drive NCDD mapping issue.

The FBI needs to track and maintain all documentation in a uniform and centralized manner so that it is easily accessible. In addition, prompt and reliable access to scanned case file data through the NCDD is a key element in the timely completion of name checks. We recommend the FBI develop instructions and additional training for analysts regarding the use of NCDD, and that the NNCP immediately resolve the directory mapping issues between the T Drive and the NCDD.

Content Analyst. In order to complete a name check, NNCP first identifies what case files may have information relative to the name check subject. Then an analyst reviews each case file for any pertinent and derogatory information. Each case file may contain numerous documents and require the analyst to review significant amounts of data. In order to improve productivity, the NNCP sought to purchase and evaluate the Content Analyst software package in December 2006 to provide analysts with the capability to search for specific text in documentation related to the search subject.²⁸ We interviewed NNCP management, analysts, and personnel from BOSU to determine how Content Analyst would be integrated into the name check process. Several personnel, including NNCP management officials, could not specify how Content Analyst would be used or the software's specific functions. One NNCP official indicated that the NNCP is not certain of the capabilities Content Analyst can provide. A planned demonstration of Content Analyst in October 2007 did not occur due to FBI technology limitations.²⁹ FBI managers also stated that the effort "stalled" while attention was focused on other initiatives.

²⁸ The developmental and testing cost of Content Analyst totals \$277,625. Two Content Analyst textual analysis software packages were purchased in May 2007 for a total cost of \$186,000. Consultation and configuration services associated with the set-up, installation, and testing of Content Analyst were purchased between March and August 2007 for \$91,625.

²⁹ The FBI encountered administrative challenges acquiring information technology servers to operate Content Analyst. A January 2008 vendor dispute inhibited the FBI from procuring new servers and the server loaned by ITOD did not maintain the required operating system to conduct a software proof-of-concept. As of March 2008, BOSU had yet to receive a Content Analyst demonstration to determine what benefits the software may provide the name check process.

REDACTED – FOR PUBLIC RELEASE

The NNCP characterized the purchase of the software as an effort to educate itself about the product. However, it took the FBI over a year, from the time it initiated the procurement, to test the software and learn that it is not compatible with its current applications. In addition, BOSU personnel stated that the Content Analyst software requires that the documentation it analyzes have recognizable text. We confirmed the text requirement by reviewing supporting documentation from the Content Analyst developer. However, prior to October 2007 files scanned to the T Drive were only available as images in Tagged Image File Formatting (TIFF), which is incapable of allowing analysts to electronically search the file text.³⁰ An NNCP manager stated that the software package was provided to the ITB for evaluation to determine if it will be compatible with a new, more efficient name check workflow process.

Continued Dependence on Human Resources

As of March 2008, the NNCP had 371 employees and contractors working on name checks.³¹ Since November 2007, the NNCP experienced almost a 30-percent increase in staffing. NNCP managers told us they needed additional personnel to: (1) eliminate the current backlog of USCIS name checks, (2) continue production on increasing numbers of name checks from all customers, and (3) work on completing all name checks within 30 to 60 days.³² The NNCP projects that 195 FBI personnel and 402 contractors will be employed by the end of FY 2008, an increase of more than 300 personnel since November 2007.

Although NNCP management is focused on reducing the backlog through increased production, NNCP officials told us that quality remains the program's primary objective throughout all phases of the process. With the large influx of new personnel, we are concerned that a high potential for

³⁰ To provide NNCP with searchable text data, DocLab began using optical character recognition (OCR) to produce a text file with each document image. In addition to producing OCR-enabled files, DocLab is also working to backscan document images already on the T Drive to make corresponding text files available for search. The FBI's collection of scanned documentation consists of 8 to 10 million files. The FBI estimates that it will complete OCR scanning on image files in May 2008, if all resources are exclusively directed to the project. The FBI hopes to increase the speed of the scanning by adding new scanning technology.

³¹ The RMD also utilizes 38 employees from Information Technology Centers (ITC) in Butte, Montana, and Savannah, Georgia, to assist in name search and dissemination activities.

³² Of the total personnel, 38 FBI employees and 189 contractors are dedicated to USCIS submissions.

REDACTED – FOR PUBLIC RELEASE

error exists by analysts and supervisors due to limited training, supervision, quality control measures, and recently implemented production measures.

At our audit closeout meetings, FBI managers stated that short-term training, supervision, and quality assurance issues were experienced due to the NNCP's rapid expansion. NNCP officials stated that new employees and contractors receive classroom, on-the-job, and supplemental training to correct common performance problems. We were also informed that a new organizational structure is in the final stages of approval, and that structure will reduce the span of control to acceptable supervisor-to-staff ratios and feature a Training and Quality Assurance unit.

Training

Personnel who conduct name checks must be properly trained in the technology used by the NNCP, the judgment process used to determine HITs or IDENTs, and procedures for disseminating information.³³ In early FY 2008, the NNCP updated its Name Search and Dissemination training program for new employees.³⁴ However, our review of the training for name check analysts indicates that classroom instructors are not provided specific training objectives or goals by NNCP management. This results in instructors not following a set training program with standardized requirements. In addition, we found that employees were provided different training manuals based on their training date, and we could not obtain a uniform set of training materials or communications from analysts serving in the same position.

Although classroom training for new name check analysts included examples of name searches and activities, there is little explanation given to assist employees in weighing identifiers for determining the difference between a HIT or IDENT.³⁵ Furthermore, the training does not provide any instruction on cultural or name linguistics, a topic that would be beneficial to analysts searching for names in FBI case files. We note that the DOS provides its analysts with extensive name searching training and provides its employees with cultural and linguistic information to aid them in performing their searching and reviewing activities.

³³ Names that have potential information are marked "HIT," while subjects that match the names and other identifying data such as date of birth and social security number are marked as "IDENT."

³⁴ The File Review Phase training program consists of on-the-job training.

³⁵ Identifiers used to match name check submissions to FBI files include date of birth, locality, social security number, and name spelling. During our audit, we noted that name check analysts weighed identifiers differently during their case file analysis.

REDACTED – FOR PUBLIC RELEASE

Moreover, new NNCP employees we interviewed did not have individual access to any NNCP systems during their classroom training. These systems, including NCP and NCDD, are essential tools used to complete name checks. While instructors used hardcopy examples to walk students through the exercises, students have very limited instruction on NCP and NCDD during their classroom instruction. Instructors called students up one at a time to perform name searches on the single computer in the room logged into NCP. Of the 18 contractors we interviewed in Winchester, many noted that the availability of access to NNCP systems, or even a mock system for use during training, would provide hands-on skill development and would have been beneficial.

In addition, no annual or recurring job-related training is required for name check analysts. The importance of recurring training opportunities is highlighted by the NNCP's implementation of the Super Filter. As previously discussed, FBI management entered into an agreement with the USCIS to identify or flag case files that the FBI and USCIS deemed not pertinent for USCIS adjudicative purposes. However, we found that several analysts involved in the name check process were unaware of the initiative. Though FBI officials state that e-mail correspondence detailed the filtering initiative, some analysts stated that they "wasted time" reviewing several case files that were flagged because they were not told by management to disregard such files. Other name check analysts and supervisors stated that they were confused by the initiative and continued to search the identified files due to the presence of pertinent and derogatory information within the file.³⁶ Moreover, personnel performing dissemination functions explained that they were not provided clear instructions by management about what data the USCIS considers pertinent and derogatory. Analysts added that they considered it appropriate to continue reviewing the flagged files to ensure that high-quality name checks were being performed. With proper training and follow-up from management to ensure effective implementation, name check analysts could have better understood why the filter was in place, and not wasted time reviewing and providing non-pertinent information to the USCIS.

³⁶ Files flagged by the USCIS because they do not contain pertinent and derogatory information for USCIS adjudication purposes may still contain pertinent or derogatory criminal history information as determined by the FBI. As previously noted, each name check customer agency determines what case file information is pertinent for its internal purposes.

REDACTED – FOR PUBLIC RELEASE

Without comprehensive training opportunities, the FBI cannot expect its analysts to complete name checks in an accurate and timely manner. In light of the training deficiencies, we recommend that the NNCP develop a formal training curriculum and recurring instruction to ensure that each name check analyst is provided with a consistent skill set. Recurring training offers the ability to refresh name check analyst skills, enforce uniform name check procedures, and communicate name check policies that affect production. In addition, we believe that failing to provide students access to the systems during training inhibits new hires from learning the systems necessary for name search production as highlighted in the discussion on the NCDD. Thus, we recommend the FBI explore providing system access opportunities to new hires during name search and dissemination training.

Supervision

When the NNCP hired a large influx of new personnel in FYs 2007 and 2008, it did not proportionally increase the number of supervisors to manage these new employees and review analysts' work. We found that while the NNCP's March 2008 business plan establishes an FBI reviewer to contractor ratio of about 15 to 1, we could not verify the actual ratio due to a lack of human resource information from NNCP. According to the NNCP, the time required to train an analyst to full production level is about 4 months. Therefore, the new analysts and contractors require experienced FBI staff to train, evaluate, guide, and provide technical supervision and approvals.

During our audit, name check personnel and their supervisors were divided between facilities in Winchester, Virginia, and Washington, D.C. Supervisors not located at the Winchester facility made weekly site visits to review contractor work, attend meetings, and fulfill other responsibilities on-site. We were told by the personnel reporting to supervisors not located at the Winchester facility that it was difficult to complete name checks without immediate review and feedback from a permanent on-site supervisor. Although analysts were instructed to ask their supervisors for assistance, some analysts expressed hesitation to do so due to their supervisor's limited time on-site. Analysts said they were concerned that these supervisors were not readily available to answer questions or provide feedback and instruction.

REDACTED – FOR PUBLIC RELEASE

NNCP supervisors told us that they are overwhelmed by the number of name checks they must review. One FBI supervisor at Winchester told us that although new hires had gone through training, she found errors in a vast majority of the work she reviewed. Another supervisor told us that she only had time to correct mistakes, not go back and show the analyst what was wrong.

In an effort to reduce the amount of review supervisors need to perform, NNCP management has asked non-supervisory FBI staff to assist in the review of name checks completed by contractors. While this procedure assists with oversight of contractors' work, it limits the ability of on-site FBI employees to perform their regular name check functions. In addition, we found that several FBI employees with less than 1 year of experience had been designated as the primary lead for questions from contractors and we are concerned that employees with limited name check experience are advising and in some cases reviewing the work of new employees.

We discussed these issues with RMD officials who said they were aware of the situation. RMD officials stated that they are seeking to reduce the number of questions to FBI supervisory analysts so supervisors can focus primarily on name check review and production. To do so, the NNCP is asking that new contractors refer their inquiries to more experienced contractors or a designated non-supervisory FBI analyst. RMD officials stated that they will continue to require that all name checks disseminated to customer agencies with pertinent and derogatory data be reviewed by FBI supervisors. In the long run, RMD officials say they plan to transition NNCP personnel in Washington to the Interim Central Records Complex (ICRC) in Winchester prior to the eventual relocation of all name check personnel to the Central Records Complex (CRC) by the end of March 2011. To mitigate short-term concerns regarding the NNCP's ability to supervise the influx of new employees, we recommend that the NNCP review its supervisor-to-staff ratio and develop a plan for immediately increasing the permanent supervisory presence at the Winchester facility.

REDACTED – FOR PUBLIC RELEASE

Quality Assurance Program

We also reviewed the quality assurance steps taken for the Name Search, File Review, and Dissemination phases of the name check process.³⁷ We found that the NNCP has not provided formal guidance or procedures to supervisors to govern quality assurance for any step of the name check process. In addition, NNCP management does not maintain a quality assurance committee or otherwise oversee the quality assurance process. Although operational supervisors perform quality assurance reviews of work performed by new analysts, no consistent or regular quality review occurs once an employee exhibits proficient work.³⁸

In our judgment, limited quality assurance reviews, coupled with the previously noted technological, training, and supervisory concerns increase the risk of errors in the name check process. RMD management conducts reviews of all LHMs sent to customer agencies, but also emphasized that given the volume of name checks, it would be impossible to perform quality assurance reviews on 100 percent of all other name check work. Nevertheless, we recommend that the NNCP develop and implement quality assurance measures and guidance for all steps of the name check process.

Name Check Production Measurement Challenges

NNCP managers stated that they recognize the value of establishing measures to accomplish goals and ensure organizational effectiveness. For several years, the NNCP has imposed production metrics in the Name Search and File Review phases of the name check process, phases with less analytical activity and more production oriented outcomes. However, contractors were the only personnel performing name checks who were held to production metrics in FY 2007. According to the NNCP, each contractor is required to process 140 name checks per month. In February 2008, NNCP managers began implementing name check production metrics for FBI analysts based on the complexity of the name check assignments and the grade level of the analysts.

³⁷ As discussed in the "Integrating Technology into the Name Check Process" section of this report, the FBI has not performed significant or regular quality assurance on its name matching search tools. According to FBI ITOD officials, no testing has been performed on the FBI's Soundex phonetic algorithm to determine its effectiveness, accuracy, and reliability, especially when matched against foreign names. As a result, we could not determine if the FBI's modified phonetic Soundex tool accurately returns potential name matches.

³⁸ See Appendix VI for a discussion of the quality assurance reviews implemented by each name check phase.

REDACTED – FOR PUBLIC RELEASE

An NNCP manager stated that they were cautious to implement production metrics due to the unique nature of each name submission and the variables that impact name check production.³⁹ For example, according to NNCP managers the primary impediment to establishing production metrics is the uncertainty of how long it generally takes to complete a name check. Although NNCP officials estimate that three to four USCIS name submissions can be completed per day by a single analyst, this projection could not be confirmed because the NNCP does not track the specific work performance of FBI or contract personnel.⁴⁰

Despite the NNCP's recent efforts to implement production measurements, we question the accuracy and reliability of the recently enacted metrics. The primary objective of the NNCP metrics is to identify the total number of name checks closed, completed, and disseminated by analysts. Without reliable data inputs, including the total number of name checks received and completed, management cannot properly assess, interpret, and manage results, and the FBI runs the risk of not hiring enough personnel to meet the demands of increasing customer submissions.⁴¹ Therefore, we recommend that the NNCP develop and implement a reliable name check submission and completion tracking function so that it can monitor its name check production activities. We also recommend that the NNCP develop plans for reevaluating production metrics on a periodic basis to appropriately evaluate staff production efforts.

Conclusion

Despite the increased demand for its services, the NNCP's methods for providing name check information rely on outdated and inefficient technology, and depend heavily on manual efforts to process name check submissions. We identified deficiencies with the technology utilized by the NNCP, as well as its plans for integrating new technology into the name check process. Among these deficiencies, we noted that the NNCP continues to rely upon an outdated phonetic name matching algorithm that can result

³⁹ Variables that may impact name check production include the location of the submission within the processing queue, the workload of analysts, the volume of expedite submissions, the number of potential matches associated with a submission, the location of hardcopy files associated with a submission, and the availability of staff and resources.

⁴⁰ Several FBI contractors indicate that they maintain informal tracking of their daily time and name check production that is provided to a non-FBI contracting official on a periodic basis. The FBI does not maintain records of contractor hours for measurement purposes.

⁴¹ As discussed in Finding II and Appendix V, the NNCP does not maintain an accurate system for tracking name checks.

REDACTED – FOR PUBLIC RELEASE

in a high volume of false negatives and false positives in the name check process. In addition, the NNCP has not ensured the full utilization of NCDD.

The impact of NNCP's technological shortcomings on name check production and efficiency is exacerbated by shortcomings in the management of NNCP's human resources. We determined that the NNCP's training of name check analysts is inconsistent, infrequent, and inadequate. Furthermore, we noted a scarcity of experienced supervisory staff available to coach and review the work of numerous contractors who the FBI hired to boost production. These deficiencies increase the likelihood that name checks are conducted using inconsistent procedures, impacting the overall quality and potentially the accuracy of name check work. NNCP supervisors are also unable to effectively implement name check production metrics because of the lack of a consistent name check tracking system, and NNCP has not implemented a comprehensive quality assurance process. These deficiencies are of concern given the large investment in terms of human capital that is being used to reduce the NNCP's backlog.

Recommendations

We recommend that the FBI:

1. Implement procedures to periodically test and update its name matching phonetic search tools.
2. Explore other phonetic search tools to work in conjunction with or as a replacement for its current Soundex-based algorithm.
3. Ensure that the NNCP participates fully in the work of the federal identity matching community.
4. Ensure that the NNCP coordinate closely with the ITB to assure that interim and long-term technology efforts modernize the FBI's name matching capability.
5. Develop standardized instructions and training for analysts regarding the use of the NCDD.
6. Immediately resolve the directory mapping issues between the T Drive and the NCDD.

REDACTED – FOR PUBLIC RELEASE

7. Develop and implement a formal curriculum that includes job-related annual or recurring training to enhance process consistency and program continuity.
8. Explore providing system access opportunities to new hires during name search and dissemination training.
9. Review supervisor-to-staff ratio, and develop a plan for immediately increasing the supervisory presence at the Winchester facility.
10. Develop and implement quality assurance measures and guidance for all steps of the name check process.
11. Develop and implement a reliable name check submission and completion tracking function so that NNCP can effectively monitor its name check production activities.
12. Develop plans for reevaluating production metrics on a periodic basis to appropriately evaluate personnel production.

REDACTED – FOR PUBLIC RELEASE**II. NAME CHECK MONITORING AND PROGRAM IMPROVEMENTS**

Due in part to limited automation, NNCP management is unable to appropriately measure and monitor name check workflow. The lack of an effective measurement and tracking system delays name check processing and hinders the NNCP's interaction with customer agencies and FBI field divisions. Valid and reliable production statistics are necessary for the NNCP to adjust staffing levels in response to incoming name check volume, corroborate incoming submissions with customer agency submissions, and keep FBI contributing divisions informed on requirements, policies, and deadlines. While FBI officials stated that their long-term objective is to implement a largely automated name check process, we found that the FBI did not raise its name check user fees for 17 years, resulting in lost opportunities to enhance its automated systems and the NNCP's staffing levels. In addition, NNCP is working without a well-defined business plan to guide its automation, work flow, staffing, fee structure, communications, and program improvements.

Monitoring Workflow

An essential component to ensuring timely name checks is measuring and monitoring the name check workflow process. NNCP management recognizes that deficiencies in program monitoring hinder its ability to assess production trends, and officials repeatedly emphasized that technology limitations prevent them from developing advanced performance measurements without time-consuming manual data retrieval from the FBI's Information Technology Operations Division (ITOD).

During our audit, NNCP officials were refining a customized production model to consolidate several measurements captured by the Name Check Program (NCP) mainframe application. NNCP officials stated that the model will aid management in monitoring name check production by capturing the number of customer submissions received, in progress, and completed; the name check phase where submissions are located; and the rate of processing by FBI and contract personnel. Subsequent to our audit, NNCP managers informed us that the model is in use and providing the basis for forecasted and actual name check production. Nevertheless, even if the new production model provide results that accurately reflect data in the NCP mainframe application, the resulting information may be questionable due to the reliability of the underlying data. For example, during our audit we

REDACTED – FOR PUBLIC RELEASE

noted that NNCP management was unable to measure and monitor name check workflow due to limitations in its automated systems to accumulate production statistics and inadequate tracking mechanisms to account for expedited name check requests and field division file reviews.

Name Check Production Statistics

During our audit, we requested several measurements associated with name check production. In many cases, NNCP management could not provide specific reports on the incoming work, such as the number of high priority requests (expedites) versus routine requests and the status of name check requests from FBI field divisions. According to a mission needs statement dated December 2005, an internal assessment completed in June 2007, and an external assessment completed in December 2007, the reliability of NNCP tracking and reporting are constantly suspect, and the NNCP systems do not offer proper management controls or reporting options on efficiency and effectiveness due in part to multiple stand-alone systems and databases that are not always synchronized. In addition, for the information that was provided, we compared various data sources from the FBI to determine its reliability, and found inconsistencies that led us to doubt the accuracy and validity of production data being used for current production statistics. Valid and reliable production statistics would allow the FBI to adjust staffing levels in response to incoming name check volume, and corroborate incoming submissions with customer agency submissions.

Prior to FY 2006, NNCP managers lacked access to necessary name check production reports. However, with cooperation from ITOD, the NNCP now receives data via an FBI Intranet report function.⁴² Although NNCP management now has access to necessary production reports, it still lacks the capability to accurately produce, analyze, and report certain name check production measurements. For example, according to the December 2007 external assessment, NNCP does not have automated real-time performance metrics for new versus trained personnel, and managers must create custom tracking reports using spreadsheets and other tools to create metrics for decision making and to manage workloads. In addition, the NCP mainframe application cannot group analysts by name check unit or contractor to

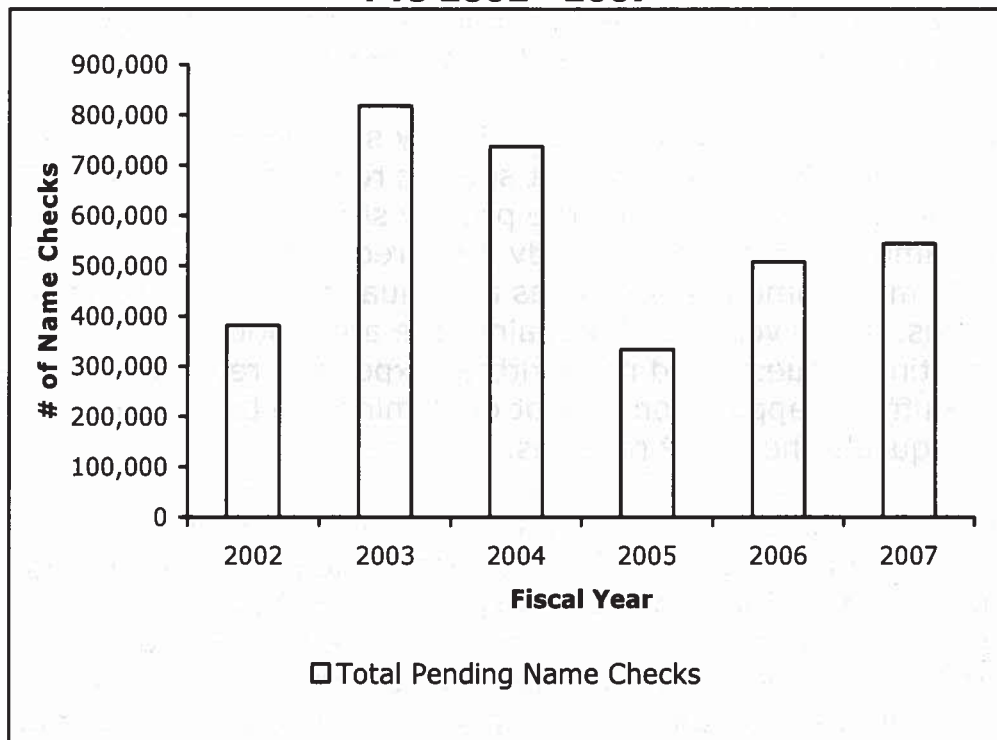
⁴² The Intranet provides data from the FBI NCP mainframe application. The Intranet, however, is not interoperable with the NCP mainframe and must be updated periodically with changes to the mainframe data. Appendix V discusses the reports the NNCP can now obtain and the reasons we do not believe the data is reliable.

REDACTED – FOR PUBLIC RELEASE

determine the production volume by specific groups.⁴³ The NNCP also cannot automatically: (1) report where a particular name check is in the processing queue, and (2) target and evaluate individual name checks by the phases subsequent to the Batch Run. Without such discreet measurements, NNCP management is limited in its ability to develop effective backlog reduction plans.

As displayed in Table 10, the FBI reduced the backlog of name check requests in FYs 2004 and 2005, but the pending number of name checks increased in FYs 2006 and 2007.

**TABLE 10: Total Customer Submissions Pending
FYs 2002 –2007**



Source: FBI NNCP

Tracking Requests for Expedited Name Checks

Name check requests are received from customer agencies in various formats, including an automated secure network portal, magnetic tape, or manual hardcopy such as a request by e-mail, facsimile, letter, or telephone. While a majority of USCIS requests are routine and submitted via magnetic tape, if USCIS wants the name check expedited it generally sends a facsimile

⁴³ NCDD can produce reports depicting volume by team. However, this information is based on archived data from the NCP mainframe application that are periodically uploaded into NCDD.

REDACTED – FOR PUBLIC RELEASE

to a specific individual at the NNCP who determines if the name check is already in the NCP mainframe application. USCIS will request expedited name checks for various reasons including medical emergency, military deployment, or loss of Social Security Benefits.

A request for an expedited name check is considered a top priority and is generally sent to the front of the name check processing queue with other priority submissions. However, moving a name check request to the front of the queue does not mean the request will necessarily be completed before other name check requests. The completion of name checks is dependent upon numerous factors including the number of FBI files that need reviewing, the location of the files, and whether the file referenced is in an on-going investigation or the information in the file comes from a third party (another agency). The NNCP tries to limit the number of requests for expedited name checks by USCIS to 100 per week.

If USCIS is requesting that a previously submitted name check be expedited, the NNCP will identify that specific request within the NCP mainframe application and adjust the priority status accordingly. If the expedited name check has not already been requested, it must be entered into the NCP mainframe application as a manual request with appropriate priority status. However, the NCP mainframe application cannot distinguish between routine requests and reprioritized expedited requests. Therefore, the NCP mainframe application cannot determine the total number of expedited requests the NNCP receives.

Prior to June 2007, the analyst receiving expedited submissions did not track reprioritized customer submissions because it was not required by NNCP management. Concerned that expedited USCIS name checks were not being received by the NNCP, in June 2007 the USCIS began requesting a periodic listing of USCIS expedite submissions received by the NNCP. In an attempt to verify the accounting for expedite submissions, we compared the submission volume from June to September 2007 and determined that the NNCP analyst calculated more expedited USCIS name check submissions – 1,495 for 4 months – than the 374 manual submissions identified in the NCP mainframe application for the entire fiscal year.⁴⁴

⁴⁴ Further, the NNCP indicated that between October and November 2007 several changes in the USCIS personnel responsible for sending USCIS expedite name checks to the NNCP created confusion in calculating the volume of USCIS expedited name check requests. The NNCP is working to resolve the matter and account for name checks submitted during that time period.

REDACTED – FOR PUBLIC RELEASE

Expedite submissions are considered a priority for customer agencies such as the USCIS. Therefore, the NNCP should ensure the NCP mainframe application can identify and account for expedited submissions. Additionally, although the NNCP now tracks reprioritized expedited USCIS submissions in a spreadsheet, it does not track reprioritized expedite submissions from other customer agencies. We recommend that the NNCP work with customer agencies and develop a formal mechanism to receive and monitor expedite submissions.

Field Division File Reviews

The NNCP's difficulty in tracking the status of name check submissions also delays name check processing when a pertinent file is located in one of the FBI's 265 worldwide field office locations. When sending a name check request to an FBI field division for file review, an NNCP analyst may send an e-mail, an Electronic Communication (EC), or call the field division's point of contact (POC). ECs are tracked in the FBI's Automated Case Support (ACS) system, which records the date the request was uploaded, assigned, and closed. However, during our audit file review requests made by telephone and e-mail were not consistently tracked or recorded by the NNCP. In cases where derogatory information on the subject is identified, a field division reviewer will send an LHM to the NNCP analyst for dissemination to the customer agency. We discussed and observed the field division file review request process with NNCP personnel in Winchester, Virginia, and were told that field division responses delay the NNCP in completing name check requests. The NNCP, however, could not quantify these delays.

In FY 2007, 7,222 ECs were assigned to field divisions and Legal Attaché offices for NNCP file reviews. We reviewed EC activity from FBI field divisions located in San Francisco, Los Angeles, New York, Miami, and Washington, D.C. These field divisions comprised almost 40 percent of all ECs assigned by NNCP in FY 2007 and were identified by NNCP personnel as being slow responding field divisions.⁴⁵ We tested a total sample of 296 ECs and found that 42 percent were closed after the deadline. This resulted in requests being on average 11 days late, as shown in Table 11:

⁴⁵ Telephone and e-mail field division file review requests were not consistently tracked or recorded by NNCP and therefore could not be used in testing. Therefore, it is impossible to determine how many requests were submitted via e-mail or telephone and if these requests delay the name check process.

REDACTED – FOR PUBLIC RELEASE**TABLE 11: Timeliness**

Field Divisions	Percentage of Sample Late (All Customer Agencies)	Average Number of Days Late
Washington, D.C.	64	24
New York	33	2
Miami	57	14
Los Angeles	45	10
San Francisco	12	4
Total	42	11

Source: OIG testing of ECs provided by FBI Field Divisions

As mentioned previously, NNCP officials have a 30-day goal for processing all name check requests. Our testing revealed that the NNCP tried adhering to this goal by establishing deadlines for field divisions to respond to NNCP file review requests. However, we noted that deadlines were inconsistent across field divisions and customer agencies. Therefore, we believe it is misleading to generalize that field divisions delay name check processing. As shown in Table 12, our testing found that field divisions had an average of 26 days to complete a USCIS name check request, 22 days to complete an OPM request, 59 days to complete a Central Intelligence Agency (CIA) request, and 20 days to complete a U.S. Department of Energy (DOE) request. We noted that these deadlines also changed by field division. Washington, D.C. was given 28 days to complete a USCIS name check request, while New York was given 20 days and Los Angeles was given 30. These deadlines are not consistent with the NNCP's 30-day processing goal. Our review of the ECs also indicated several instances of short deadlines such as a few days, and we found two instances where the EC was assigned after the deadline date in ACS had already passed.

TABLE 12: Field Division Deadlines in Days

Field Divisions	Average Deadline (USCIS)	Average Deadline (OPM)	Average Deadline (CIA)⁴⁶	Average Deadline (DOE)
Washington, D.C.	28	15	60	21
New York	20	11	N/A	22
Miami	27	20	60	21
Los Angeles	30	50	58	21
San Francisco	25	16	N/A	16
Total	26	22	59	20

Source: OIG Testing of ECs provided by FBI Field Divisions

⁴⁶ For the New York and San Francisco field divisions, the sample did not capture any requests from the CIA.

REDACTED – FOR PUBLIC RELEASE

Field division personnel told us they believed that the NNCP often sets unrealistic processing times. Three field divisions stated that their closed files are stored off site and take time to access. In addition, we were told by two field divisions that NNCP uploads ECs incorrectly. The POC at one field division told us that ECs had been uploaded to employees that were no longer with the field division, some of whom had been gone for an extensive period of time. We tested the processing time for the field divisions we sampled and found that field divisions took on average 32 days to complete a name check request. However, the time varies dramatically between field divisions, as noted in Table 13.

TABLE 13: Processing Times in Days

Field Division	Average Processing Time
Washington, D.C.	47
New York	22
Miami	40
Los Angeles	44
San Francisco	9
Total	32

Source: OIG Testing of ECs provided by FBI Field Divisions

While San Francisco had a dedicated person to handle NNCP requests, in many cases the person responsible for handling field division file review requests has other responsibilities and is assigned NNCP requests as an ancillary duty.

We also reviewed the POC list provided by the NNCP to its analysts, and determined that three field divisions had no POC and no contact information listed, while five other divisions lacked contact information for the POC. For one of our sampled field divisions, we were told that the POC listed on the sheet had left the FBI almost 2 years prior to our review. The POCs in our five sampled field divisions stated that the NNCP lacked a centralized POC for field divisions and none had regular contact with the NNCP. None of the field division POCs we interviewed had any name search or file review training or guidance. In fact, some POCs were not aware of how the name check process works.

From our discussions with the POCs at the five sampled field divisions, we determined that NNCP follow up on outstanding file review requests (lead) was infrequent and inconsistent. On the day we contacted one of the sampled field divisions (October 2007), the POC had received a phone call from the NNCP related to a request uploaded in February 2007. After researching the EC serial number in ACS, the POC determined that the lead

REDACTED – FOR PUBLIC RELEASE

had not been assigned to the field division. The POC expressed frustration that it took almost 7 months for the NNCP to follow up on the request. At another field division, we were shown several pages of NNCP EC requests that had been assigned to the wrong person, and thus lingered unassigned in ACS having been uploaded to someone besides the POC. In some cases, the POC told us the ECs were assigned to persons no longer at the field division, and this POC did not know that these leads were outstanding or had been uploaded in the system. This same employee indicated that several months prior to our visit, the RMD had contacted the field division's Special Agent in Charge to determine the status of six name checks. The field division could find no record of leads set in ACS for the requests. Without regular and consistent follow up, we were told that field divisions unknowingly leave misassigned ECs in ACS, which delays the processing of the name check request. Given the considerable problems the field divisions face in processing name check requests, we cannot determine if delays are caused by the field divisions or the NNCP's processes. Therefore, we recommend the FBI develop guidelines for submitting field division file review requests and follow-up procedures. We also recommend that the NNCP identify a central point of contact for field divisions in order to improve communications.

NNCP Interaction with Customer Agencies

As a reimbursable program, NNCP officials must work with customer agencies to provide information that meets their needs. We met with officials from the USCIS, OPM, and DOS to determine how they interact with the NNCP, how they transmit and track name check submissions to the NNCP, and their level of satisfaction with NNCP's name check services. Each of the customers stated that the NNCP provides critical information that cannot be obtained through other means. This is particularly true for the USCIS, which despite long-delayed name checks, continues to value the NNCP's services.

OPM officials stated that they needed to play an active role in the name check process with the issuance in 2004 of Homeland Security Presidential Directive 12, which mandated background investigations for all federal employees and contractors, and a subsequent federal law that imposes limits on security clearance processing times for federal employment.⁴⁷ As a result, OPM in cooperation with the FBI designated an

⁴⁷ The Intelligence Reform and Terrorism Prevention Act (Pub. L. No. 108-458 (2004)) requires adjudicative agencies such as OPM to ultimately adjudicate applications within an average of 60 days.

REDACTED – FOR PUBLIC RELEASE

on-site official to oversee its name check requests at the NNCP. According to OPM, this resulted in an increase in NNCP's productivity for OPM's name checks by introducing a new way of transmitting name check requests via a secure portal, developing a new system to link the OPM requests to the FBI system, providing 31 contractors to perform OPM name checks, and tailoring the NNCP training to meet OPM needs.⁴⁸

FBI managers stated that they are now in touch with USCIS officials on a regular basis to discuss processing delays. As previously discussed, the resubmission of USCIS name checks in FY 2003 is one contributor to the NNCP's delays. With advance notice and planning, FBI officials said they may have been able to reduce the impact of the 2.7 million USCIS resubmissions on the name check workload. In addition, the USCIS received nearly 7 million applications or petitions for immigration benefits in FY 2007, including nearly 1.4 million petitions for naturalization. This record number of applications and petitions may be caused by applicants filing their applications and petitions to avoid a fee increase that went into effect on July 30, 2007. Given these trends, the FBI needs to adequately communicate with customers and plan for future surges in name check requests.

In contrast to NNCP managers, name check analysts have minimal to no contact with USCIS representatives outside of NNCP facilities in Washington, D.C. Therefore, if a question arises on a name check that could be resolved by acquiring additional information, NNCP personnel have generally deferred to NNCP supervisors who, as previously noted, were overwhelmed by the large number of new FBI employees and contractors. Given the success that OPM had with its on-site personnel, we recommend that the NNCP provide USCIS the opportunity to either maintain an on-site representative in the NNCP's Winchester, Virginia, facility to oversee USCIS name check requests or establish a dedicated central point of contact for NNCP analysts to contact for additional information.

Cost Recovery

During the audit, NNCP officials stated that its backlog of name checks is partially due to reliance on manual processes and that technological improvements could not be implemented due to a lack of funding. However, while the FBI is authorized to charge a fee for name checks and is required

⁴⁸ The new method of transmitting name check requests and responses is via a secure portal, which allows the FBI and OPM to transmit name checks through a shared interface, allowing OPM to match a name check response from the FBI with the original request. The secure portal eliminates "lost" requests that can occur with magnetic tape and reduced the number of OPM duplicate requests.

REDACTED – FOR PUBLIC RELEASE

to reassess its fees biennially, the FBI did not revise the fees it charged for name checks until FY 2008, 17 years after the first fees were implemented.⁴⁹ Further, the FBI did not charge customers an authorized surcharge to fund FBI's technological enhancements. According to a senior FBI official, the FBI saw no reason to revise the NNCP's fee structure during the previous 17 years because it believed that resources were adequate to handle the workload. However, the FBI agrees that the NNCP was understaffed and is lacking in modern automation and technology.

As noted in Table 14, the NNCP established a new fee structure for FY 2008 that increased the cost of a name check by 7 to 177 percent depending on the type of name check services required. Additionally, the NNCP now includes a \$1 technology charge to fund future automation and IT enhancements of name checks. The FBI estimates that its \$1 technology charge will generate nearly \$7.2 million for IT investments in FYs 2008 and 2009. Although during the course of this audit the FBI assured us that it plans to evaluate its fee structure every 2 years, we recommend that the FBI develop formal procedures for reassessing its fee structure biennially to ensure proper cost recovery.

⁴⁹ The FBI may establish and collect fees to process name check requests for non-criminal justice, non-law enforcement employment, licensing purposes, and for certain employees of private sector contractors with classified federal contracts. The fees may be used for salaries and other expenses incurred in providing these services, and include an automation surcharge to fund future technology improvements. (See 28 U.S.C. § 534 (2002)). OMB Circular A-25 requires the review and adjustment, where applicable, of user fees every 2 years. However, fee adjustments must be consistent with the Circular's policies.

REDACTED – FOR PUBLIC RELEASE**TABLE 14: NNCP Name Check Fees**

Name Check Service⁵⁰	Fees FYs 1991 – 2007	Fees FY 2008
Electronic Review (Batch Process)	\$1.40	\$1.50
Name Check Analyst Review (Routine)	\$10.65	\$29.50
Manual Submission (Paper Based Request)	\$12.00	\$29.50
Name Check Analyst Review (Expedite)	\$22.65	\$56.00

Source: FBI Finance Division

In addition to not reassessing its fees on a biennial basis, we found that some customers are frequently not charged for name check services related to special events such as National Football League or Major League Baseball games. NNCP officials said that several customer submissions are filtered through various FBI divisions and offices for national security purposes. FBI divisions and offices designated these customer's requests as high priority and of national significance; therefore, the name check requests are given law enforcement status and are not subject to the name check fees.

We reviewed the FBI's roster of customers submitted for law enforcement purposes and saw potential areas of lost funds. As shown in Table 15, special event submissions exceeded 260,000 submissions between FYs 2003 and 2007. Depending upon the type of name check service received, the NNCP has not collected between \$376,660 and \$9,322,340 in potential name check service fees for these high-priority events. According to NNCP officials, the customers listed often require priority designations and consume the immediate attention of analysts who were working on other name check submissions.

⁵⁰ If the electronically submitted name check goes through the batch run and results in a determination of "NO RECORD" the customer is charged the electronic review charge only. If the name check needs further attention by a name check analyst or was submitted manually, the name check falls into the next two categories of fees. Finally, if the customer requests an expedite name check, the name check is moved up in the work queue; for this consideration the customer is charged a higher fee.

REDACTED – FOR PUBLIC RELEASE**TABLE 15: Name Check Submissions
Filtered through FBI Divisions and Offices
(FYs 2003 – 2007)**

Customer/ Event	Name Check Submissions	Minimum Non-Law Enforcement Fee⁵¹	Maximum Non-Law Enforcement Fee⁵²
Army-Navy Collegiate Football	12,015	\$ 16,821	\$ 416,320
Major League Baseball	12,590	17,626	436,244
Belmont Stakes	7,397	10,356	256,306
Breeder's Cup	1,805	2,527	62,543
National Football League	112,557	157,580	3,900,100
Preakness Stakes	2,146	3,004	74,359
Greece & Torino Olympic Games	59,949	83,928	2,077,233
U.S. Golf Open	7,874	11,024	272,834
U.S. Tennis Open	50,408	70,571	1,746,637
Women's World Cup Soccer	2,302	3,223	79,764
TOTAL:	269,043	\$376,660	\$9,322,340

Source: FBI NNCP

We question whether the FBI and U.S. taxpayers should be required to absorb the full cost for these customers' identification services. As a sign of change, NNCP management said that Major League Baseball has agreed to pay for some of its name check services beginning in FY 2008. However, we recommend that the FBI review the fees charged to customers and establish payment criteria together with a uniform policy for accepting name check submissions from its divisions and offices from these high priority customers.

Long Term Plans for Improving NNCP Operations

The FBI recognizes the need to reengineer the NNCP and believes that one way to address the name check backlog is to have a modern records management system. In FY 2004, the FBI's RMD introduced plans to implement a modern records management facility known as the Central Records Complex (CRC) to improve how the FBI organizes and retains its

⁵¹ The minimum service fee charged by the FBI is \$1.40 per name check submission. This service fee for names submitted on electronic medium includes only an electronic Batch Run search of the FBI files.

⁵² The maximum fee charged by the FBI is \$34.65 per name check submission. This service fee is applied to manual name submissions designated as expedites by the submitting customer agency. All requests for an expedited name check are provided the highest priority level, and are generally sent to the top of the queue with other priority submissions, which indicates to analysts that this request should be started first.

REDACTED – FOR PUBLIC RELEASE

records. While the CRC is not being pursued solely for the benefit of the NNCP, the FBI believes CRC will solve many of the causes contributing to the current name check delays. In addition, FBI officials stated that their long-term objective is to implement a largely automated name check process. However, we noted that the NNCP is working without a well-defined business plan to guide its automation, workflow, staffing, fee structure, and program improvement initiatives.

Central Records Complex

According to NNCP officials, many name checks are delayed while analysts wait to acquire hardcopy documentation from FBI files. According to RMD, about 30 percent of USCIS name checks reaching the dissemination stage require access to paper files. In addition, RMD officials stated that many documents, such as faxes, paper copies of external documents, and receipts, are not available electronically. By improving how the FBI organizes and retains its records, analysts will have the ability to easily locate FBI files and will be provided scanned electronic documentation for dissemination. As planned, the CRC will: (1) consolidate all FBI records (excluding active case files) in a single facility, (2) provide a comprehensive inventory database to search and request files, (3) use an automated storage and retrieval system to physically pull requested hardcopy files, (4) offer scan-on-demand capability to convert paper files to electronic form for automated accessibility, and (5) provide electronic storage of scanned files for immediate access to subsequent requestors. The RMD anticipates that requests to review files that once took weeks or even months to retrieve will be available within minutes. As of January 2008, the FBI projects that the CRC will be completed by December 2010, and plans to move personnel and operate the facility by the end of March 2011.

We could not evaluate the long-term impact the CRC will have on the NNCP due to uncertainties with the project, including how the NNCP will address the relocation of material and physical resources to the CRC, the training required for CRC operation, as well as the timely delivery of CRC components. While RMD management recognizes the need for a carefully planned transition, we did not note any formal strategic planning to address the impact of the CRC on name check production.

The NNCP believes that the CRC will speed the name check process because closed files will be centrally located and the NNCP will be less dependent on field offices for the retrieval and review of files. Although having NNCP supervisors and staff located in one facility with closed files will improve production, we believe that the CRC will have less impact on the NNCP workflow process than the RMD anticipates because FBI case files after

REDACTED – FOR PUBLIC RELEASE

1995 should already be available electronically via the Electronic Case File (ECF) program within ACS; open case files will continue to be maintained at individual field divisions; and according to the FBI, every terrorism record is already digitized. While we cannot quantify the number of LHMs that result from information obtained in case files closed prior to 1995, we understand that as time progresses files prior to 1995 will become less relevant to the name check process. Moreover, the agreement signed by USCIS and FBI officials in October 2007 creating the Super and Mega filters facilitated the closure of over 15,000 name checks, eliminated over 50,000 files from current and future review, and eliminated just over 27,000 names from the name check process. Omitting these files from name check processing further reduces the number of files that are accessed by NNCP analysts. Finally, as Sentinel is implemented the FBI's paper-based records will become less relevant because future case file records will be maintained electronically.

Long-Term Business Plan

The NNCP identified general requirements that included a single name check application, a tracking system with precise metrics, and an effective workload management and distribution system. Rather than reengineering the existing processes, the NNCP supplemented its antiquated processes by significantly increasing the number of personnel performing manual name check functions. In addition, the only significant technological enhancements we noted were a user-friendly dissemination interface to scanned documentation and efforts to implement a text recognition tool. However, these efforts have not solved the lingering backlog of name check requests.

We believe that the NNCP requires a detailed business plan incorporating established milestones with accurate reimbursable fee assessments to reduce its backlog and aid in the implementation of new technology. A well-defined business plan would assist NNCP managers in prioritizing and addressing the significant issues hampering this program's operations and help ensure the success of ongoing initiatives. We believe that the NNCP's operations would benefit from developing such a long-term plan to improve workflow monitoring, reduce the communication breakdowns between the NNCP and its customer agencies, ensure proper cost recovery through name check fees, and guide long-term operational improvements.

REDACTED – FOR PUBLIC RELEASE

During our audit, the NNCP developed a draft plan for FY 2007 NNCP operations, as well as customer-level operations plans for OPM and USCIS. The FY 2007 draft plan is a general plan for the NNCP that highlighted the NNCP's mission, organization, and corrective action initiatives. However, it did not include vital elements such as an assessment of the NNCP core competencies, the steps necessary to achieve program objectives, and a plan or timeline to deliver the identified corrective actions.

In March and April 2008, the NNCP finalized customer-level operations plans with USCIS and OPM, respectively. According to the USCIS plan, the NNCP and USCIS hope to have addressed all name checks pending more than 2 years by July 2008 and those pending more than 1 year by November 2008. The plan also outlines how the NNCP will meet its June 2009 goal of processing 98 percent of USCIS's name check requests within 30 days. Likewise, the OPM plan discusses eliminating by April 2009 all OPM name checks pending over 40 days. Both plans rely on using the NNCP's current processes and state that the FBI is issuing a statement of work designed to obtain the services of a contractor to reengineer the name check process with contemporary technology and business practices.

According to the FBI, while the NNCP has executed customer-level operations plans, it has not yet participated in the FBI's Strategy Management System (SMS) to address the need for overall strategic planning. In the summer of 2006, the FBI began implementing SMS to help the FBI map its strategic objectives and align day-to-day operations. The FBI's Resource Planning Office (RPO) is responsible for implementing SMS within the FBI, and many of the FBI's operational divisions and key support divisions have completed this process. RPO managers indicated that SMS has proven useful and effective for other FBI Divisions at aligning priorities and resources. According to RPO managers, the process of aligning RMD's strategies with the overall FBI strategies will begin in July 2008 and should be completed by October 2008.

Conclusion

Our audit identified areas where NNCP monitoring of name check processing requires improvement. NNCP management was unable to monitor name check workflow due to limited automation and inconsistencies in the name check process. Although the FBI could have raised significant money by charging appropriate user fees to its customers, we found that the FBI did not raise its fees for 17 years, resulting in lost opportunities to enhance its antiquated automated systems and the NNCP's staffing levels. We believe that the NNCP requires a detailed business plan incorporating

REDACTED – FOR PUBLIC RELEASE

established milestones with accurate reimbursable fee assessments to reduce the backlog and aid in the implementation of new technology.

Recommendations

We recommend that the FBI:

13. Work with customer agencies and develop a formal mechanism to receive and monitor all expedite submissions.
14. Develop and maintain a current list of central points of contact for field divisions in order to improve communication between the NNCP and field divisions.
15. Develop guidelines for submitting field division file review requests and follow-up.
16. Provide USCIS an opportunity to improve communications at the name check analyst level by overseeing its name check requests at the Winchester, Virginia, facility with an on-site representative or establishing a dedicated central point of contact for NNCP analysts to contact for additional information.
17. Develop procedures for reassessing its fee structure every 2 years to ensure proper cost recovery.
18. Establish a uniform policy for accepting and charging FBI field divisions for third-party name check submissions.
19. Develop a long-term business plan for improving the efficiency and accuracy of the NNCP's name check process.

REDACTED – FOR PUBLIC RELEASE

III. FINGERPRINT IDENTIFICATION TIMELINESS AND ACCURACY

Since FY 2005, the FBI has processed over 20 million fingerprint identification requests annually. In contrast to the name check process, we found that the FBI's fingerprint identification process is largely automated, allowing FBI to generally process requests accurately and timely. Sophisticated technology combined with trained personnel, efficient tracking mechanisms, and proficient communication methods have enabled the FBI to process millions of fingerprint submissions per year. In FY 2007, CJIS completed 98.8 percent of all civil fingerprint identifications within 24 hours. In addition, CJIS seeks customers' input for new technology and proactively enhances the technology to be as automated as possible.

Automating Fingerprint Identification

In the early 1990s, the FBI partnered with the law enforcement community to revitalize the fingerprint identification process, leading to the development of IAFIS, which became operational in July 1999. Prior to IAFIS, substantial delays were a normal part of the fingerprint identification process because fingerprint cards had to be physically transported and processed. As a result, fingerprint identifications could often take months to complete.

As a result of the automation, fingerprint identifications occur rapidly. For example, in FY 2007 CJIS processed civil fingerprint submissions within 24 hours in 98.8 percent of the cases. Three large agencies who utilize CJIS services – USCIS, OPM and DOS – raised no quality or timeliness issues when we interviewed them about the FBI's fingerprint identification services. We determined that unlike delays with name checks, the FBI's fingerprint checks were not impeding USCIS's ability to adjudicate immigration benefits.

In December 2007, CJIS announced a 10-year, \$1 billion effort to enhance and expand its biometric identification services. Termed the Next Generation Identification (NGI) program, the effort seeks to incorporate a multimodal biometric framework that includes enhanced photographic identification with facial recognition and image searching of scars, marks,

REDACTED – FOR PUBLIC RELEASE

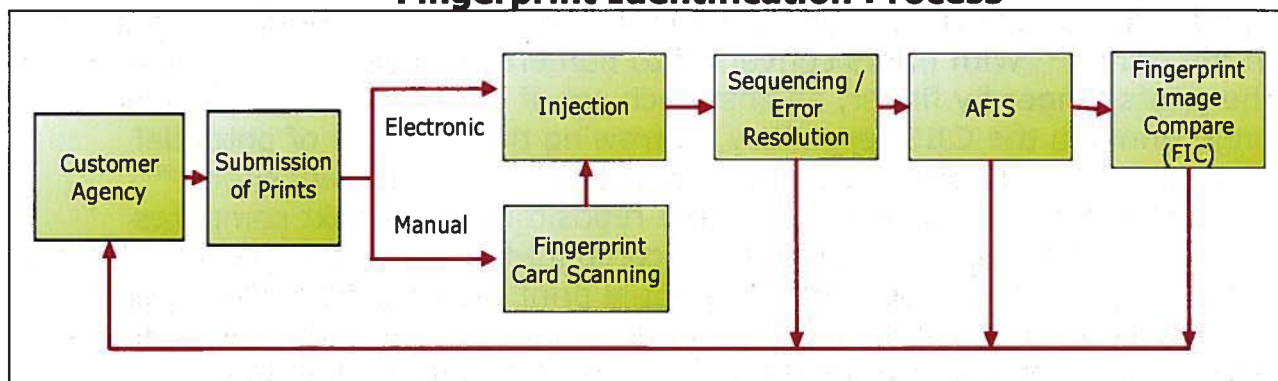
and tattoos, palm prints, iris scanning, and “Rap-Back” services.⁵³ The plans also include improvements to fingerprint functionality, with increased processing capacity, storage, and accuracy. As part of the NGI development process, CJIS participated in User Requirement Canvasses, which included onsite and telephone interviews of agencies who submit fingerprint requests and written surveys resulting in the identification of over 1,000 new requirements.⁵⁴

Fingerprint Identification Workflow Process

IAFIS’s key functions are automated and technology combined with workflow monitoring have enabled the FBI to timely process millions of fingerprint submissions per year with minimal human intervention. Figure C below depicts the IAFIS fingerprint identification workflow process. From a high-level perspective, the fingerprint process involves five distinct steps: (1) submission of electronic or manual fingerprints from customer agencies; (2) the receipt and injection of the prints into IAFIS followed by print error resolution and sequencing, if necessary; (3) automated analysis and identification of fingerprints by AFIS; (4) manual Fingerprint Image Compare (FIC), if necessary; and (5) generation and transmission of customer agency fingerprint check responses.

⁵³ The Rap Back service will allow customer agencies to enroll specific individuals who received a CJIS security check for future criminal history notifications. If an enrolled individual is arrested, charged with a crime, or performs an act that is recorded in one of the CJIS law enforcement databases, the customer agency will receive notification from CJIS.

⁵⁴ The User Requirement Canvass was part of an NGI study contract. The canvass was performed by a CJIS contractor and an NGI representative to identify new requirements. Additionally, CJIS worked in collaborative meetings, such as an NGI workshop, Advisory Policy Board, Working Groups, Compact Council, and the IAFIS Interface Evaluation Task Force Meetings to discuss new service requirements.

REDACTED – FOR PUBLIC RELEASE**FIGURE C: High Level Perspective of the CJIS Fingerprint Identification Process**

Source: FBI CJIS Division

Fingerprints are usually sent electronically to the FBI from federal, state, or local agencies.⁵⁵ Customers provide 10 rolled prints, 10 flat prints, and descriptor information such as name, gender, or address.⁵⁶ For each 10-print submission, an automated search for criminal information on the subject is initiated.

Automated Fingerprint Identification System Analysis and Identification

The comparison of fingerprints to repository information occurs in AFIS. AFIS is the core automated identification module in the integrated fingerprint identification process; it utilizes a mathematical algorithm that extracts various identifying characteristics of a fingerprint image and converts those characteristics into numeric parameters that can be compared. In essence, the degree to which the numeric parameters of a submitted fingerprint match those of another set of fingerprints stored in the electronic repository is represented in a score indicating the closeness of the match.

⁵⁵ Eight percent of fingerprints are sent manually. When hardcopy fingerprints are submitted to the FBI, the prints are sent to a contractor who converts the manual prints to an electronic format. The contractor generally takes 72 hours to convert the manual prints. On average, the FBI takes 14 days to process manual prints.

⁵⁶ Flat prints are taken by placing the impressions of the left four and right four fingers of each hand captured simultaneously, then acquiring each of the thumb prints individually. Rolled prints are taken by rolling the finger from nail edge to nail edge on a reader, resulting in significantly more fingerprint data. Flat prints provide 40-percent less data than rolled prints.

REDACTED – FOR PUBLIC RELEASE

The process of fingerprint identification requires the comparison of several features of the fingerprint pattern. Using an algorithm, AFIS numerically scores the fingerprints that correspond to the points of interest in the prints.⁵⁷ With prints converted to numerical values, AFIS compares the prints, finger by finger, against each set of the more than 50 million fingerprints in the CJIS repository, narrowing the universe of potential matches from 100 percent to 4 percent of the total CJIS repository.⁵⁸ Utilizing the smaller percentage of the repository, AFIS next compares minutia points. Minutia locations are compared at various angles of rotation, identifying the best 1 percent of potential print matches from the 4 percent searched. With a smaller set of potential print matches, AFIS performs its final comparisons, known as the Two-Finger Attributed Relation Graph (ARG), and if necessary the Ten-Finger ARG.

Depending on the ARG score, AFIS can identify a positive match to a subject in the repository, identify that no match exists in the repository, or refer the prints for manual review (also known as Fingerprint Image Compare or FIC).⁵⁹ If the match between two sets of fingerprints is so robust that it yields a score greater than 20,000, the submission will pass through AFIS without human intervention and generate an automatic response indicating a match has been identified. CJIS personnel call those “lights out” submissions. CJIS has also set score ranges to indicate when a fingerprint examiner should intervene and verify a fingerprint match’s accuracy before accepting what the automated system determined. In what is largely an automated process, the FIC is the manual component of the fingerprint identification process. Based upon the accuracy of the fingerprint match to a repository print as determined by the ARG score threshold, customer submitted prints are compared to a repository print by one or two fingerprint examiners.

⁵⁷ CJIS incorporates both fingerprint patterns and minutiae, or points of interest in a fingerprint, into its identification algorithms. The three basic patterns of the fingerprint ridges are the arch, loop, and whorl. The minutia types may include ridge endings, ridge bifurcation (where a ridge splits in two), short ridges, and ridge crossovers, among other things. For each minutia point, a vector or mathematical equation is stored so that the algorithm may account for the points’ type, location, and angle. AFIS will compare the submitted vectors to the vectors stored in the CJIS print repository.

⁵⁸ The comparison eliminates prints by their sequence placement to the corresponding repository prints in the same sequence by pattern class and ridge count. To record a successful match, all 10 pattern classes must correlate and 9 of the 10 ridge counts must correlate.

⁵⁹ The FIC function is a process performed by individuals who are trained to identify and compare specific characteristics of fingerprint minutia between two separate images in order to determine whether a submitted print is a match with the master print.

REDACTED – FOR PUBLIC RELEASE

As shown in Table 16, CJIS officials have gradually decreased the lights-out threshold:

TABLE 16: History of ARG Score Adjustments

Date	Lights Out – Match	1 FIC Required	2 FIC Required
Initial	64,800	20,000 to 64,800	2,800 to 19,999
11/24/2003	Greater than 45,000	20,000 to 44,999	2,800 to 19,999
02/17/2004	Greater than 40,000	20,000 to 39,999	2,800 to 19,999
04/11/2005	Greater than 40,000	16,000 to 39,999	2,800 to 15,999
02/06/2006	Greater than 38,000	16,000 to 37,999	2,800 to 15,999
04/05/2006	Greater than 35,000	16,000 to 34,999	2,800 to 15,999
12/21/2006	Greater than 30,000	16,000 to 29,999	2,800 to 15,999
05/22/2007	Greater than 25,000	16,000 to 24,999	2,800 to 15,999
09/25/2007	Greater than 20,000	16,000 to 19,999	2,800 to 15,999

Source: FBI CJIS

With a confidence-level threshold of 20,000, approximately 72 percent of fingerprint submissions are able to pass through AFIS automatically without human intervention. As CJIS makes such adjustments, a greater volume of fingerprint submissions pass through the automated process without any human intervention, improving AFIS response times. Thus, adjustments to ARG threshold scores are crucial in the management of fingerprint identification workflow.

We reviewed the basis for lowering the lights-out threshold to ensure the reliability of AFIS' results. Our discussions with CJIS management and IT personnel revealed that monthly capacity planning meetings are held to review operational and testing data for the past fiscal year and to consider upgrades and adjustments to AFIS that will allow it to better meet customer needs and performance goals. CJIS officials said they make modifications to AFIS based on several factors, such as technology enhancements, the increasing volume of fingerprints, upcoming initiatives that would increase the volume of fingerprints, and staffing levels.

REDACTED – FOR PUBLIC RELEASE

We reviewed a study prepared by the FBI entitled *Automation of Fingerprint Image Compare*, which reveals that CJIS conducted a 2-week evaluation of the AFIS-threshold change to determine the impact and the accuracy of AFIS-performed identification decisions.⁶⁰ In addition, we reviewed CJIS internal memorandums detailing the threshold changes and noted that CJIS-IT personnel performed system enhancements, tested the changes, and monitored the system after changes were implemented. One such test uses regression test software. The regression test set, which is comprised of 10,000 names, is run through the revised system and compared to the known results in order to determine the accuracy of the revised system. According to CJIS IT management, any abnormalities are corrected immediately.

In addition to the specific testing regarding changes, CJIS identified several quality control processes in place to validate accuracy or identify problems. Specifically, CJIS mentioned an Operational Analysis System Integrity Support Group that researches a variety of resources to detect erroneous comparisons or missed identifications outside the normal workflow. CJIS also has a Quality Assurance Team to detect false positives and negatives.⁶¹ We reviewed the two latest reports and noted that the number of errors was insignificant and that corrective action had been taken.⁶²

⁶⁰ Federal Bureau of Investigation, Criminal Justice Information Services Division, White Paper *Automation of Fingerprint Image Compare* (January 31, 2004). The study discussed the 2-week evaluation of the initial AFIS High-Threshold change from 64,800 to 45,000 (November 24, 2003). The study determined the impact and accuracy of AFIS-performed FIC decisions and concluded that the 45,000 AFIS Threshold should be maintained, and also recommended a further reduction of the AFIS High-Confidence Threshold Level to 40,000.

⁶¹ A false positive occurs when either IAFIS or a fingerprint examiner indicates that a fingerprint submission matches a print in the repository, when in fact it does not match the print. A false negative is when either IAFIS or a fingerprint examiner indicates that a print does not match a specific print, when in fact the print is a match.

⁶² In 2006, the Operational Analysis System Integrity Support Group identified 136 errors, of which 108 were system-caused, with the remainder employee-caused errors. In 2005, the group identified 86 errors, of which 54 were system-caused, with the remainder employee-caused errors. Given that CJIS processed 20 million prints in FY 2005 and 23 million prints in 2006, the noted errors were insignificant.

REDACTED – FOR PUBLIC RELEASE

We found that while CJIS personnel perform a variety of tests supporting adjustments to the ARG scoring threshold and could easily recite the methods used for processing changes to AFIS, CJIS does not have written policies and procedures for documenting and approving adjustments to AFIS. We believe that the lack of written policies and procedures is an internal control weakness that could lead to unapproved and undocumented changes. Therefore, we recommend that CJIS develop and implement written policies and procedures for documenting and approving adjustments to AFIS.

Fingerprint Fee Structure

The FBI establishes and collects fees to process fingerprint identification records for non-criminal justice, non-law enforcement employment, licensing purposes, and for certain employees of private sector contractors with classified federal contracts.⁶³ Prior to FY 2008, CJIS had not revised the fees charged for fingerprint identifications since FY 1994, which was 5 years prior to the implementation of IAFIS.⁶⁴ In FY 2008, CJIS adjusted the fee schedule to help account for current costs in human resources, capital assets, and continued automation. Table 17 compares the fingerprint fee structure for FYs 1994 through 2007 to the new fees established in FY 2008.

⁶³ The fees may be used for salaries and other expenses incurred in providing these services, and include an automation surcharge to fund future technology improvements. See 28 U.S.C. § 534 (2002).

⁶⁴ According to CJIS management, prior to the FY 2008 user fee study CJIS dedicated a significant effort to develop an activity-based cost model. However, until FY 2008, OMB did not officially approve the model.

REDACTED – FOR PUBLIC RELEASE**TABLE 17: Fingerprint Identification Fees**

Fingerprint Identification Service	Requestor	FY 1994-2007 Fee	FY 2008 Fee
Volunteer (Electronic or Manual)*	Federal & Non-Federal	\$18.00	\$15.25
Non-Law Enforcement(Electronic)	Federal	\$16.00	\$19.25
Non-Law Enforcement(Electronic)*	Non-Federal	\$24.00	\$19.25
Non-Law Enforcement (Manual)	Federal	\$18.00	\$30.25
Non-Law Enforcement(Manual)*	Non-Federal	\$24.00	\$30.25
Non-Law Enforcement (Electronic In/Manual Out ⁶⁵)*	Non-Federal	\$24.00	\$26.00

Source: FBI CJIS Division

* includes \$2 billing charge

The new schedule is based on full-cost recovery and is intended to account for the cost of providing identification services.⁶⁶ For example, CJIS has restructured its manual searching fees to account for the increased costs of processing manual fingerprint card submissions versus the electronic submissions that feed directly into IAFIS. In consideration for the planned advancements to CJIS biometric services, and because the FBI is authorized and required to assess its fee structure biennially with an automation surcharge, we recommend that the FBI include as part of its business planning a process for reassessing its fee structure every 2 years to ensure proper cost recovery and future automation expenses.⁶⁷

⁶⁵ For this type of service, CJIS authorization is required. To date, only non-federal customers have requested this service.

⁶⁶ The fee structure was developed to cover costs for the FBI conducting fingerprint-based and name-based Criminal History Record Information identifications. Bearing Point, Inc. developed the fee structure using Activity Based Costing software.

⁶⁷ Office of Management and Budget (OMB) Circular A-25 requires the review and adjustment, where applicable, of user fees every 2 years. However, fee adjustments must be consistent with the Circular's policies.

REDACTED – FOR PUBLIC RELEASE**Personnel**

Although the fingerprint process is mostly automated, CJIS relies on an experienced, well-trained work force to manually perform quality control, sequencing, or fingerprint identification when the fingerprint does not reach the lights-out threshold. CJIS management closely monitors work-in-process and allocates resources to bottlenecks while reviewing the daily or monthly performance statistics.

Training

CJIS has a training unit in the Identification Services Unit that has offered training classes to both employees and CJIS customers.⁶⁸ Training is required before an employee performs AFIS functions, such as FIC, quality control, and logic error resolution (LER).⁶⁹ In addition, if CJIS personnel have not performed a function for a period of time, they are required to take refresher training prior to working in that area. Each function has different training requirements. For example, as shown in Table 18 below the required training for FIC varies depending on how long it has been since the individual performed the function.

TABLE 18: Required FIC training

Length of Time Since Performing FIC	Required Training Period
Never performed FIC	7-9 weeks training
Greater than 1 year	40 hours
Between 180 days and 1 year	16 hours
Between 90-180 days	8 hours
Between 60-90 days	4 hours

Source: FBI CJIS

⁶⁸ CJIS provides customers fingerprint training classes upon request including a 1-day course entitled "Taking Legible Fingerprints" and a 3-day course entitled "Basic Pattern and Recognition."

⁶⁹ The Quality Check Unit is responsible for conducting a detailed analysis of each Criminal and Civil 10-print submission processed by IAFIS to determine if the information on the submission meets basic processing criteria. The LER application is used to resolve errors and inconsistencies that the Interstate Identification Index (III) finds when trying to process a file maintenance request. The objective of LER is to correct all errors that may prevent III from updating the Subject Criminal History Record (SCH). The FIC function is a process performed by individuals who are trained to identify and compare specific characteristics of fingerprint minutiae between two separate images to determine whether a submitted print is a match with the master print.

REDACTED – FOR PUBLIC RELEASE

Annually, employees must also take a 1-day refresher training course that includes the review of the Standard Operating Manuals, memorandums, IAFIS notes and “work-arounds” that apply to the function the employee performs. CJIS provides Standard Operating Manuals for various IAFIS functions, such as the following:

- Quality Check, version 6.0, dated September 21, 2006
- Logic Error Resolution, version 5.0 dated April 9, 2007
- Fingerprint Sequence Check, version 5.0 dated June 22, 2006
- Fingerprint Image Compare, Verify Fingerprint Compare, version 5.0, dated June 22, 2006

The manuals outline the objective of the specific function and responsibilities of various parties involved with the process, detail procedural steps in the process, and provide needed codes or reference check lists. The manuals were constructed to be a user friendly reference to operators with precise instructions and illustrated examples.

Quality Control

Though rare, past incidents of fingerprint misidentifications highlight the need for quality assurance processes and employee accountability.⁷⁰ CJIS has a Standard Operating Manual, which provides broad checklists for each IAFIS function, states that the main objective of the quality assurance examiners is to detect and submit discrepancies to the appropriate personnel. CJIS also has compiled a comprehensive manual, Performance Resource Guide, dated April 1, 2007, that establishes accountability for errors and the processes for handling those errors.⁷¹ The intent of the document is to provide CJIS officials with tools and suggestions for evaluating an employee’s performance.

⁷⁰ In May 2004, the FBI arrested Brandon Mayfield as a material witness in an investigation of the terrorist attacks on commuter trains in Madrid, Spain. Mayfield had been identified by two Latent Print Unit examiners, as well as the Unit Chief in the Latent Print Unit, as the source of a fingerprint found on a bag of detonators in Madrid that was connected to the attacks. Two weeks after Mayfield was arrested, the Spanish National Police informed the FBI that it had identified an Algerian national as the source of the fingerprint on the bag. After the FBI Laboratory examined the fingerprints of the Algerian, it withdrew its identification of Mayfield. The corrective action taken by the FBI Laboratory on the three examiners included providing written explanation for the error, removal from casework, technical review of the examiners’ past cases, proficiency testing, and a training exercise. U.S. Department of Justice Office of the Inspector General, *A Review of the FBI’s Handling of the Brandon Mayfield Case*, Special Report, January 2006.

⁷¹ Federal Bureau of Investigation, Criminal Justice Information Services Division, Identification and Investigative Services Section, internal guidance entitled *Performance Resource Guide*, dated April 1, 2007.

REDACTED – FOR PUBLIC RELEASE

The Performance Resource Guide identifies the Quality Assurance Team, which consists of three related groups: the Product Verification Group, the Quality Assurance Group, and the Statistical Trending, Analysis and Reporting Group. Each group consists of functional experts providing specific verification or validation services. The main objective of the Quality Assurance Team is to detect and immediately correct discrepancies or errors found in CJIS products and services. The Quality Assurance Team logs, tracks and analyzes each error and forwards the error case to the appropriate supervisor. This assists management in identifying system issues and training needs, streamlining business processes, and establishing a confidence level for products and services.

The CJIS Performance Resource Guide outlines acceptable performance and specifies how the calculated accuracy rate impacts employee performance as noted in Table 19.

TABLE 19: Accuracy Parameters Used by CJIS in Performance Evaluation

Outstanding Accuracy	Excellent Accuracy	Successful Accuracy	Minimally Successful Accuracy	Unacceptable Accuracy
Above 99.98%	99.98%	99.97%	99.96%	Below 99.96%

Source: CJIS Performance Resource Guide dated April 1, 2007

To manage errors and ensure that all employees are held to fair guidelines in connection with deficiencies in their work product, a point value is assigned to each error type – the more serious the error, the greater the point value. Points are accumulated by individual personnel and the supervisor calculates the accuracy rate in a prescribed manner. The manual outlines various possible corrective actions to improve accuracy ranging from monitoring telephone use to providing refresher training.

Production Monitoring

As previously noted, fingerprint identification services are provided for criminal and civil submissions, with criminal justice submissions treated as a higher priority. Civil submissions for non-criminal justice purposes are of less priority and have a slightly longer average response time. CJIS's stated vision is to provide world-class person-centric biometric identification

REDACTED – FOR PUBLIC RELEASE

services, including advanced fingerprint, new biometric capabilities, and efficiencies in associated information services.⁷²

In order to quantify this vision, CJIS has established finite system performance metrics in its Strategic Plan. For criminal fingerprints, 95 percent of all submissions are to be processed and returned to the requestor within 2 hours. For civil fingerprints, 95 percent of all submissions are to be processed and returned to the requestor within 24 hours.

We reviewed the methodology CJIS uses to compile the statistics and observed that CJIS has surpassed these metrics as shown in Table 20.

TABLE 20: Electronic Response Times for Fingerprints

Fiscal Year	Criminal		Civil	
	Average In Minutes	Percent Within 2 hours	Average in Minutes	Percent Within 24 hours
2007	15	98%	180	98.8%
2006	21	96.8%	203	98.2%
2005	28	96.7%	195	99.0%
2004	35	94.5%	128	98.7%
2003	65	90.0%	149	97.5%
2002	50	90.3%	145	98.8%

Source: FBI CJIS Division

In FY 2007 CJIS completed 98 percent of the 10-print criminal fingerprints in 2 hours, and 98.8 percent of the 10-print civil fingerprints in 24 hours. CJIS has developed monitoring processes that measure the performance of IAFIS including queue monitoring, daily and monthly statistics, and performance metrics for individuals.

Queue Monitoring

The CJIS Operations Control Center (OCC) is responsible for controlling the flow of fingerprints in IAFIS. Through the OCC, management is aware of the number of fingerprints being submitted to IAFIS, the number of prints in “work-in-process,” and if any bottlenecks are building within the queues. The OCC monitors the “work-in-process” and the injection of incoming submissions into IAFIS, ensuring that enough personnel are available to process fingerprint submissions to meet CJIS response time goals. In addition to controlling the injection of prints, the OCC monitors the workload

⁷² For identification services, the person-centric services model focuses operational efforts on the complete end-to-end processing of individual biometric and biographical information in the delivery of criminal history information to qualified partners.

REDACTED – FOR PUBLIC RELEASE

flow throughout the IAFIS process. OCC directs personnel to switch tasks to reduce bottlenecks, such as switching from quality control to logic error resolution.

In addition, CJIS is able to augment staff through the Staffing and Technical Operations Resource Management (STORM) plan that was initiated in September 2006. This plan retrains former fingerprint examiners in the fingerprint process so they can assist during busy periods. Those assisting may only participate for an hour or two per day. This augmentation helps CJIS continue to provide timely services to customers.

Statistics

CJIS tracks every request for a fingerprint identification from the time it enters IAFIS until the results are returned to the customer.⁷³ The Statistics Department produces three major reports:⁷⁴

- **The Early Morning Report.** Provided to management by 7 a.m. every day, this report contains daily and cumulative statistical information on IAFIS performance. The report is intended for mid-level managers who monitor daily receipts and closeouts of fingerprint submissions and also monitor response times.
- **The Operations Status Report.** Transmitted to more senior management at CJIS, this daily report presents a brief snapshot of total fingerprint processing activity, response times, and staffing levels.
- **The Monthly System Performance Report.** Similar to the Operations Status Report, this report presents response times and IAFIS activity over a cumulative time period.

According to the IAFIS Director of Statistics, the workload follows certain patterns. For example, response time varies by day of the week, and there also may be seasonal fluctuations during the year. If bottlenecks occur in the system, CJIS personnel meet to discuss ways to address the issue.

⁷³ Fingerprint requests are tracked using a variety of identifiers, such as submission identification numbers, type of transaction code, and requesting agency identifiers.

⁷⁴ The statisticians track response times for electronic criminal response and electronic civil submissions. For electronic criminal checks, IAFIS is programmed to tabulate the number of submissions responded to every minute up to 180 minutes, then every hour from 4 to 72 hours. For electronic civil prints, IAFIS is programmed to tabulate number of submissions responded to every minute up to 120 minutes, then by hour up to 72 hours.

REDACTED – FOR PUBLIC RELEASE

Performance Metrics for Individuals

CJIS does not mandate specific performance metrics for its manual functions. However, supervisors have the ability to quantify individual production and error rates. In addition, as part of the performance appraisal, individuals participate in identifying and setting relevant goals and objectives for their own work. This objective is set at the beginning of a performance period and can be adjusted throughout the rating period. At the end of the rating period, the employee's actual achievement is calculated, taking into consideration production and accuracy.

In its strategic plan, CJIS has established a gain-sharing program that provides pay for performance awards to fingerprint examiners who meet eligibility requirements. To be eligible, examiners must work at least 44 hours in the FIC function each month and maintain an overall productivity average of at least 50 prints per hour for each month in the quarter. FIC examiners with more than two IAFIS errors in a quarter will not be eligible for the monetary incentive during the quarter.

Customer Interaction

During our audit we interviewed three large non-law enforcement customers: USCIS, DOS, and OPM. These customers indicated that they were generally pleased with the timeliness of services provided by CJIS. Further, the USCIS has onsite representation at CJIS that promotes communication, coordination, and problem resolution between DHS and the FBI in a timely and mutually beneficial manner.

The FBI also established the CJIS Advisory Process to obtain user community advice and guidance on the operation of CJIS programs. The Advisory Process contains two components: the Advisory Policy Board (APB) and working groups. The APB is responsible for reviewing policy, technical, and operational issues related to CJIS Division programs, and making appropriate recommendations to the FBI Director. The APB is composed of 33 representatives from criminal justice and national security agencies throughout the United States. Working groups and subcommittees were developed to review operational, policy, and technical issues related to CJIS Division programs and policies and make recommendations to the APB. All 50 states as well as U.S. territories and the Royal Canadian Mounted Police are organized into five working groups: Federal, North Central, North Eastern, Southern, and Western. Currently, the APB has eight subcommittees, including a subcommittee on Identification Services. This subcommittee addresses issues pertaining to fingerprint identification and criminal justice use of Criminal History Record Information, and is

REDACTED – FOR PUBLIC RELEASE

responsible for all projects related to the FBI's fingerprint identification program. Through the use of the APB, CJIS has provided a formal avenue for IAFIS users to discuss desired changes or relevant issues.

Conclusion

Automation combined with trained personnel, efficient tracking mechanisms, and significant interaction with customers have enabled the FBI to process millions of fingerprint submissions per year in a generally timely and accurate manner. CJIS has exceeded the system performance metric for timeliness established for both civil and criminal 10-print processes, and the major customers interviewed were satisfied with CJIS's performance. In addition, CJIS seeks customers' input for new technology and proactively enhances the current technology to increase automation as much as possible. In this vein, CJIS initiated the Next Generation Identification (NGI) program, a 10-year, \$1 billion effort to enhance and expand its biometric identification services.

We made two recommendations to enhance the FBI's fingerprint identification. First, we believe the FBI should include as part of its business plan a process for reassessing its fee structure every 2 years to ensure proper cost recovery and future automation. Second, while procedures for changing AFIS were generally understood, CJIS should develop and implement written policies or procedures for documenting and approving changes to AFIS.

Recommendations

We recommend that the FBI:

20. Include as part of its business planning a process for reassessing its fee structure every 2 years to ensure proper cost recovery and future automation.
21. Develop and implement written policies and procedures for documenting and approving adjustments to AFIS.

EXHIBIT 97

EVALUATION OF THE ACCURACY OF E-VERIFY FINDINGS

July 2012

Report Submitted to:

U.S. Department of Homeland Security
Washington, DC

Prepared by:

Westat
Rockville, Maryland

CONTENTS

<u>Chapter</u>		<u>Page</u>
	EXECUTIVE SUMMARY	ix
I.	INTRODUCTION.....	1
	1. Evaluation Goals.....	1
	2. The E-Verify Process.....	2
	2.1. Overview of the E-Verify Process	2
	2.2. Matching Process.....	6
	2.3. Resolution Process.....	6
	3. Overview of Databases Used in E-Verify	8
	3.1. Databases Used in Automatic Searches	8
	3.2. Systems/Databases Used in USCIS Second- and Third-Level Reviews.....	10
II.	METHODOLOGY.....	13
	1. Introduction	13
	2. Data Sources.....	13
	2.1. Interviews With Federal Officials.....	13
	2.2. E-Verify Transaction Data	14
	2.3. Employer Registration Data.....	15
	2.4. System Testing	15
	2.5. Document Reviews	15
	3. Measurement and Data Analysis	15
	3.1. Introduction	15
	3.2. Accuracy	16
	3.3. Case Characteristics.....	16
	3.4. Classification of Names	18
III.	FINDINGS ABOUT E-VERIFY ACCURACY.....	21
	1. Introduction	21
	2. Overall Findings	21
	2.1. Introduction	21
	2.2. Accuracy	22
	2.3. Accuracy and Citizenship Status	23

**CONTENTS
CONTINUED**

<u>Chapter</u>	<u>Page</u>
3.	Accuracy of E-Verify Review Stages 26
3.1.	Introduction 26
3.2.	Automated Review 26
3.3.	USCIS Second-Level Review 36
3.4.	TNC Resolution Process 38
3.5.	Improving Accuracy for Unauthorized Workers..... 44
IV.	FINAL NONCONFIRMATION ACCURACY RATES CHARACTERIZED BY THE REASONS WORKERS WERE NOT AUTOMATICALLY FOUND EMPLOYMENT AUTHORIZED 47
1.	Introduction 47
2.	Tier 1 Cases 48
2.1.	What Types of Cases Account for the Largest Number of Cases in Which Employment- Authorized Workers Received FNCs? 48
2.2.	What Additional Information is Available to Help Decide How to Allocate Resources?..... 49
2.3.	Confirming Employment-Authorization Status of Naturalized Citizens..... 51
2.4.	SSA and USCIS Name Mismatches 53
2.5.	Form I-94 Number Not Found..... 58
3.	Tier 2 Reasons 60
3.1.	Background 60
3.2.	What Types of Cases Have Unusually Low Accuracy Rates? 60
3.3.	Other Measures Affecting Resource Decisions 61
3.4.	Immigration Status Does Not Clearly Indicate if Nonimmigrant is Authorized to Work 62
3.5.	USCIS Date of Birth Only Mismatch Cases 65
3.6.	Employer-Referred Name Mismatch Cases 66
4.	Differences Between Citizens and Noncitizens..... 68
4.1.	Introduction 68
4.2.	Findings..... 68
4.3.	Possible Improvements 70

CONTENTS
CONTINUED

<u>Chapter</u>	<u>Page</u>
V. CONCLUSIONS AND RECOMMENDATIONS.....	71
1. Background	71
1.1. Introduction	71
1.2. Overall Accuracy	72
2. Workers.....	72
3. Employers.....	73
3.1. Worker Notification	73
3.2. Inaccurate Form I-9s	74
3.3. Reviews of Names	74
4. Federal Government.....	75
4.1. Database Accuracy	75
4.2. Other Recommendations to Improve the Accuracy of Automated Reviews.....	78
4.3. Second- and Third-Level Reviews.....	78
5. Future Research	80
Glossary	GL-1
 <u>Appendix</u>	
A The Source and Accuracy of Federal Data Used to Confirm E-Verify Cases.....	A-1
B Steps for Cleaning the Transaction Database.....	B-1
C Measuring Accuracy in <i>Evaluation of the Accuracy of E-Verify Findings</i>	C-1
D Supplemental Tables	D-1

**CONTENTS
CONTINUED**

<u>Exhibit</u>		<u>Page</u>
I-1.	Verification Process for Persons Attesting to Be U.S. Citizens on Form I-9	3
I-2.	Verification Process for Persons Attesting to Be Noncitizens on Form I-9	4
III-1.	Erroneous TNC Trend: July 2004–June 2010.....	22
III-2.	Estimated Employment-Authorization Status of Workers Receiving FNCs: FY 2009	23
III-3.	Erroneous TNC Rates, by Form I-9 Birth/Citizenship Status: FY 2009	24
III-4.	Erroneous TNC Rates, by Attested Citizenship Status: July 2004–June 2010.....	25
III-5.	USCIS Outcomes for Noncitizens With SSA Records Showing Them to Have Permanent Employment Authorization: FY 2009.....	35
III-6.	Accuracy of USCIS Automated Reviews With and Without a Second-Level Review, by Stages in the Automated Checking Process: FY 2009	37
III-7.	SSA Resolved TNC Cases, by Whether Case Was on EV-STAR: FY 2009	42
IV-1.	Reasons for Initial TNCs Being Issued to Employment-Authorized Workers Who Later Received FNCs: FY 2009.....	49
IV-2.	FNC Accuracy Rates for Tier 1 Reasons: FY 2009	50
IV-3.	Estimated Percent of Unauthorized Workers Identified for Tier 1 Cases, by Initial Reason for Not Receiving an Automated Finding of Employment Authorized: FY 2009	51
IV-4.	Characteristics of SSA Name Mismatch Cases Resolved After a TNC: FY 2009	56
IV-5.	Characteristics of USCIS Name Mismatch Cases Resolved After a TNC: FY 2009	57

CONTENTS
CONTINUED

<u>Exhibit</u>		<u>Page</u>
IV-6.	Form I-94 Mismatches, by Whether Form I-94 Number Appears to be an A-Number: FY 2009	59
IV-7.	FNC Accuracy Rates of Tier 2 Cases: FY 2009	61
IV-8.	Percent of FNCs Issued to Employment-Authorized Workers and Percent of FNCs Issued to Unauthorized Workers Accounted for by Tier 2 Reasons: FY 2009	62
IV-9.	Estimated FNC Accuracy Rates for Students, by Industry: FY 2009	63
IV-10.	FNC Accuracy Rates for Exchange Visitors, by Industry: FY 2009.....	64
IV-11.	FNC Accuracy Rates for Date of Birth Mismatch Cases, by Characteristics of Date of Birth Mismatch: FY 2009	66
IV-12	Percent of Cases Referred to E-Verify by Employer for Second-Level Review, by Type of Name Difference: FY 2009.....	67
IV-13.	Components of the Erroneous TNC Rates, by Citizenship Status: FY 2009	69
IV-14.	Erroneous TNC Rates, by Citizenship Status and Type of Name: FY 2009	70

This page intentionally left blank.

APPENDIX A

THE SOURCE AND ACCURACY OF FEDERAL DATA USED TO CONFIRM E-VERIFY CASES

1. INTRODUCTION

The purpose of this appendix is to provide more detailed background information than in the report itself on the accuracy, timeliness, and completeness of the Federal information used in the E-Verify verification process. To do this, it examines how data are initially collected, including the forms used in data collection; how data are input into Federal computer systems; and the procedures for correcting or updating data in the Federal systems.

This appendix discusses the Employment Eligibility Verification Form I-9 which contains the workers' information submitted to E-Verify and describes the Federal data which are compared with I-9 information. It starts with a discussion of information used in verifying the employment eligibility of all workers (Social Security numbers (SSNs)) and then discusses available data for U.S. citizens, and for the two major categories of noncitizens who are authorized to work in the United States: permanent residents and certain categories of nonimmigrants. These descriptions include information on how biographic information (primarily name) is obtained on forms and processed, including processing delays, systems used, how changes and corrections are made, and any relevant comments related to their use in E-Verify.

2. ALL U.S. WORKERS

2.1. Introduction

There are two forms relevant to all U.S. workers that are discussed in this section. First, there is the Form I-9 that all U.S. workers and their employers are required to complete when an employer initially hires workers. The second is the SSN Application, Form SS-5 that all persons, citizen and noncitizen alike, must complete in order to obtain an SSN to work in the United States.

2.2. Employment Eligibility Verification, Form I-9

2.2.1. Form

Employment Eligibility Verification, Form I-9, provides the information on the worker that E-Verify checks against data contained in Federal databases. Therefore, it is important that the I-9 contain information that is clearly presented and likely to be compatible with the Federal data against which it will be checked. If information on the Form I-9 is not clear and accurate it is unlikely that employers can accurately input it into E-Verify and get a successful match with Federal data.

2.2.2. Process

Unlike most Federal forms, the Form I-9 is retained in employer records and not submitted to any government agency. It was originally designed after implementation of employer sanctions legislation in 1986 making it unlawful to knowingly hire or continue to employ unauthorized workers. The I-9 was intended to provide evidence that an employer had taken due diligence in determining that a newly hired employee was authorized to work in the United States.

APPENDIX A

Since the form was originally intended to be completed and filed in employer records it was not designed for data entry. It may, therefore, not be surprising that the I-9 contains no instructions separate from the form itself on how information is to be provided, such as guidance for writing very long, compound, or unusual names.⁸⁷ Workers typically handwrite their last and first names and middle initial in a single box at the top of the form. The space provided is not sufficiently large to handle legible writing of compound names, and because of the design, name segments may run together, making it difficult for employers entering the data into E-Verify to know when a last name ends and a first name begins. Additional instructions are included in the next release of the Form I-9 handbook. The I-9 includes a separate box for maiden name but does not request information on aliases or other names ever used. It further asks for date of birth in month/day/year format, which is ambiguous as to whether the month should be written as a word or a number, which may lead to errors in translating the data into E-Verify, which asks for date of birth in numerical format.

2.2.3. Changes and Corrections of Errors

The E-Verify process includes a pre-Tentative Nonconfirmation (TNC) check which allows employers to determine whether there are any data entry errors in the submission to E-Verify. When employers detect such errors, perhaps in consultation with the worker, the original case is considered an Invalid Query and a new case with the correct information is submitted.

2.2.4. Comments

The Form I-9 is currently undergoing review. As discussed in the body of the report, this provides an opportunity to revise the form, so that, while still working for non-E-Verify employers, it is better suited for use in the automated E-Verify process. One option might be to have a separate Form I-9 for use by E-Verify employers since their requirements are somewhat different by statute and could be more so if some of the recommendations in this report are implemented. This would be parallel to the separate Forms G-845, Verification Requests, for agencies mandated to participate in the Systematic Alien Verification for Entitlements Program (SAVE) and those that are not.

2.3. SSN Cards**2.3.1. Form**

The SSN Application, Form SS-5, is a one-page form used for applying for an original SSN or making a change to record information, primarily when a name or citizenship or immigration status changes. All SSN applications are free of charge. The SS-5 asks for “Name to be Used on Card (first, full middle, and last).” There is also a space for “Full Name at Birth” if the current name is different than name at birth. There is also space for other names used previously on a Social Security Card. The Social Security Administration (SSA) now requires that a person’s legal name be used in the Social Security record; however, until late 2005 SSA allowed SSN records and cards to be in any reasonable name requested by the holder, such as a nickname or middle name, making it likely that many persons have SSN cards with names other than their legal name.

2.3.2. Process

Most U.S. citizens are now enumerated at birth through the Enumeration at Birth program, an SSA program supported by participating State Bureaus of Vital Statistics and hospitals. Citizens not

⁸⁷USCIS is providing more instructions on the Internet and plans to issue more written guidance on names later in 2011.

enumerated at birth and all noncitizens must go in person to an SSA field office to apply for an SSN and submit evidence of name and proof of identity, date of birth, and evidence of U.S. citizenship or immigration status. Noncitizens must provide a current unexpired document issued by Department of Homeland Security (DHS) that shows immigration status and work authorization (unless the applicant can demonstrate a valid nonwork reason why he or she needs an SSN). SSA has required evidence of identity for all applicants and also maintained information on citizenship status of persons issued SSNs since 1978. Since 2002, immigration status has been verified through the USCIS SAVE Program⁸⁸ before a number is issued or a change in immigration or citizenship status is made in SSA records. Data entry into Numident is done by Service Representatives at SSA field offices. Current procedures include printing out the information that will be used for the record creation or update and showing it to the applicant for review and approval prior to submitting the data for SSN issuance and card production.

SSA issues three types of SSN cards: unrestricted cards, cards that are valid for employment only with a DHS Employment Authorization Document (EAD), and nonwork cards. The latter two types of cards are issued only to noncitizens; however, cards can be reissued with fewer restrictions when holders' immigration status changes.⁸⁹

Cards for approved applications are produced centrally and generally issued within 2 weeks of application. However, many changes must be verified with the source that issued the documentation. This means that U.S. citizen information may need to be verified with state vital records offices, which is often done electronically. Although most SAVE referrals are verified immediately with USCIS this check may take up to two weeks and in a few cases much longer. SSA does not require that legal name change documents from courts and marriage certificates be verified.

2.3.3. System

SSA's centralized Numerical Index File, known as Numident, is used in enumeration for SSNs and issuance of SSN cards. Numident, created as an electronic system in the 1970s, contains information on about 465 million persons who have been issued SSNs since 1936, including their SSN, name, date of birth, and place of birth. Numident also includes fields for aliases a person has used, including a maiden name or other name used prior to another type of legal name change.

SSNs are unique identifiers and are only assigned once; they are not recycled after the holder is deceased. Efforts are made to assign only one SSN to an individual over a lifetime except in certain cases of identity theft or witness protection. There is only one Numident record for each assigned SSN.

Numident contains 15 characters each for first and middle name, 20 characters for last name, and 4 characters for suffix. Characters beyond these are truncated in Numident, and the overflow is designated with an asterisk (*). The SSN card, however, allows up to 26 characters on the first line for first name and middle name or initial and another 26 characters on the second line for last name and suffix. Single names are listed in the last name field. Special characters appearing in names such as spaces, hyphens, and apostrophes, are included on SSN cards.

⁸⁸The USCIS SAVE Program is similar to E-Verify in that it verifies immigration status for Federal, state, and local benefit and licensing agencies.

⁸⁹The nonwork SSN card is only issued to noncitizens who need an SSN to receive public benefits. However, since most noncitizens who are not work authorized are also not eligible for most public benefits, these cards are issued infrequently. Noncitizens who are not work authorized but need a number for tax purposes can apply to IRS for an Individual Taxpayer Identification Number (ITIN), which can be used in lieu of an SSN for tax purposes.

APPENDIX A**2.3.4. Changes and Correction of Errors**

When errors are made on SSN cards, the individual must complete another SS-5, indicate the mistake that was made, prove his or her identity, and provide legal documentation of the correct information as well as the old information. Changes to Numident, such as updates to a name or citizenship status, create a new entry in the Numident record but do not overwrite earlier Numident information. As a fraud-prevention effort, only three SSN cards may be issued to an individual in a given year and no more than 10 cards may be issued in a lifetime. Cards to show legal name changes or changes in type of SSN card do not count toward these limits.

2.3.5. Use in E-Verify

E-Verify checks SSA records based on SSN and related biographic information for all cases verified through E-Verify.

2.3.6. Comments

While the initial enumeration process has been found to be highly accurate in GAO and OIG reviews, unreported changes to name and citizenship status result in inaccuracies in some Numident records over time. Although SSA reports that it encourages updates to immigration or citizenship status, some reluctance to do so was observed during ongoing discussions between SSA and USCIS because this change requires additional workload for its field office staff and SSA does not view this as a part of its core mission until the person applies for Social Security benefits. However, SSA has more recently taken steps to encourage reporting of immigration and citizenship status changes along with legal name changes. These changes require an in-person visit by the number holder with official proof of the legal change to be made to the Numident record. SSA has also approved wording in USCIS materials given to new citizens to encourage them to visit SSA to update their citizenship status and any name changes made as a part of the naturalization process.

SSA has been criticized for not having current immigration and citizenship status, and therefore not having reliable data on the employment authorization status of noncitizens. However, because immigration status for some noncitizens changes several times over the course of their stay in the United States, it would be very difficult to keep SSA records correctly updated. To provide a reliable link between SSA and DHS records, use of a common numerical identifier would be required for both agencies. Although all SSA records include an SSN, a majority of DHS records do not.⁹⁰

Delays in issuing original SSN cards to noncitizens due to unavailability of DHS data to verify against in SAVE verifications, may result in delays in the verification of noncitizen workers through E-Verify since an SSN is required to enter cases into E-Verify. This delay may create uncertainty among employers about the employment-authorization status of these workers and result in prohibited practices such as delayed training or reduced pay as if they had received TNCs.

⁹⁰Since many noncitizens in the United States do not have work authorization, the SSN could not become the sole DHS numerical identifier.

3. U.S. CITIZENS

3.1. Introduction

Three documents issued to U.S. citizens which are used to document U.S. citizenship are discussed in this section. The first is the U.S. passport which can be issued to all U.S. citizens, whether native or foreign born. The second is a Certificate of Naturalization issued to naturalized citizens. The third document, the Certificate of Citizenship, is issued to derivative citizens if they apply for it. Neither the Certificate of Naturalization nor the Certificate of Citizenship can be used as proof of U.S. citizenship for I-9 purposes. However, data on naturalized citizens are input into USCIS databases used in E-Verify.

3.2. All U.S. Citizens—U.S. Passports

3.2.1. Forms

Applications for U.S. passports are made using Department of State Form DS-11 for issuance of an original passport or DS-82 for a passport renewal. These forms can be completed manually or online. The adult application fee is \$135 for a new passport and \$110 for a renewal.⁹¹ The DS-11 asks for last name in the top box and first and middle in a box below it. Another question asks if a different name has ever been used (maiden, previous marriage, legal name change) and leaves two spaces for entering such names; applicants are directed to attach additional pages with relevant information if necessary.

The Department of State Foreign Affairs Manual includes a detailed appendix of over 30 pages on names to be used in passports, including how to handle many forms of unusual names (such as names that are one word, hyphenated, or numbers); errors in names, names after marriage, divorce, or adoption; special instructions for Slavic, Asian, Arabic, and Hispanic names; and names that are too long for the passport data page. The name used on the passport is normally the name on the document that serves as evidence of citizenship and identity (and the one that best identifies the applicant) unless the name has been legally changed.

The name on the passport does not have to be identical to the identity document as long as the name refers reasonably to the same person – i.e., there could be initials versus spelled out names or shorter versions of a name. Additionally, an applicant can change the spelling of his or her name if it is pronounced the same (Smith and Smyth) or change the order of names (Samuel Thomas to Thomas Samuel). A person with multiple names may also drop a name on his or her passport. Further, a passport may be issued in a nickname as long as it is a common derivative of the given name (Bob for Robert.) A person may also translate a foreign name (Giuseppe to Joseph).

3.2.2. Process

First-time applicants and children under age 16 must apply for a passport in person before a designated court or post office official, at a domestic U.S. passport office, or at an overseas consular post. Renewals may be submitted by mail to a centralized facility. Applications are usually processed at one of three passport processing centers, and passports are produced at two passport production centers. Contract staff enter data passport information. Each passport is issued with a unique passport number.

⁹¹A Passport Card can also be used for I-9 purposes. This card can be used only for land and sea travel between the United States and Mexico, Canada, Bermuda, and the Caribbean, costs \$55 for first time holders or \$30 for holders of a U.S. passport.

APPENDIX A

As of April 2011, the Passport Office advised it was taking 4 to 6 weeks to issue a passport. With expedited service, available for an additional \$60, issuance was taking only 2 to 3 weeks.

3.2.3. System

U.S. passport data are processed in the Consular Affairs Passport Information Electronic Records System (PIERS).

3.2.4. Changes or Correction of Errors

The Passport Agency has extensive instructions for correcting errors or making changes to update information in a U.S. passport. Changes and corrections are requested using Form DS-5504. Printing errors can be corrected free of charge at any time while the passport is valid. Name changes are also free of charge for the first year in which the passport is valid. After one year, changes must be requested on Form DS-82 by renewing the passport and paying the full passport renewal fee.

3.2.5. Use in E-Verify

Passport data accessed through Customs and Border Protection 's (CBP) access to the Department of State' s Consular Consolidated Database (CCD) have been part of the automated E-Verify check since 2009 for persons presenting U.S. passports as proof of identity and employment authorization in the I-9 verification process.

3.2.6. Comments

Use of variants of given names, including different spellings, use of middle names or nicknames, reversed names, or translated names, may affect the likelihood of a mismatch with I-9 data in E-Verify. If the worker uses his or her legal name on the I-9 and an alternate name on the passport, the opportunity for mismatches will be increased.

The Department of State documents U.S. citizenship at the time of the first U.S. passport application for those persons who derive citizenship and do not have Certificates of Citizenship from USCIS. Acquiring a U.S. passport is both quicker and significantly cheaper than applying for a Certificate of Citizenship, and also provides documentation required for international travel. Therefore, the addition of Department of State passport data to E-Verify checks is likely to be helpful in reducing TNCs during the verification process. However, currently fewer than 10 percent of workers attesting to U.S. citizenship present a U.S. passport in the I-9 process, which reduces the effectiveness of this check.

3.3. Naturalized Citizens—Certificate of Naturalization**3.3.1. Form**

Permanent residents who are at least 18 years of age and meet the qualifications for naturalization can apply to USCIS using a Form N-400. The application fee for the N-400s is \$595 plus an \$85 biometrics fee. The N-400 asks for "current legal name," including boxes for family name (last name), given name (first name), and full middle name (if applicable). It also asks for the same names exactly as they appear on the Permanent Resident Card. There is also a question asking for any other names ever used with separate boxes for family (last), given (first), and middle names, and space for three additional names. A fourth question asks if the applicant wants to legally change his or her name during the naturalization process. If yes, there are boxes for the new name, including family name (last name), given name (first

name), and full middle name. The N-400 also asks for USCIS A-number and SSN, although SSN has not always been a required data element.

3.3.2. Process

Since January 22, 2009,⁹² most N-400s are sent to a USCIS Lockbox location for initial data entry and fee collection. Accuracy of scanned data input at the Lockbox is reviewed by contract staff for critical elements, which includes name and date of birth. Data fields that cannot be read during Lockbox data entry are sent to data correction where the case file is reviewed to determine the required accurate information. After the Lockbox processes are completed, the hard copy application is mailed to the USCIS National Benefits Center (NBC) where an application number is assigned and the application combined with the relevant A-file. This material is then sent to the appropriate field office for processing, interviewing, and bestowing U.S. citizenship either administratively by USCIS or by a court.

According to the USCIS website, the processing time for N-400s is 5 months in most offices, but a few offices are taking 7 months or more to complete naturalization cases.

3.3.3. System

Naturalization cases are processed in the centralized Computer-Linked Application Information Management System 4 (CLAIMS4),⁹³ a case tracking system that facilitates processing of applications for naturalization from the time of application through final decision making and acquisition of U.S. citizenship. CLAIMS4 citizenship data go back to the late 1990s and include former A-number and SSN; matches can also be made on the basis of name, date of birth, and nationality or place of birth. CLAIMS4 has a 66-character limit for name—18 each for first and middle name and 30 characters for last name. The system truncates any excess letters. Hyphens, other symbols, and punctuation are not allowed.

3.3.4. Use in E-Verify

CLAIMS4 information is checked in the E-Verify automated process.

3.3.5. Changes and Correction of Data

A naturalized citizen may apply to USCIS for a new Naturalization Certificate by filing Form N-565 with a \$345 filing fee and submitting the original document and proof of the new name, such as a marriage certificate or court order. Two of the four USCIS Service Centers process these applications.

3.3.6. Comments

Use of CLAIMS4, the Redesigned Naturalization Automated Casework System (RNACS), a district-run local naturalization system, used prior to 1996, and the Central Index System (CIS) to verify that noncitizen workers have become U.S. citizens as reported on the Form I-9 when SSA data have not been updated to reflect this new status, has reduced issuance of TNCs to U.S. citizens. However, these systems

⁹²Prior to that time, they were sent to the four service centers for pre-processing before going to field offices. In the past, smaller offices used the Redesigned Naturalization Automated Casework System (RNACS) instead of CLAIMS4.

⁹³Prior to implementation of CLAIMS4, RNACS, a district-run local naturalization system, was used to track naturalization applications from 1986 to 1996. RNACS data, like CLAIMS4, are automatically checked by E-Verify when a worker claiming to be a U.S. citizen on the Form I-9 does not appear as a U.S. citizen or have Numident information showing that the worker has permanent employment-authorization status. RNACS includes older naturalization data than CLAIMS4 and also includes data for some USCIS offices where CLAIMS4 was not initially implemented. It includes new citizens' former A-numbers but not their SSNs.

APPENDIX A

do not always include SSN, and A-number is not collected for persons attesting to U.S. citizenship on the Form I-9. These factors reduce the likelihood of a match. Additionally, these databases do not include data on persons who naturalized before the mid- 1990s or persons who derive U.S. citizenship.

3.4. Derivative U.S. Citizens—Certificate of Citizenship**3.4.1. Form**

When one or more parents of permanent resident children under the age of 18 naturalize, their children normally derive U.S. citizenship. An application for a Certificate of Citizenship for these citizens can be made at any time on a USCIS Form N-600. The filing fee is \$600.⁹⁴ Application for a Certificate of Citizenship also can be made by certain other persons alleging that they are U.S. citizens at birth abroad by virtue of their parentage, or by parents alleging that their adopted or other children automatically became U.S. citizens upon establishing residence as permanent residents in the United States.

3.4.2. Process

Applications for Certificates of Citizenship are sent to and processed manually in local USCIS field offices. According to the USCIS website, the processing time for N-600s is 5 months in most offices, but a few offices are taking 10 months to over one year.

3.4.3. Changes and Corrections of Data

A derivative citizen who has been issued a Certificate of Citizenship may apply to USCIS for a new Certificate of Citizenship by filing Form N-565 with a \$345 filing fee and submitting the original document and proof of the new name, such as a marriage certificate or court order. Two of the four Service Centers process these applications.

3.4.4. System

Derivative citizenship information is not routinely entered into an automated system.

3.4.5. Use in E-Verify

Data are not readily available for use in E-Verify; these citizens may be verified through the passport check if their passport number is available.

3.4.6. Comments

Most persons who derive citizenship do not apply for Certificates of Citizenship, and when they do, cases are manually processed in local offices and the U.S. citizenship status is not normally entered into an automated system. In those cases the only record of issuance of the certificate is in the person's A-file, which requires a manual search during a second or third stage E-Verify review. There is no proof of U.S. citizenship in the A-files of persons not applying for a Certificate of Citizenship. In the case of an individual deriving citizenship through birth abroad to U.S. parents, if no application for a Certificate of Citizenship is made, USCIS will have no file on the individual and no record of the individual's citizenship.

⁹⁴The filing fee is \$550 if the N-600 is filed on behalf of an adopted minor child.

Because of the lower cost and expediency, the Department of State documents U.S. citizenship at the time of the first U.S. passport application for a majority of persons who derived citizenship and does not request Certificates of Citizenship from USCIS.⁹⁵ Acquiring a U.S. passport is both quicker and significantly cheaper than applying for a Certificate of Citizenship; it also provides the documentation required for international travel. Therefore, the addition of Department of State passport data to E-Verify checks is likely to be helpful in reducing TNCs during the verification process. However, currently less than 10 percent of workers attesting to U.S. citizenship present a U.S. passport in the I-9 process, which reduces the effectiveness of this check.

4. PERMANENT RESIDENTS (IMMIGRANTS)—PERMANENT RESIDENT “GREEN” CARDS

4.1. Introduction

Although immigrants to the United States are normally thought of as coming from other countries with immigrant visas, a slight majority of new immigrants are in the United States in another lawful status⁹⁶ at the time they become permanent residents. USCIS rather than the Department of State processes adjustment of status cases using the same qualifying standards as Department of State. The final outcome of processing for both immigrants arriving with immigrant visas and those adjusting status is a Permanent Resident Card (Form I-551 or “green card”).

This section provides an overview of how new immigrants and data on them are processed. Immigrants from outside the United States go through several steps of visa-related processing at Department of State consular posts and inspection by a CBP officer at a port of entry, with biographic data collected at both stages. Data sharing of basic biographic and case information on newly arriving immigrants has existed between DHS and Department of State for at least a decade to reduce duplicate data entry during the pre- and immediate post-immigration processes for this group. Following approval of adjustment of status at local USCIS offices, case processing for data entry and issuance of the Permanent Resident Card is very similar to that for new immigrant arrivals.

4.2. Forms

Form DC-230 Part 1, Application for Immigrant Visa and Alien Registration, is completed along with subsequent forms during the visa application process and payment of a fee ranging from \$330 to \$720 depending on the type of immigrant visa. The visa application form requests “Family Name, First Name, and Middle Name” on the same full line on the form and provides no instructions for how name is written. A second line asks for “Other Names Used or Aliases (If married woman, give married [SIC] name).” Ultimately, the name used on the final visa application must match the name in the foreign passport.

Applicants for adjustment of status to permanent residence apply to USCIS using a Form I-485, Application to Register Permanent Residence or Adjust Status, and pay a \$985 filing fee plus an \$85

⁹⁵Similarly, it is likely that most U.S. citizens who derived citizenship and received Certificates of Citizenship also apply for U.S. passports at some point.

⁹⁶Noncitizens approved as refugees or asylees are admitted permanently but USCIS issues them time-limited, renewable employment-authorization documents (EADs) upon their application. After one year, refugees and asylees can apply to USCIS using Form I-485 to adjust their status to lawful permanent resident. Data on asylees are initially maintained in the USCIS Refugee, Asylum, and Parole System (RAPS), a case tracking system containing information on affirmative asylum applications submitted to USCIS asylum offices. It also includes referral of asylum cases to EOIR for consideration when USCIS asylum officers are not able to grant relief.

APPENDIX A

biometrics fee. The Form I-485, which asks for “Family Name (Last Name),” “Given Name (First Name),” and “Middle Initial,” provides very short spaces for each name part and provides no additional instructions.

4.3. Process

Processing of new immigrant visa applications is carried out largely at consular posts throughout the world and at the National Visa Center (NVC) in New Hampshire, which does case preprocessing of the visa application for most posts. When preprocessing, data entry of key information and assignment of the A-number⁹⁷ is completed at the NVC, the case is sent to the appropriate consular post for interview of the applicant. Upon approval, the post issues a machine readable immigrant visa (MRIV) and affixes it to the applicant’s foreign passport. The prospective immigrant is given their Immigrant Visa Packet in a sealed envelope to turn over during the CBP port-of-entry inspection process to later be sent for inclusion in the paper A-file as a record of the immigration process. The prospective immigrant has six months to enter the United States once the MRIV has been issued.

When immigrants arrive at a U.S. port of entry they give the Immigrant Visa (IV) packet to the interviewing CBP officer who reviews the material, confirms the immigrant’s identity, and annotates the MRIV contained in the new immigrant’s foreign passport. The MRIV contains the statement “Upon endorsement serves as temporary I-551 evidencing permanent residence for 1 year.” Once the inspecting officer has annotated the MRIV in the foreign passport with the stamp “Processed for I-551 temporary evidence of lawful admission for permanent residence valid until (**date**). Employment authorized”, the new immigrant may use the MRIV and passport as a travel document and documentation in the I-9 process for up to one year. For new immigrants requesting an SSN card during the visa application process, an electronic file will be sent to SSA for creation of SSN cards to be mailed to them without need to visit an SSA office.

The completed IV packet is then mailed to one of two USCIS contract data entry facilities at Service Centers, which typically takes a week but may take over 30 days from some ports. USCIS contract staff then create paper A-files with the IV packet information, using the A-number created by the Department of State,⁹⁸ and prepare the files for data entry. Files are usually data entered within a week of reaching the facility and within two days of reaching the data entry stage. During data entry, electronic Department of State data related to the immigrant visa is called up and updated with arrival data. This creates the local CLAIMS3 LAN record that is subsequently uploaded into Mainframe CLAIMS3 and the Central Index System (CIS). Data on new immigrants may be available in CIS as early as 10 days to two weeks of entry, but in some cases the delay is much longer. This process also initiates production of the Permanent Resident Card that will be centrally produced in Kentucky and sent to the new immigrant. USCIS guidelines require the legal name to be used on the Permanent Resident Card. A percentage of the files undergo one or both of the following quality control checks: contractor quality assurance review of staff work and USCIS quality control file review. USCIS does acceptance sampling on completed work, and the contractor is required to have at least 99 percent accuracy on critical data, which includes name, date of birth, and A-number.

Applicants for adjustment to permanent resident status send their Forms I-485 to a contract Lockbox location or one of the USCIS Service Centers where initial data entry occurs through contract support.⁹⁹ Accuracy of scanned data input is reviewed by contract staff for critical elements, which includes name

⁹⁷Those consular posts that pre-process their own cases enter data and assign A-numbers locally.

⁹⁸The IV packet includes a strip of tear-away stickers showing the A-number and associated barcode.

⁹⁹Where the application is sent depends on the class of admission.

and date of birth. Cases processed by the Lockbox are bar coded and files placed in order before they are mailed to the appropriate USCIS field office for interview and adjudication.¹⁰⁰ Adjustment of Status cases are processed using Receipt Number as the unique identifier and also include the immigrant's A-number.¹⁰¹

Once a decision is reached in family-based cases, which is currently taking about four to six months after receipt, field office staff update the CLAIMS3 record through a web process, the Interim Case Management System (ICMS), since USCIS field offices do not have direct onsite access to CLAIMS3. Most employment-based adjustment and humanitarian adjustment cases are adjudicated using CLAIMS3 at one of the four USCIS service centers. The CLAIMS3 data from all adjustment cases are subsequently uploaded from CLAIMS LANs into CLAIMS Mainframe and then into the CIS. This process can take from a few days to a month and a half.¹⁰² This also prompts production of the Permanent Resident Card in Kentucky, which takes another two to four weeks.

Quality control checks are conducted on data scanning and entry at the Lockbox facilities on critical data elements, including name and date of birth. Data fields that cannot be read during Lockbox data entry are sent to data correction where the case is reviewed to determine accurate information. CLAIMS3 also includes edit checks and tables to validate data entered. The contractor is responsible for verifying accuracy of data entered and to correct errors. USCIS staff at each service center conducts random sample audits where they compare data keyed to original form information. Name, A-number, and Receipt Number are among the critical data elements. CLAIMS3 data are backed up daily in case of a system crash.

4.4. Systems

Immigrant visa processing is supported by two Department of State systems, the Immigrant Visa/Diversity Visa Processing Systems (IVIS/DVIS) and the Immigrant Visa Processing (IVO) system, which includes biometrics and prints the machine readable foil visas. Data are also maintained in the CCD.

Adjustment of status processing is supported by CLAIMS3, which is a case management system that was originally designed as a cash register system; it therefore has limited functionality. CLAIMS3 has a 66 character limit for name—18 each for first and middle name and 30 characters for last name. When using the auto fill Form I-485 the system stops accepting typing at these limits. For paper forms entered manually the system truncates any excess letters. Hyphens, other symbols, and punctuation are not allowed.

The CLAIMS3 data for both permanent residents entering with visas and those adjusting status are uploaded into the CIS, a searchable mainframe database containing basic biographic information, historical and current status information, and the location of the paper A-file for permanent residents as well as information on many other noncitizens other than many nonimmigrants.

¹⁰⁰Further data entry and preprocessing in CLAIMS3 is done for family-based cases at the NBC in Missouri before the case is sent to a local USCIS field office for interview and decision.

¹⁰¹The Permanent Resident Card shows both of these numbers.

¹⁰²Based on information provided by the DHS Office of Immigration Statistics in September 2010 related to when statistical data on adjustment of status and overseas-processed immigrants are available.

APPENDIX A

Data for production of the Permanent Resident Card are contained in the Image Storage and Retrieval System (ISRS),¹⁰³ which is a searchable USCIS database that contains digitized biometric information including the signature and photograph used in the production of the Permanent Resident Card.¹⁰⁴ This data runs from 1977 forward but images from before 1988 are reported to often be difficult to read. ISRS is the source of the photograph used in the E-Verify photo matching process for workers presenting a Permanent Resident (“green”) Card during the I-9 verification process. ISRS has the same character limits for names as CLAIMS3 and CIS, and since there is a limit to the number of characters that fit on a permanent resident card, the name may be truncated. For instance, Maria may be abbreviated as “Ma.” If a name is not abbreviated it is truncated once it reaches the record length.

4.5. Changes and Corrections of Data

Biographic errors detected before visa issuance are corrected at the NVC or consular post if the applicant provides official documentation (e.g., a foreign passport) showing the desired correct information. If errors are detected at a port of entry at the time of the immigrant’s arrival in the United States, any changes to the information¹⁰⁵ are made on the visa summary sheet in the packet and initialed by the CBP inspector who must also attach a signed explanatory memorandum explaining the change.

If a Permanent Resident Card is issued with incorrect information because of a USCIS administrative error, a permanent resident can file a Form I-90, Application to Replace Permanent Resident Card, free of charge along with proof of the correct information and the incorrect Form Permanent Resident Card. If the information on the card needs to be changed due to a change in name, for instance, the same process is followed but the resident must pay a filing fee of \$365 plus a biometrics fee of \$85. These requests can often be filed electronically or sent to a Lockbox location where data are entered into the CLAIMS3 system. According to the USCIS website, USCIS is currently taking three and a half months to adjudicate Forms I-90. If immigrants have been in the United States for more than a year, so that the MRIV is no longer valid, they will need to show the receipt for filing the I-90 as temporary proof of employment authorization in the I-9 process if they change jobs before they receive their new card.

4.6. Use in E-Verify

CIS data are checked as part of the automatic E-Verify check, and CLAIMS3 data are checked as part of the second step verification process. As indicated above, the E-Verify photo matching process for persons presenting Permanent Resident Cards during the I-9 process relies on the photograph returned by ISRS that was used to make the original document.

4.7. Comments

CLAIMS3 is available to staff in the four USCIS Service Centers and the NBC but not in the over 50 local USCIS field offices that are responsible for adjudicating adjustment of status cases. Local offices must use a web process, the ICMS, to update CLAIMS3 records about final case decisions. This workaround requires USCIS staff to take separate actions to submit this information that can result in delays in availability of current case information in CLAIMS3. CLAIMS3 data are initially processed within each of the service/benefits centers on CLAIMS3 LANs and then uploaded to the national mainframe CLAIMS3 database and then into the CIS. Although USCIS reports that there are fail safes to

¹⁰³ISRS is now known as the Customer Profile Management System (CPMS.)

¹⁰⁴Current Permanent Resident Cards have a 10-year validity period and although the holder’s status is still valid, cards must be renewed before they expire.

¹⁰⁵Changes described relate to gender, marital status, and mailing address and NOT to name and date of birth.

identify incomplete or failed uploads, when problems occur, delays in availability of current information results, which in turn affects accuracy of E-Verify verifications.

The limit on the number of spaces in CLAIMS3, CIS, and ISRS for name may be insufficient for persons with compound names, particularly when both the first and last names may have two or more parts. Use of abbreviations for names (such as “Ma” for “Maria”) as well as lack of hyphens or other symbols in names may also result in names on the Permanent Resident Card appearing different than names on I-9s and other documentation.

The high cost of changing a name on a Permanent Resident Card is clearly a disincentive for correcting a change in name on a card before it expires, which occurs on a 10-year cycle. This undoubtedly leads to increased erroneous TNCs for permanent residents who have not changed their name with USCIS.

Once USCIS approves adjustment to permanent resident cases, system updates into CLAIMS3 and CIS take from a few days to a month and a half.¹⁰⁶ Although most applicants for adjustment of status have EADs, there may be unnecessary second-level verifications and TNCs in the E-Verify process because CIS records have not been updated.

Although the ISRS photo-match capability is highly accurate, ISRS does not have information on cases where the Permanent Resident Card has been revoked, and therefore could provide incorrect information indicating a card was valid when a noncitizen was no longer in lawful permanent resident status.

5. NONIMMIGRANTS

5.1. Introduction

Nonimmigrants are noncitizens who are admitted to the United States for temporary periods of time and specific purposes. They are divided into a large number of classes of admission depending on the purpose of the visit. Nonimmigrant classes of admission with employment authorization are of primary interest in this appendix.

Nonimmigrants are initially processed for nonimmigrant visas overseas at Department of State consular posts.¹⁰⁷ Foreign nationals apply for a specific type of nonimmigrant visa depending on the purpose of their visit to the United States, and the machine readable nonimmigrant visa (MRNIV) that is affixed to the recipient’s foreign passport includes the class of nonimmigrant admission,¹⁰⁸ the visa validity period (often 10 years), and the number of admissions that the person can make using the visa (often indefinite). Upon arrival at a U.S. port of entry, CBP inspects and admits qualified nonimmigrants for specific periods of time.

Nonimmigrants in many work-authorized categories—primarily those that will work for a specific employer or program—use their I-94 Arrival-Departure Document along with their foreign passport as

¹⁰⁶Based on information provided by the DHS Office of Immigration Statistics in September 2010 related to when statistical data on adjustment of status and overseas-processed immigrants are available.

¹⁰⁷Nonimmigrant visitors for business or pleasure from designated countries may enter the United States without nonimmigrant visas under the Visa Waiver Program; they are not work authorized. There are a number of other exceptions to visa requirements for nonimmigrants, including most Canadians (regardless of their nonimmigrant classification).

¹⁰⁸The DHS Office of Immigration Statistics is the “owner” of all nonimmigrant class of admission codes, which are based on the nonimmigrant classifications in the Immigration and Nationality Act.

APPENDIX A

proof of identity and employment authorization. Other nonimmigrants who either are or may be authorized to work must apply for and be issued an EAD as proof of their employment- authorized status. USCIS regulations at 8 CFR 274a.12 specify which nonimmigrants may use their I-94 and which must apply for an EAD. If nonimmigrants want to change their length of authorized stay in the United States or change to a different nonimmigrant class of admission they must also apply to USCIS and be approved. This section of the appendix discusses each of these topics: I-94s, EADs, and nonimmigrant changes of status or extension of stay.

5.2. Arrival/Departure Documents (I-94s)**5.2.1. Forms**

Before traveling to the United States most nonimmigrants who will be employed must have a valid nonimmigrant visa in their foreign passport. Most nonimmigrant visa applications are now submitted electronically through the Electronic Visa Application Form (EVAF) by the applicant or their representative and are processed by consular officers at posts. Fees range from \$140 to \$390 depending on the class of admission, with most work-related nonimmigrant visas having \$150 fees. The NIV application requests family, first, and middle names in a single box on the hard copy application but has separate boxes for surname (as listed in passport) and first and middle names (as listed in passport) on the EVAF. Examples are given on the electronic form, and a compound surname is used in the example. Instructions are also provided for cases where there is no given name listed in the passport (enter FNU.) Instructions on the NIV application say that surname(s) and given names should be as listed in the passport. It also asks for other names used currently or in the past, including maiden, religious, professional, or any other names. Each nonimmigrant visa is uniquely numbered and the number is available in the CCD.

All nonimmigrants, including those with visas who are authorized to work incident to their nonimmigrant status,¹⁰⁹ complete a CBP Form I-94, with arrival and departure sections, before or upon arrival at a U.S. air or sea port of entry.¹¹⁰ In many cases the I-94 serves as the employment authorization document for nonimmigrants because they are working for a specific employer who has petitioned for their temporary admission and U.S. employment. The I-94 asks for “Family Name” and “First (Given) Name.” There are 19 spaces on the form for family name and 13 spaces for first name. There are no instructions for writing name or on handling hyphenated or compound names.¹¹¹ I-94 numbers are preprinted on the document, and are supposed to be unique, although occasionally carriers print already assigned blocks of numbers. The I-94 also requests nonimmigrants to provide their passport number on the form.

5.2.2. Process

The I-94 may be electronically printed by a carrier (usually an airline), but foreign nationals usually complete it by hand. Although instructions and forms may be printed in many languages in airline brochures or on specially produced forms, the submitted I-94 must be completed in English in the Roman

¹⁰⁹ Only work-authorized nonimmigrants are discussed in this report. This is a group defined by USCIS regulations at 8 CFR 274a.12(a) and (b) that does not need to apply separately for authorization to work or be issued an I-766 Employment Authorization Document because their ability to work is inherent in their nonimmigrant status either because of their status or because their employment is limited to a specific employer or program. This latter group includes nonimmigrant classifications where an employer has petitioned to USCIS and been approved to employ them for a given period of time, such as H, L, O, or P nonimmigrants.

¹¹⁰ Nonimmigrant arrivals at land ports of entry are now captured electronically.

¹¹¹ The Spanish version of the I-94 asks for “apellidos” (last names) in the plural.

alphabet.¹¹² The officer may annotate additional information, such as A-number, occupation and/or petition number, on the reverse side of the I-94 for specified classes of admission.

During the inspection, the CBP officer rubber stamps the I-94 arrival and departure sections and the passport with admission information (port of entry, date, and inspector number) and annotates by hand the nonimmigrant class of admission based on the classification on the nonimmigrant visa and the “date admitted until.” Both are written in a space provided within the admission stamp. Unless the nonimmigrant formally applies and is granted an extension of that period by USCIS, he or she must depart by that date or be in unlawful status.¹¹³ Typically, for workers coming to work for a specific employer or program, the date admitted until for employment-authorized nonimmigrants reflects the petition period, if one exists, plus another 10 days. Nonimmigrants in some categories, notably most F students and J exchange visitors, are given stays for “duration of status” which means they are admitted for a period as long as they continue to comply with the provisions of their temporary nonimmigrant status.¹¹⁴

The arrival portions of Forms I-94 are sent to a dedicated centralized CBP contract data center in Kentucky where they are scanned and data entered into the nonimmigrant portion of TECS.¹¹⁵ The CBP Inspector affixes the departure portion of the I-94 to the nonimmigrant’s foreign passport and upon departure from the United States it is pulled by the carrier and sent to the CBP contractor for data entry and matching with the arrival portion.¹¹⁶

Inspectors at ports of entry are instructed to express mail the arrival portion of the Form I-94 within 24 hours to the CBP contract data entry facility in Kentucky. However, late in the day arrivals, weekends, holidays, and bad weather can result in a several day delay in shipping and arrival of I-94s at the contract data entry site. At one time the contractor matched receipt of I-94 batches with flight arrival schedules to ensure they received I-94s for all flights; according to CBP this is no longer done, so there may be batches of I-94s for entire flights that are not received and keyed. Once received, the contractor processes, scans, and data enters I-94 information into the local system within 72 hours. Upload of nonimmigrant data into the TECS mainframe, which is done on an ongoing basis, takes another day. With this series of steps, there is typically a minimum of a 10 to 14 day delay between the arrival of a nonimmigrant and availability of their information in TECS, and the delay for some I-94s can be much longer. Efforts such as sending electronically scanned I-94s from large airports and use of electronic I-94s for land border arrivals have been made to reduce the delay in availability of some nonimmigrant data. CBP told the evaluation team that it has plans to replace the I-94 system with a totally electronic system during 2013.

To minimize the problem of I-94 data latency in TECS, USCIS began using data available through CBP from the Advanced Passenger Information System (APIS), which provides data on all persons arriving in the United States by air or sea carrier on a real-time basis. APIS information comes from passenger or carrier-input biographic information during ticketing and by law must be sent electronically to the U.S.

¹¹²Illegible, poor, or ambiguous handwriting is the source of a major portion of errors on I-94s.

¹¹³Extensions of nonimmigrant stay are discussed later in this section.

¹¹⁴Data on students and exchange visitors and their dependents are collected, maintained, and managed in SEVIS, maintained by ICE to ensure they are maintaining the lawful status required by their programs. It also contains information on the approval of educational institutions and programs that are authorized to accept these nonimmigrants. There is currently no automated data on employment authorization in SEVIS records, although work is underway to provide them.

¹¹⁵TECS is not an acronym. It originally stood for Treasury Enforcement Communications System, but after moving with the Customs Service in Treasury to CBP in DHS, the system is now “TECS.”

¹¹⁶If an E-Verify verification shows an I-94 number with a departure date, the case is referred to second-level verification since the person has presumably departed the country. The most likely case is that the nonimmigrant has reentered and is using the wrong documentation.

APPENDIX A

port of arrival before a plane is secured for departure or a ship arrives at a U.S. port. CBP inspectors match APIS records to the information in passports during the inspection process. APIS data include a first and last name as well as middle name if available. APIS data has a self-generated number and includes passport number, but does not include A-number, I-94 number, or visa number.

5.2.3. Systems

Information on nonimmigrant visas is maintained in the Nonimmigrant Visa System (NIV) and replicated in the Department of State CCD, a data warehouse that holds current and archived data from many consular systems. It provides near real-time transaction activity on consular domestic and post activity.¹¹⁷

Nonimmigrant arrival and departure information is maintained in the CBP TECS system and contains information on the arrivals and departures of noncitizens admitted to the United States temporarily with visas for specified purposes as nonimmigrants. TECS includes 13 characters for the first name and 19 characters for the last name. Any additional characters are truncated. These limits will be eliminated in the new electronic arrival system, currently scheduled to be implemented during 2013 when the I-94 is phased out.

APIS data are also accessed through CBP to search for nonimmigrant records when they are not yet available in TECS.

5.2.4. Changes and Correction of Data

Accuracy of nonimmigrant visa information is the responsibility of the applicant and consular staff processing the visa. Manual review of the completeness and accuracy of information is conducted when the application is accepted. If an error in name, date of birth, or class of admission is detected during inspection at a U.S. port of entry, the CBP inspector makes the correction. If an error in name, date of birth, class, or period of admission is detected on a Form I-94 based on action taken at the time of arrival, the form and documentation of the correct information can be taken to a designated CBP deferred inspection office for correction without charge. Corrected records do not necessarily replace the earlier records in TECS. Nonimmigrants needing to replace lost, stolen, mutilated, or incorrect I-94s can file a Form I-102 along with a \$330 fee to USCIS. USCIS processing time for I-102s is currently about two and a half months.

If at the time of data entry the I-94 has critical errors such as missing, incomplete, or illogical data, the data cannot be entered into TECS and the record is sent to an “exception file” which is also available in the Verification Information System (VIS) as part of TECS. Certain specified DHS/USCIS employees can make corrections to TECS records, including completing or correcting information in the TECS exception file records, when the current and corrected data are presented to them by MPAs or other DHS staff. Once these corrections are made, the new TECS record is sent back to CPS. The VIS locates the original record and overwrites it with the corrected record, thereby making the system accurate. A similar process has been used to update VIS through CLAIMS3 updates related to changes of nonimmigrant status, extensions of stay, or adjustment to lawful permanent resident; however, the evaluation team was told that USCIS terminated this process in March 2011.

¹¹⁷A portion of these data needed for employment verification can be accessed by MPAs through the Enterprise Service Bus (ESB) using PCQS.

5.2.5. Use in E-Verify

TECS and APIS are both accessed in the E-Verify automated verification process. Limited information on nonimmigrant visa issuance is available from CCD through PCQS for second and third step verifications.

5.2.6. Comments

TECS is the most error prone database accessed by E-Verify, which particularly affects the ability to accurately verify nonimmigrants. The problems are pervasive. Space on I-94s is very tight and handwritten I-94 biographic information and CBP inspector notations on class of admission and date by which the nonimmigrant must depart are often ambiguous or not clearly legible. Data entry staff lack any corroborating documentation to resolve ambiguous data and can easily make errors if what they are viewing is not completely clear. Mistakes in data entry between “l,” “j,” and “i,” and “4,” “7,” and “9,” for instance, are very common. Because of the large volume of I-94s processed annually, errors in even a small percentage of cases results in a significant number of verification-related problems. Further, delays in getting I-94s into TECS result in data not being available for verification through SAVE for issuance of SSNs or for E-Verify verifications. This can result in issuance of erroneous TNCs.

Some of the problem results from the divided responsibility for the post-admission correction of errors between USCIS and CBP. Much of this conflict relates to interagency unwillingness to do the work of the other, but workers get caught in the middle. A final issue worth noting is the lack of instructions or clear process for making I-94 corrections for name changes subsequent to arrival. It is reasonable to believe that, since some nonimmigrants are admitted for several years, name changes due to marriage, divorce, or “Americanization” of names are common.

While APIS data are available on a real-time basis, their promise has not been realized. The evaluation team was told by USCIS staff that data consistency with APIS is not high and that the lack of an I-94 number in APIS requires that a match be attempted on the nonimmigrant’s name and date of birth. CBP officers further told the evaluation team that APIS data are not an accurate source of the most recent information on a noncitizen’s admission. Apparently Arrival/Departure Information System (ADIS) data from the DHS U.S. VISIT Program would be a better source of information for verification of recent noncitizen arrivals. ADIS uses Department of State visa issuance data in CCD that is activated by the swipe of a foreign passport at the time of arrival in the United States, which adds information on time and place of admission to the already data-rich record.

5.3. Employment Authorization Documents (EADs)

5.3.1. Form

Nonimmigrants in certain classes of admission may apply to USCIS for an original, replacement, or renewal EAD using Form I-765 which requires a \$380 filing fee.¹¹⁸ A small space is provided for listing family name (in CAPS), and first and middle name; additional guidance is not provided. The I-765 application form requests the applicant to list any SSN ever used, and any A-Number or I-94 Number issued, although these are not necessarily automated. The EAD shows both the noncitizen’s A-number and the unique receipt number related to the issuance of that card.

¹¹⁸Certain classes of admission, including those for humanitarian purposes, are exempt from the filing fee.

APPENDIX A

EADs (USCIS Form I-766) are issued to several groups of noncitizens, including certain¹¹⁹ noncitizens whose authorization for employment is inherent in their immigration status, and other noncitizens who are in specified immigration classifications that may apply to USCIS for employment authorization. EADs are required as evidence of employment authorization in the second group and may be necessary for some noncitizens in the first group. EADs are usually valid for a period of one or two years and can be renewed if the noncitizen continues to be in an immigration status with employment authorization. The EAD shows the section of the Code of Federal Regulations (starting with 8 CFR 274a.12) under which the noncitizen qualifies for employment authorization in the United States rather than the noncitizen's class of admission.

5.3.2. Process

Most I-765 applications for EADs are initially sent to and data entered at a contract USCIS Lockbox location and then downloaded into CLAIMS3 for processing at one of the four USCIS Service Centers, depending on the immigration status of the applicant. Additionally, many categories of noncitizens are able to file their forms with USCIS electronically.¹²⁰ The EAD application is then adjudicated at one of the four USCIS Service Centers in the local CLAIMS3 LAN. After case completion these data are uploaded into the National CLAIMS3 Mainframe and into the CIS. The CIS information is subsequently downloaded into VIS/CPS on a nightly basis.

EADs are issued through USCIS's ISRS discussed earlier, which includes data from the card as well as the photograph and any biometric data that have been captured during the process.

USCIS processing time for applications for EADs is currently three months, with faster processing for initial applications by applicants for asylum whose cases have not been decided after 150 days; in these cases, the average processing time is currently three weeks. EADs for refugees are supposed to be issued more quickly because the EAD is typically their only form of identification and is needed to apply for other forms of identification such as an SSN, a driver's license, or for public benefits.

5.3.3. Systems

EAD applications are processed in CLAIMS3, and the documents are printed using ISRS, both discussed above. Both of these systems provide 18 characters each for the first and middle names and 30 for the last name on EADs. Because there is a limit to the number of characters that fit on the EAD a name is truncated once it reaches the record length. USCIS guidelines require the permanent resident's legal name to be used on the EAD.

5.3.4. Changes and Correction of Data

The I-765 application is filed to request a replacement EAD if the EAD card was "lost, stolen, mutilated, or contains erroneous information, such as a misspelled name." There is no charge for the replacement if the error on the card was due to a USCIS administrative error. Other changes, such as a name change due to marriage, require that the applicant pay the full \$380 application fee.

¹¹⁹ Pursuant to regulations at 8CFR §274a.12.

¹²⁰ These cases are downloaded directly into CLAIMS3 and routed electronically to the appropriate USCIS Service Center for processing.

5.3.5. Use in E-Verify

The EAD is one of the primary documents USCIS issues as evidence of employment authorization for noncitizens in temporary statuses and serves as evidence of temporary employment authorization in the I-9 and E-Verify employment verification processes. ISRS is checked during the E-Verify automated check and CLAIMS3 during the second-level check. As indicated above, the E-Verify photo matching process for persons presenting EADs during the I-9 process also relies on the ISRS photograph used to make the EAD that E-Verify returns to the employer to match with the photo contained on the EAD.

5.3.6. Comments

The fees for a replacement card would likely serve as a disincentive to request a name change on an EAD until it needed to be renewed. While this would be expected to lead to unnecessary erroneous TNCs, most EADs are replaced on an annual or biannual basis so the period where the name was inaccurate would be relatively short.

The EAD is not evidence of lawful presence since EADs may be issued to some out-of-status noncitizens who are in proceedings before an immigration court or during an appeal of a court's decision. Moreover, although an EAD may have a future expiration date, if the noncitizen is no longer in the status in which he or she was issued the card or another work-authorized status, the noncitizen is no longer authorized to work. In this latter case, an employer could hire a person and assume the person was work authorized based on the EAD and only find out during an E-Verify check that the worker was no longer in an employment-authorized status.

To add further confusion, some noncitizens that are issued EADs, such as refugees and asylees, have permanent employment authorization and can adjust to permanent resident status after one year. In such cases, an expired EAD does not mean that these noncitizens are not work authorized. Noncitizens with work-authorized status that continues past the expiration date on the EAD must reapply for a new EAD and are encouraged to do so in advance of the card's expiration date to avoid having a period when they are without evidence of their continuing permission to work. These noncitizens typically are able to obtain other evidence of identity and work authorization, such as a driver's license and unrestricted Social Security Card, that satisfies I-9 requirements; however, the A-number is still needed in order to verify work-authorized status.

Verifications of EADs are based on Receipt or A-number rather than an I-94 number. Without evidence of a valid EAD and A-number, noncitizens in these categories will not be found to be work authorized by E-Verify even though a matching I-94 exists.

5.4. Change of Nonimmigrant Status and Extension of Nonimmigrant Stay

5.4.1. Form

Nonimmigrants wanting to change status to another nonimmigrant category or to extend the time that they can stay legally in the United States file USCIS Form I-539 and pay a \$290 application fee. The form provides separate spaces for family, first, and middle names. No additional guidance on providing complex types of names is provided.

APPENDIX A**5.4.2. Process**

The I-539 is filed electronically or sent to a Service Center or Lockbox, depending on the nonimmigrant class of admission.¹²¹ Applicants are encouraged to apply at least 45 days in advance of the expiration date of their stay or time when they need to change nonimmigrant status.

Data from the I-539 are usually entered into CLAIMS3¹²² at the Lockbox or Service Center as described for the EAD. The CLAIMS approval notice includes a tear-off section that serves as a replacement Form I-94 showing the new nonimmigrant status and/or extension of stay date. The CLAIMS3 data to extend or change nonimmigrant status update VIS records nightly.

USCIS processing time for Form I-539 applications is currently two and a half months. Since the adjudication is processed in the local CLAIMS3 LAN and uploaded nightly to Mainframe CLAIMS3 and then CIS, the change should be reflected in CIS and VIS within a few days of the decision unless there are problems with uploading data.

5.4.3. System

The I-539 is processed in CLAIMS3, which uses Receipt Number as the numerical identifier. Because CLAIMS3 is event based, it does not consolidate information for individuals who have multiple application records in CLAIMS3. Multiple CLAIMS3 records may be especially likely for nonimmigrants filing Form I-539 who may, for instance, also have applied for an earlier change or extension or an EAD.

5.4.4. Changes and Corrections to Data

Updated information after USCIS approves applications for extensions of nonimmigrant stay or changes from one nonimmigrant class of admission to another in CLAIMS3 is sent to TECS to be appended to the original TECS record. This new information is used to update VIS records nightly. In some cases incorrect information in TECS can also be updated by designated USCIS or DHS officials after the problem is identified and the correction is documented as part of an E-Verify third-step verification process.

5.4.5. Use in E-Verify

CLAIMS3 is accessed during second and third step E-Verify verifications.

¹²¹ Certain diplomats and foreign government and NATO officials file with the Department of State or an international organization.

¹²² The USCIS Adjudicators' Manual states that "If the application is not processed in CLAIMS, the original I-94 must be manually noted on the reverse with the approval date, office three-letter code, and officer stamp number." There is also a notation that a new nonimmigrant visa is required to reenter the United States in the present (new) status.

APPENDIX B.

STEPS FOR CLEANING THE TRANSACTION DATABASE

This appendix describes the approaches used to clean the E-Verify Transaction Database. The main purpose of the cleaning is to identify and delete as many transactions as possible that were entered in error or that are duplicated. It is not always easy to determine which transactions should be removed. For example, the duplicate Social Security numbers (SSNs) for several employers were examined to see if it was reasonable to assume that when two SSNs were transmitted close together in time, they were related to a single case rather than multiple hiring of the same person or of different persons fraudulently using the same SSNs.

To improve the cleaning process, the evaluation team intensively reviewed the cleaning steps described in the last report, examined the records on the initial file to determine whether the rules make sense in terms of what is on the database, and modified the rules as necessary. The most significant modification was to calculate the sequence of various verification events. Although it is not possible to develop a perfect measure that will place all cases in accurate sequential order, the evaluation team believes that applying this measure results in a database that more accurately reflects what is happening to individuals being screened by the E-Verify Program and correctly identifies the cases to be retained.

This process is divided into four sets of actions: (1) preliminary steps, (2) SSN checks, (3) alien number (A-number) checks, and (4) name checks. Each is examined in turn. The flowcharts illustrating the steps are provided following the narrative.

1. PRELIMINARY STEPS

Prior to examining the transaction record, the EV-STAR data were merged with the initial Transaction Database. The preliminary steps involved identifying and deleting the cases that are clearly invalid transactions. The potential sources of invalid transactions included in the initial database were cases closed as invalid queries, records that appear to be identical for a particular case (referred to here as system duplicates), test cases, and cases transmitted using the PC system that preceded the Web Basic Pilot. Exhibit B-1 summarizes the preliminary steps. Of the over 10.5 million records from September 2008 through October 2009 on the initial Transaction Database, 273,925 (2.6 percent) were deleted because the employer closed the case with a closure code of "IQ," indicating it was an invalid query. Another 49,504 (0.5 percent) were deleted because they appeared to be system duplicates; that is, all of the case information and the initiated date were the same. We also deleted one case that appeared to be an "out of date window" case.

Following the preliminary checks, records were examined to determine if they were multiple records transmitted for a single case and, if so, to determine the cause of the duplication and take the necessary corrective action. To be considered two records for a single case, the records had to be matched on one or more of the checks described below (i.e., the SSN check, the A-number check, or the name check). Determining the reason for multiple records for a given case is, however, not straightforward. For instance, there is not an easy way to distinguish between individuals who are rehired by the same employer and employers hiring multiple persons fraudulently using a specific SSN. The evaluation team, therefore, developed and applied a set of rules to use in classifying duplicate records for a case.

APPENDIX B**2. SOCIAL SECURITY NUMBER CHECKS**

Exhibit B-2 indicates the sequence of checks run on the cases with duplicate SSNs. The first check was to identify whether it seems likely that the employer should have closed the case as an invalid query but failed to do so. For example, when an employer submits two nonidentical records on the same day for the same SSN that differ from one another on basic identifying information such as last name, the evaluation team assumes that the case with the earlier event measure should have been closed.¹²³ This step led to the deletion of 51,282 records.

Cases were assumed to be resubmittals of cases that had been referred to the Social Security Administration (SSA) when two records for an employer had the same SSN and hire date, the case with the lower verification number was an SSA Tentative Nonconfirmation (TNC), and the event measure of the lower case number was not more recent than the case with the higher case number. This step led to deletion of 10,016 cases; prior to deletion of a case with these duplicate records, information from the record with the lowest verification number was used to complete the fields describing the initial disposition of the case.

Duplicate records were assumed to be mistaken resubmittals of authorized cases when the duplicate SSN cases from the employer received a system response of authorized. Approximately 197,297 cases were deleted based on this rule.

Duplicate records were assumed to be resolved SSA TNC cases when workers claim to be U.S. citizens and have records on EV-STAR and resolution codes. Based on this rule, 907 cases were deleted.

In addition, duplicate record cases were assumed to be U.S. Citizenship and Immigration Services (USCIS) cases resolved at the third stage when they had a third resolution code indicating that they had been resolved at the third stage. Based on this rule, we deleted 1,088 cases.

3. ALIEN NUMBER CHECKS

Of the 905,492 cases with A-numbers, 1,191 had A-numbers that were clearly made up (e.g., a number consisting only of 9s); these were not subject to cleaning based on A-numbers because they most likely were numbers entered by employers when the correct A-number was not available.¹²⁴ Cases with the remaining A-numbers were examined during a process that was similar to that used for the duplicate SSNs except that it was A-numbers that were checked for possible duplicates. Since the SSN check preceded the A-number check, and since all cases have SSNs and only noncitizen cases have A-numbers, it is not surprising that the duplicate A-number checks resulted in the deletion of fewer cases than the duplicate SSN number checks. Based on the cleaning rules (Exhibit B-3), 2,919 records were deleted because they should have been closed as invalid queries. Another 134 records were deleted because they appeared to be work-authorized cases that had been mistakenly resubmitted, and an additional 21 records were deleted as probable third-stage resolved cases.

4. NAME CHECKS

To perform name checks, all the name fields were changed to upper case and all special characters were deleted to ensure all records had the same name formats and a matching variable was constructed from

¹²³The event measure indicates where the case was in the verification process.

¹²⁴When no A-number was available for a case with an I-94 number, the I-94 number was used instead of the A-number.

the name and birth date of the case. This cleaning routine was primarily designed to identify duplicate records that would not have been identified in the SSN and A-number checks because, for example, the employer realized that an incorrect SSN or A-number had been transmitted and he/she resubmitted the corrected information without closing the original case as an invalid query. Based on the checks (Exhibit B-4), 14,971 records were deleted as cases that should have been coded as invalid queries. In addition, 2,946 cases were deleted because they appeared to be mistaken duplicates, and 24 duplicate records were deleted for cases that appeared to be resolved TNC cases.

5. TOTAL CASES CLEANED

A total of 605,035 (6 percent) were removed during the cleaning process (Exhibit B-5). Of the removed cases, 323,430 (53 percent) were deleted at the preliminary step, 260,590 (43 percent) were removed during SSN checks, and an additional 3 percent were removed during A-number (3,074 cases) or name (17,941 cases) checks.

EXHIBIT 98
FILED UNDER SEAL

EXHIBIT 99
FILED UNDER SEAL

EXHIBIT 100
FILED UNDER SEAL