



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Conclusion

OFO invests in outbound inspections through numerous ongoing outbound operations and infrastructure upgrades. Seizures of \$58 million in currency and 2,306 firearms in FYs 2018 through 2022 demonstrate the value of outbound inspections to CBP's mission. When used consistently, outbound inspections are an effective tool to deter criminal activity by depriving TCOs of resources they need to continue illegal operations. As shown in Table 2, increased frequency of outbound inspections directly correlates to increased seizures. Similarly, a lack of outbound inspections directly correlates to a lack of seizures. Interdiction of narcotics, currency, and weapons disrupts and degrades the ability of TCOs to deliver illicit drugs and profit from them.

Recommendations

Recommendation 1: We recommend the Executive Assistant Commissioner of CBP's Office of Field Operations conduct an analysis of the costs and benefits of outbound inspections and issue a report on the findings to assist the Office of Field Operations in determining whether it should:

- establish an office responsible for outbound inspections, including budget and staffing needs, training, and program metrics;
- establish a minimum frequency of outbound inspections at land border crossings; and
- request more funding for outbound inspections.

Recommendation 2: We recommend the Executive Assistant Commissioner of CBP's Office of Field Operations develop and institute a comprehensive policy for outbound inspections.

Recommendation 3: We recommend the Executive Assistant Commissioner of CBP's Office of Field Operations assess infrastructure, internet connectivity, and technology at each land border crossing and ensure that officers have the necessary resources to conduct outbound inspections and can operate in a safe working environment.

CBP Comments and OIG Analysis

CBP concurred with all three recommendations. In its management response, CBP was pleased that our report acknowledged that outbound inspections are an effective tool to deter criminal activity by depriving TCOs of needed resources. However, CBP expressed concern that we mischaracterized the data delays identified in the report. The delay obtaining the data necessary for this



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

audit was calculated based on the time it took to obtain the requested data, which began on March 23, 2022, when initially requested, to August 15, 2022, when the data was transferred. A copy of CBP's response is in Appendix B. CBP also provided technical comments, and we revised the report as appropriate.

As we noted during the audit, the team appreciates CBP's staff at the POEs and within the LEOD providing vital insight about how outbound inspections affect the TCOs. The cooperation was integral in ensuring the audit team made implementable recommendations.

CBP Response to Recommendation 1: Concur. In early FY 2023, OFO established its Outbound Enforcement Strategy Workgroup, which has already established goals addressing this recommendation and proposed the findings to the Executive Assistant Commissioner of OFO. OFO will establish a dedicated office with outbound oversight focusing on creating a robust outbound posture, dedicated outbound funding string, training unique to each modality, and reportable metrics. Estimated Completion Date (ECD): April 30, 2024.

OIG Analysis of CBP Comments: These actions are responsive to the recommendation, which we consider open and resolved. We will close this recommendation when OFO provides us with a copy of the report provided to the Executive Assistant Commissioner of OFO that details the findings of its analysis of outbound inspections.

CBP Response to Recommendation 2: Concur. OFO's Outbound Enforcement Strategy Workgroup will enhance and unify the outbound policy by updating and consolidating outdated outbound policies and procedures, as appropriate, to produce a comprehensive updated policy. ECD: April 30, 2024.

OIG Analysis of CBP Comments: These actions are responsive to the recommendation, which we consider open and resolved. We will close this recommendation when OFO provides us with a copy of the issued comprehensive outbound inspection policy.

CBP Response to Recommendation 3: Concur. OFO's Outbound Enforcement Strategy Workgroup will complete POE surveys that assess requirements and needs related to infrastructure, internet connectivity, and technology. OFO facilities will also examine current facilities and future facilities and determine efforts needed, as appropriate, to ensure a safe operating environment. ECD: April 30, 2024.



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

OIG Analysis of CBP Comments: These actions are responsive to the recommendation, which we consider open and resolved. We will close this recommendation when OFO provides evidence of assessments completed to evaluate infrastructure and resources available for officers to conduct outbound inspections at land border crossings. OFO should also provide evidence of actions taken to ensure officers have necessary resources to conduct outbound inspections and can operate in a safe working environment.



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

The objective of this audit was to determine the extent to which CBP uses outbound inspections to prevent the illegal exportation of currency, firearms, explosives, ammunition, and narcotics at land POEs. We originally conducted this audit under two separate projects with objectives specific to the Southwest border and the northern border.¹² However, we determined the findings were the same and it was a better use of resources to combine the projects and issue one audit report under the above detailed objective. We focused our audit on personal vehicles and pedestrians. The scope of our audit was FYs 2018 through 2022, allowing us to review pre-pandemic and pandemic conditions.

To answer our objective, we reviewed applicable Federal laws and regulations as well as CBP policies, procedures, and budget information related to the outbound inspection program. In addition, we reviewed DHS OIG and U.S. Government Accountability Office reports, media articles, and congressional testimony.

To learn about CBP's outbound inspection related roles and responsibilities, we obtained relevant documents and interviewed CBP officials from the:

- Facilities Management and Engineering Office
- Field Operations Academy
- Field Operations Facilities Project Management Office
- Land Border Integration Division
- OFO Activity Based Costing and Reimbursable Programs Division
- OFO Fines, Penalties, and Forfeitures Division
- OFO Law Enforcement Operations Division
- OFO Non-Intrusive Inspection Division
- OFO Office of Budget Execution
- OFO Planning, Program Analysis, and Evaluation
- Office of Facilities and Asset Management
- Office of Finance, Budget Directorate
- Office of Professional Responsibility

¹² OIG project numbers 22-034-AUD-CBP, *CBP Searches of Outbound Vehicles at Land Ports of Entry* and 22-059-AUD-CBP, *CBP Outbound Inspections at Land Ports of Entry on the Northern Border*.



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- Policy Directorate, Office of the Commissioner

Further, we contacted CBP officials at eight field offices with oversight of land border crossings we visited. We observed infrastructure and technology at 42 of 47 land border crossings along the Southwest border and 66 of 120 land border crossings on the northern border. We judgmentally selected our sample of site visits based on traffic volume, type of traffic (commercial vs. personal), proximity to other land border crossings, and weather. We interviewed senior POE officials for each of these land border crossings. We also observed outbound inspections at land border crossings that conducted inspections during our visit.

We interviewed officials from the DHS Office of the Chief Financial Officer, Program Analysis and Evaluation Division to obtain an overview of CBP OFO's performance measures related to outbound inspections at the POEs. We also interviewed officials from the General Services Administration to obtain information on its role and involvement with land POEs' operations and infrastructure. Additionally, we met with the Department of the Treasury to learn about CBP's ability to use the TFF.

As part of the audit, we requested data extracts from the TECS system. This system contains temporary and permanent enforcement, inspection, and operational records relevant to the antiterrorism and law enforcement mission of CBP and numerous other Federal agencies it supports. We aggregated data on personal vehicle and pedestrian encounters at POEs on both the Southwest and northern borders. However, due to system limitations we were unable to extract only personal vehicle and pedestrian encounters as needed for our audit because the data provided did not distinguish between commercial and non-commercial (i.e., personally owned) vehicles. Because commercial vehicles were not included in our audit scope, we used alternate means to answer our audit objective.

We received direct access to SEACATS, which contains data on seizures, including currency, firearms, ammunition, explosives, and narcotics seizures at land border crossings along the Southwest and northern borders. We obtained and analyzed SEACATS data for FYs 2018 through 2022, specific to personal vehicles and pedestrians. We reviewed the data and performed limited testing for validity, completeness, and accuracy. Overall, we determined that the data was sufficiently reliable to support our audit conclusions.



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

In planning and performing our audit, we identified the internal control components and underlying internal control principles that were significant to the audit objective. Specifically, we reviewed CBP's control environment, risk assessments, control activities, information and communication methods, and monitoring controls. We identified internal control deficiencies that could adversely affect CBP and its ability to ensure it uses outbound inspections to prevent the illegal exportation of currency, firearms, explosives, ammunition, and narcotics at land POEs. We discussed these identified deficiencies in the body of our report. Because we limited our review to these internal control components and underlying principles our work may not have disclosed all internal control deficiencies that may have existed at the time of our audit.

We conducted this performance audit between March 2022 and May 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG's Access to DHS Information

As part of our audit, we requested complete data extracts from CBP; this took approximately 4 months to acquire. These data extracts included a sampling and full extract on outbound vehicle and pedestrian crossings from TECS for FYs 2018 through 2022. The data provided by CBP was validated through alternate methods, as noted above.



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue, NW
Washington, DC 20229



**U.S. Customs and
Border Protection**

June 29, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Henry A. Moak, Jr.
Senior Component Accountable Official
U.S. Customs and Border Protection

SUBJECT: Management Response to Draft Report: "CBP Outbound
Inspections Disrupt Transnational Criminal Organization
Illicit Operations" (Project No. 22-059-AUD-CBP)

Thank you for the opportunity to comment on this draft report. U.S. Customs and Border Protection (CBP) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

Senior CBP leadership is pleased with OIG's acknowledgement that outbound inspections by CBP's Office of Field Operations (OFO) are an effective tool to deter criminal activity by depriving transnational criminal organizations of resources they need to continue illegal operations. OIG also noted that from fiscal year (FY) 2018 through FY 2022, OFO seized \$58 million in currency and 4,940 firearms. CBP remains committed to protecting the American people and safeguarding our borders, while enhancing the Nation's economic prosperity, to include ensuring the safety and admissibility of goods and people entering the United States.

CBP leadership disagrees, however, with the OIG's misleading characterization of a 117-day delay in receiving data extracts from the TECS system. Due to the huge quantity of data requested pertaining to encounters at both the southwest and northern borders, a considerable amount of time was required to extract the data OIG sought. At no time did CBP intentionally delay providing relevant information or impede the progress of this audit. On the contrary, throughout the audit CBP program officials and subject matter experts worked with the OIG staff to provide all information needed for the audit.

Examples include:

1. While attempting to be responsive to OIG's various requests for information, CBP originally provided a 30-day subset of OIG's larger 5-year request, the receipt of which the OIG had agreed would address its needs; however, the OIG subsequently changed its request for data from FYs 2017-2021 to 2018-2022, further exacerbating the alleged delay in OIG receiving requested information;
2. CBP made available untold numbers of privacy and law enforcement sensitive



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- records, and worked diligently with the OIG to provide broad access to other information, and minimize any delays in accommodating OIG's requests, while adhering to CBP's legal obligations, such as protecting personally identifiable information (PII) associated with vulnerable populations;
3. CBP provided OIG access to one of the largest data extracts CBP has ever produced in response to an audit, which included the data transfer of approximately 269 million records and 62 gigabytes of data; and
 4. CBP provided significant assistance in terms of personnel and time, responding to ongoing, multiple requests for clarification from the OIG audit and data analytics teams regarding the interpretation of the data that CBP made available.

CBP is also concerned with OIG's confusing statements:

“We aggregated data on personal vehicle and pedestrian encounters at POEs [ports of entry] on both the Southwest and northern borders. However, we were unable to extract only personal vehicle and pedestrian encounters, as needed for our audit. As a result, we used alternate means to answer our audit objective.”

These statements unjustly seem to indicate that at some level CBP was at fault for something, but do not specifically say what that might have been. The statements do not provide any operational or system context and, in short, create more questions than answers for “cold readers” of OIG report, thus doing a disservice to all involved with this audit.

Lastly, leadership is concerned that, while the draft report notes OIG reported this “access denial” in its Fall 2022 Semiannual Report to Congress,¹ it does not mention the Secretary of Homeland Security's disagreement with this allegation as documented in the Secretary's letter transmitting this report to Congress. It thus withholds additional important context from “cold readers” of OIG's report.

The draft report contained three recommendations, with which CBP concurs. Enclosed find our detailed response to each recommendation. CBP previously submitted technical comments under separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Enclosure

¹ DHS OIG Semiannual Report to Congress for the Period April 1, 2022 – September 30, 2022, <https://www.oig.dhs.gov/sites/default/files/assets/SAR/2022/oig-sar-apr22-sept22.pdf>



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Enclosure: Management Response to Recommendations
Contained in Project No. 22-059-AUD-CBP**

OIG recommended that the Executive Assistant Commissioner (EAC) of CBP OFO:

Recommendation 1: Conduct a cost-benefit analysis of outbound inspections and issue a report on the findings to assist OFO in determining whether it should:

- a. establish an office responsible for outbound inspections, including budget and staffing needs, training, and program metrics;
- b. establish a minimum frequency of outbound inspections at land border crossings; and
- c. request more funding for outbound inspections.

Response: Concur. In early FY 2023, the EAC of CBP's OFO established an outbound enforcement strategy workgroup, which will lay out an outbound enforcement strategy that encompasses all modalities, to include Air, Sea, General Aviation, Cargo Express Consignment and Passenger for the Southern and Northern borders. The working group already established goals (both long and short-term) addressing this recommendation and proposed the findings to the EAC OFO. OFO will establish a dedicated office with outbound oversight focusing on creating a robust outbound posture, dedicated outbound funding string, training unique to each modality, and reportable metrics. Estimated Completion Date (ECD): April 30, 2024.

Recommendation 2: Develop and institute a comprehensive policy for outbound inspections.

Response: Concur. CBP's OFO Outbound Enforcement Strategy Workgroup will enhance and unify the outbound policy by updating and consolidating outdated outbound policies and procedures, as appropriate, to produce a comprehensive updated policy. ECD: April 30, 2024.

Recommendation 3: Assess infrastructure, internet connectivity, and technology at each land border crossing and ensure that officers have the necessary resources to conduct outbound inspections and can operate in a safe working environment.

Response: Concur. CBP's OFO Outbound Enforcement Strategy Workgroup will complete port of entry surveys that assess requirements and needs related to infrastructure, internet connectivity, and technology. OFO facilities will also examine current facilities and future facilities and determine efforts needed, as appropriate, to ensure a safe operating environment. ECD: April 30, 2024.



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Site Visits, FY 2022 Seizures, and Inspection Frequency

Border	State	Border Crossing	FY 2022 Seizure Cases	Inspection Frequency
SWB	TX	Amistad Dam		
SWB	CA	Andrade		
SWB	TX	Anzalduas (McAllen)		
SWB	TX	Bridge of the Americas (El Paso)		
SWB	TX	Brownsville and Matamoros Bridge (Brownsville)		
SWB	CA	Calexico East		
SWB	CA	Calexico West		
SWB	TX	Colombia Solidarity Bridge (Laredo)		
SWB	NM	Columbus		
SWB	AZ	DeConcini and Morley Gate (Nogales)		
SWB	TX	Del Rio		
SWB	TX	Donna		
SWB	AZ	Douglas		
SWB	TX	Eagle Pass Bridge I		
SWB	TX	Eagle Pass Bridge II		
SWB	TX	Falcon Dam		
SWB	TX	Fort Hancock		
SWB	TX	Gateway to the Americas (Laredo)		
SWB	TX	Gateway International Bridge (Brownsville)		
SWB	TX	Hidalgo		
SWB	TX	Lincoln Juarez Bridge (Laredo)		
SWB	TX	Los Ebanos Ferry		
SWB	TX	Los Indios Free Trade Bridge		
SWB	AZ	Lukeville		
SWB	AZ	Mariposa (Nogales)		
SWB	AZ	Naco		
SWB	CA	Otay Mesa		
SWB	TX	Paso Del Norte Bridge (El Paso)		
SWB	TX	Pharr		
SWB	TX	Presidio		
SWB	TX	Progreso		



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Border	State	Border Crossing	FY 2022 Seizure Cases	Inspection Frequency
SWB	TX	Rio Grande City		
SWB	TX	Roma		
SWB	AZ	San Luis I		
SWB	CA	San Ysidro		
SWB	NM	Santa Teresa		
SWB	TX	Stanton Street Bridge (El Paso)		
SWB	CA	Tecate		
SWB	TX	Tornillo		
SWB	TX	Veterans International Bridge (Brownsville)		
SWB	TX	World Trade Bridge (Laredo)		
SWB	TX	Ysleta		
NB	NY	Alexandria Bay		
NB	MI	Algonac Ferry (Port Huron)		
NB	MI	Ambassador Bridge (Detroit)		
NB	ND	Ambrose		
NB	ND	Antler		
NB	MN	Baudette		
NB	VT	Beebe Plain Station		
NB	VT	Beecher Falls		
NB	MI	Blue Water Bridge (Port Huron)		
NB	ME	Calais		
NB	VT	Canaan Station		
NB	NY	Cannons Corners		
NB	ND	Carbury		
NB	NY	Champlain		
NB	NY	Chateaugay		
NB	VT	Derby Line - I-91		
NB	VT	Derby Line - Route 5		
NB	MI	Detroit - Windsor Tunnel		
NB	ND	Dunseith		
NB	VT	East Richford Station		
NB	ME	Easton Station		
NB	ME	Ferry Point (Calais)		
NB	NY	Fort Covington		
NB	ME	Fort Fairfield		
NB	ME	Fort Kent		



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Border	State	Border Crossing	FY 2022 Seizure Cases	Inspection Frequency
NB	ND	Fortuna		
NB	MN	Grand Portage		
NB	ME	Hamlin Station		
NB	VT	Highgate Springs		
NB	ME	Houlton		
NB	MN	International Falls		
NB	WA	Kenneth G. Ward Port of Entry Lynden		
NB	MN	Lancaster		
NB	NY	Lewiston Bridge (Buffalo)		
NB	ME	Limestone		
NB	NY	Massena		
NB	ME	Milltown (Calais)		
NB	NY	Mooers		
NB	VT	Morses Line Station		
NB	ND	Noonan		
NB	ND	Northgate		
NB	VT	Norton		
NB	NY	Ogdensburg		
NB	ME	Orient Station		
NB	NY	Overtons Corners		
NB	WA	Pacific Highway (Blaine)		
NB	WA	Peace Arch (Blaine)		
NB	NY	Peace Bridge (Buffalo)		
NB	ND	Pembina		
NB	MN	Pinecreek		
NB	VT	Pinnacle Road Station		
NB	ND	Portal		
NB	NY	Rainbow Bridge (Niagara Falls)		
NB	VT	Richford		
NB	MN	Roseau		
NB	NY	Rouses Point		
NB	MI	Sault Sainte Marie		
NB	ND	Sherwood		
NB	WA	Sumas		
NB	MT	Sweetgrass		
NB	NY	Trout River		



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Border	State	Border Crossing	FY 2022 Seizure Cases	Inspection Frequency
NB	ME	Van Buren		
NB	MN	Warroad		
NB	VT	West Berkshire Station		
NB	ND	Westhope		
NB	NY	Whirlpool Bridge (Buffalo)		

Source: POE leadership responses to DHS OIG email and SEACATS FY 2022 seizure data



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D

Office of Audits Major Contributors to This Report

Shelley Howes, Audit Director
Heather Dugan, Audit Manager
Diane Benton, Auditor-in-Charge
Stephanie Wiley, Auditor-in-Charge
Melissa Brown, Auditor
Denis Foley, Auditor
Kierra Pineda, Auditor
Richard Puglisi, Program Analyst
Lindsey Koch, Communications Analyst
Sandra Parsons, Data Services Division Director
Gaven Ehrlich, Supervisory Program Analyst
Azriel Krongauz, Data Scientist
Christopher Stephens, Independent Reference Reviewer



LAW ENFORCEMENT SENSITIVE
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
CBP Component Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

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

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



OIG HOTLINE

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

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

**USCIS Has Generally
Met Statutory
Requirements
to Adjudicate Asylum
Applications from
Paroled Afghan
Evacuees**





OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

August 18, 2023

MEMORANDUM FOR: The Honorable Ur M. Jaddou
Director
U.S. Citizenship and Immigration Services

FROM: Joseph V. Cuffari, Ph.D. **JOSEPH V CUFFARI** Digitally signed by
Inspector General **CUFFARI** JOSEPH V CUFFARI
Date: 2023.08.18
10:24:04 -04'00'

SUBJECT: *USCIS Has Generally Met Statutory Requirements
to Adjudicate Asylum Applications from Paroled Afghan
Evacuees*

Attached for your action is our final report, *USCIS Has Generally Met Statutory Requirements to Adjudicate Asylum Applications from Paroled Afghan Evacuees*. We incorporated the formal comments provided by your office.

The report contains one recommendation aimed at improving asylum application processing for individuals who arrived in the United States under Operation Allies Welcome. Your office concurred with this recommendation. Based on information provided in your response to the draft report, we consider the recommendation open and resolved. Once your office has fully implemented the recommendation, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions.

Please send your response or closure request to
OIGInspectionsFollowup@oig.dhs.gov.

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

Please contact me with any questions, or your staff may contact Thomas Kait, Deputy Inspector General for Inspections and Evaluations, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

USCIS Has Generally Met Statutory Requirements to Adjudicate Asylum Applications from Paroled Afghan Evacuees

August 18, 2023

Why We Did This Inspection

We conducted this inspection to assess USCIS' ability to meet statutory timelines for adjudicating asylum applications from Afghans arriving in the United States under OAW.

What We Recommend

We recommend that USCIS continue to evaluate its operations and ensure consistent compliance with statutory timelines for interviewing asylum applicants from the OAW population.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

In our review of the Department of Homeland Security's preparations to receive and expedite requests from Afghan evacuees for long-term legal status, we found that members of the Operation Allies Welcome (OAW) population had filed only limited numbers of applications for asylum as of May 31, 2022, although they likely remain eligible to apply into 2024.

U.S. Citizenship and Immigration Services (USCIS) has met OAW-specific processing timelines established by the *Afghanistan Supplemental Appropriations Act of 2022* for the majority of applications that have been filed and has adjusted its operations to expedite adjudications. However, a surge of applications over a short period of time may strain USCIS operations given the required processing timelines and the preexisting non-OAW application backlog.

USCIS Response

USCIS concurred with our recommendation. We consider the recommendation resolved and open.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background	3
Overview of USCIS and the Asylum Application Process	4
Results of Inspection.....	5
USCIS Met Processing Timeframes for Most Asylum Applications, but Application Numbers Were Limited and Processing Times Trended Higher through October 2022.....	5
USCIS Has Adjusted Its Operations to Process Applications from the OAW Population	10
A Surge of Asylum Applications May Challenge USCIS' Asylum Operations.....	14
Conclusion.....	14
Recommendation	15
Management Comments and OIG Analysis	15

Appendixes

Appendix A: Objective, Scope, and Methodology	16
Appendix B: USCIS Comments to the Draft Report	18
Appendix C: Office of Inspections and Evaluations Major Contributors to This Report	21
Appendix D: Report Distribution.....	22



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Abbreviations

INA	<i>Immigration and Nationality Act</i>
OAW	Operation Allies Welcome
RAIO	Refugee, Asylum, and International Operations Directorate
SCOPS	Service Center Operations Directorate
TPS	temporary protected status
USCIS	U.S. Citizenship and Immigration Services



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

In August 2021, the Department of Homeland Security was designated to lead and coordinate the Federal Government's Operation Allies Welcome (OAW), to support Afghans resettling in the United States after the collapse of the Afghan central government. Between August 20, 2021, and February 19, 2022, the U.S. Government flew approximately 85,000 Afghan evacuees into the United States.

An estimated 12,000 Afghan evacuees had U.S. citizenship or long-term legal immigration status. The other approximately 73,000 Afghans who arrived under OAW had no immigration status and were paroled into the United States, allowing them to enter and remain in the country. Their parole will remain valid for up to 2 years, provided they comply with the terms of parole.¹ Subsequently, Afghans who resided in the United States as of March 15, 2022, and who were "continuously physically present" in the United States as of May 20, 2022, including those in the OAW population, became eligible to apply for temporary protected status (TPS) under a designation made by the DHS Secretary.² The designation allows eligible Afghans, including those in the OAW population, to apply for TPS until November 20, 2023.³ As discussed below, under DHS rules, members of the OAW population who also apply for and receive TPS will continue to be eligible to apply for asylum beyond the expiration of their 2021 parole.

The OAW population can apply to U.S. Citizenship and Immigration Services (USCIS) for other immigration benefits as appropriate to remain in the United States long term, including asylum.⁴ In addition, some within the OAW population may be eligible for or have obtained long-term legal status through other channels, such as a family-based petition for lawful permanent resident status.

¹ The DHS Secretary "may parole into the United States temporarily under such conditions as he may prescribe only on a case-by-case basis for urgent humanitarian reasons or significant public benefit any alien applying for admission to the United States." See 8 U.S.C. § 1182(d)(5)(A).

² The TPS designation, which was made by the DHS Secretary and was based on "ongoing armed conflict and the extraordinary and temporary conditions" in Afghanistan, allows successful applicants to lawfully reside with employment authorization in the United States for up to 18 months. *Designation of Afghanistan for Temporary Protected Status*, 87 Fed. Reg. 30976 (May 20, 2022).

³ The DHS Secretary must review the designation not later than 60 days prior to its expiration to determine whether the conditions continue to exist and, if so, extend the period of designation. See 8 U.S.C. § 1254a(b)(3)(A).

⁴ Asylum allows an individual to remain in the United States; obtain employment authorization; and, eventually, apply to adjust to lawful permanent resident status.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Our objective was to assess DHS' preparations to receive and expedite requests from Afghan evacuees for long-term legal status, specifically asylum. Our scope included the applications submitted to USCIS by Afghans who were paroled into the United States as part of OAW as of May 31, 2022.

Overview of USCIS and the Asylum Application Process

USCIS oversees lawful immigration to the United States. USCIS adjudicates requests for immigration and citizenship benefits, promotes awareness and understanding of citizenship, and ensures the integrity of the immigration system. USCIS' Refugee, Asylum, and International Operations Directorate (RAIO) adjudicates asylum, refugee, and humanitarian applications.

Asylum offers protection to a non-U.S. citizen who is a refugee, which is defined as someone outside of his or her country:

who is unable or unwilling to return to, and is unable or unwilling to avail himself or herself of the protection of, that country because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.⁵

The asylum process for members of the OAW population is the same as for any other asylum applicant,⁶ except for the required application processing times, which we describe below. To receive asylum, an individual must file a Form I-589, Application for Asylum and for Withholding of Removal. During our fieldwork, the majority of applications were paper based,⁷ with USCIS' Service Center Operations Directorate (SCOPS) receiving these applications, reviewing them for completion, and entering data into a USCIS case management system to initiate automated security checks.⁸ SCOPS then transmitted the application to RAIO's Asylum Division for adjudication.

During the adjudication process, the asylum office schedules an in-person interview with the applicant where the asylum officer will verify information from the application and elicit testimony to determine the applicant's eligibility under asylum criteria. To be eligible for asylum, the applicant has the burden

⁵ 8 U.S.C. § 1101(a)(42).

⁶ This report describes the affirmative asylum process, which is available for individuals who are not in proceedings for removal from the United States.

⁷ As described later, a USCIS official said online filing of the Form I-589 was available for testing purposes during some periods covered by our fieldwork, and it became generally available in November 2022.

⁸ As of May 31, 2023, SCOPS stopped receiving asylum applications. See <https://www.uscis.gov/newsroom/alerts/uscis-changes-filing-location-and-documentation-requirements-for-certain-affirmative-asylum>.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

of proving that he or she is a “refugee”⁹ and that the application was filed within 1 year of arrival in the United States.¹⁰ In the event the application is not filed within 1 year of arrival, the *Immigration and Nationality Act* (INA) requires the applicant to demonstrate “changed circumstances which materially affect the applicant’s eligibility for asylum” or “extraordinary circumstances relating to the delay in filing.”¹¹

After the interview, the asylum officer will complete background and security checks; resolve any pending issues; determine eligibility for asylum, including whether any bars to asylum exist;¹² and write up a case assessment. A supervisory asylum officer will review the assessment for legal sufficiency regarding whether the applicant meets asylum criteria; if the supervisor identifies any insufficiencies in a case that require correction, the supervisor will return the case to the asylum officer. Corrections can include revising the assessment or security checks. In some cases, the supervisor may identify an insufficiency in the interview, and the applicant may need to return to the office for a follow-up interview. The applicant receives their adjudication decision in the mail along with an explanation of the decision’s effect on the applicant’s immigration status and presence in the United States.

Results of Inspection

USCIS Met Processing Timeframes for Most Asylum Applications, but Application Numbers Were Limited and Processing Times Trended Higher through October 2022

Few asylum applications from the OAW population had been filed by May 31, 2022. USCIS met OAW-specific processing timelines for most of these applications from the OAW population, though processing times increased through October 2022. USCIS adjusted its operations to decrease processing times. Although we were unable to determine whether these changes were effective, the introduction of electronic asylum applications for all applicants should improve processing times.

⁹ 8 U.S.C. § 1158(b)(1)(B)(i).

¹⁰ 8 U.S.C. § 1158(a)(2)(B).

¹¹ 8 U.S.C. § 1158(a)(2)(D).

¹² See <https://www.uscis.gov/humanitarian/refugees-and-asylum/asylum/asylum-bars>.



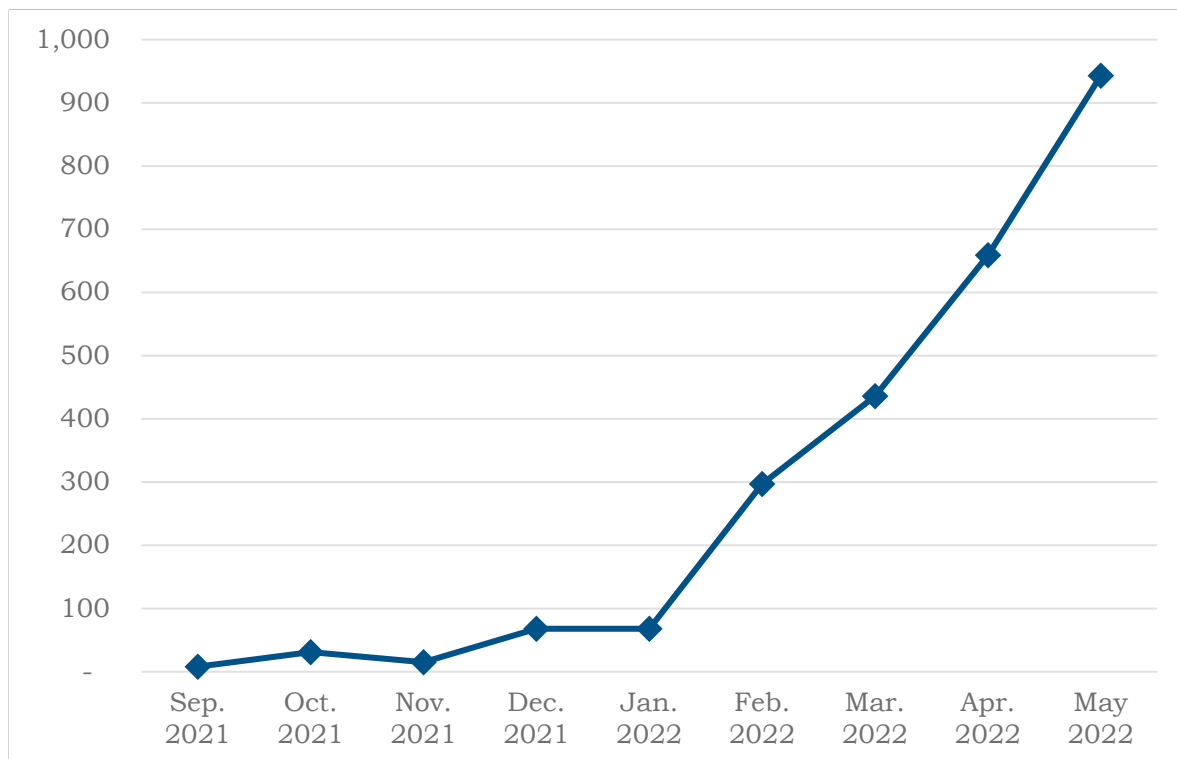
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The OAW Population Filed Limited Numbers of Asylum Applications as of May 2022

As of May 31, 2022, only 2,525 of the approximately 73,000 (or 3.5 percent) people in the OAW population had filed for asylum.¹³ Being a member of the OAW population does not guarantee an application will be granted, though as of June 2023, nearly all OAW applicants had been approved.¹⁴ Figure 1 shows monthly asylum application filing volume through May 2022.

Figure 1. Monthly Asylum Application Filing Volume for the OAW Population (Total 2,525 Applicants)



Source: DHS Office of Inspector General analysis of USCIS data

Under the INA, asylum applicants generally must file within 1 year of arriving in the United States. However, the OAW population's parole and allowances under DHS regulations to apply for asylum within a "reasonable period" after

¹³ As described in our methodology, the number of applicants may be more than the number of applications because family members meeting certain criteria may apply on the same application.

¹⁴ As of June 2023, completed cases had an approval rate greater than 99 percent.

<https://www.uscis.gov/sites/default/files/document/outreach-engagements/AsylumQuarterlyEngagement-FY23Q3Presentation.pdf>



OFFICE OF INSPECTOR GENERAL

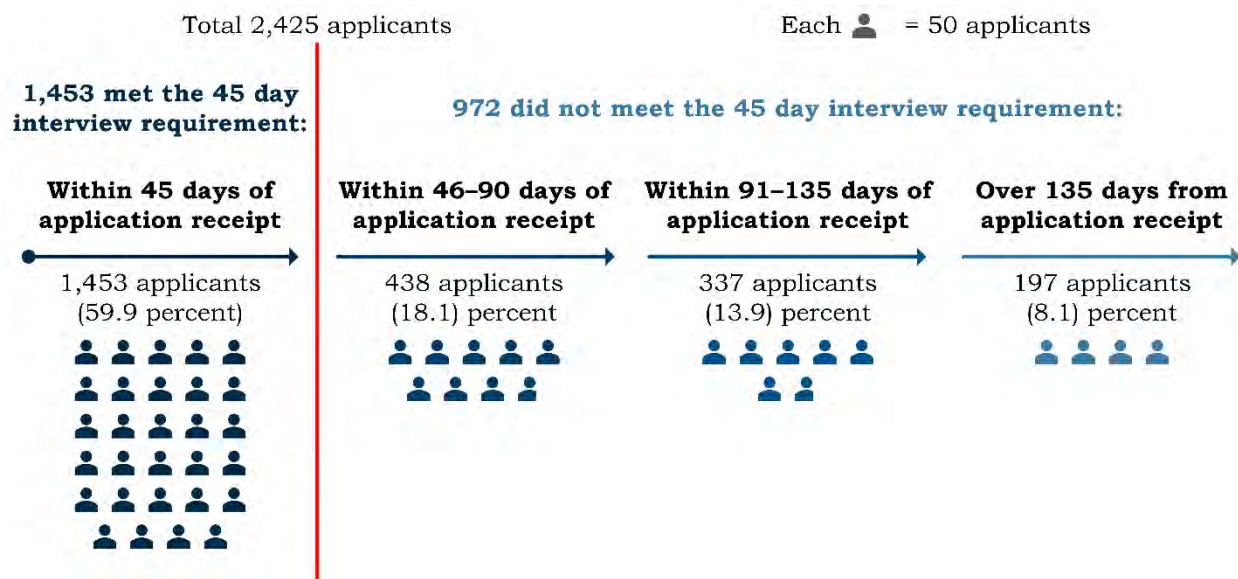
Department of Homeland Security

expiration of parole or TPS¹⁵ make it possible that members of the OAW population who arrived in 2021 will be able to apply for asylum into 2024.

Asylum Application Processing Times Increased through October 2022

The *Afghanistan Supplemental Appropriations Act of 2022*¹⁶ (the Act) requires expedited processing for asylum applications from the OAW population. First, the Act requires USCIS to interview an OAW asylum applicant within 45 days of receipt of the application. For non-OAW asylum applicants, USCIS may schedule interviews beyond 45 days for exceptional circumstances.¹⁷ Out of 2,525 asylum applicants from the OAW population who submitted applications as of May 31, 2022, USCIS completed interviews for 2,425 (or 96 percent), and satisfied the 45-day requirement for 1,453 (or 59.9 percent).

Figure 2. Interview Timeframes for OAW Asylum Applications



Source: DHS Office of Inspector General analysis of USCIS data

Second, the Act requires USCIS to adjudicate asylum applications from the OAW population within 150 days, absent exceptional circumstances. This timeframe is faster than that for non-OAW applicants, which is 180 days, absent exceptional circumstances.¹⁸ Out of the 2,525 asylum applicants from the OAW population who had applied as of May 31, 2022, USCIS completed adjudication for 931 (or 36.9 percent), and satisfied the 150-day requirement for 561 (or 60.3 percent).

¹⁵ See 8 C.F.R. § 208.4(a)(5)(iv).

¹⁶ Pub. L. No. 117-43.

¹⁷ See 8 U.S.C. § 1158(d)(5)(A).

¹⁸ See 8 U.S.C. § 1158(d)(5)(A).

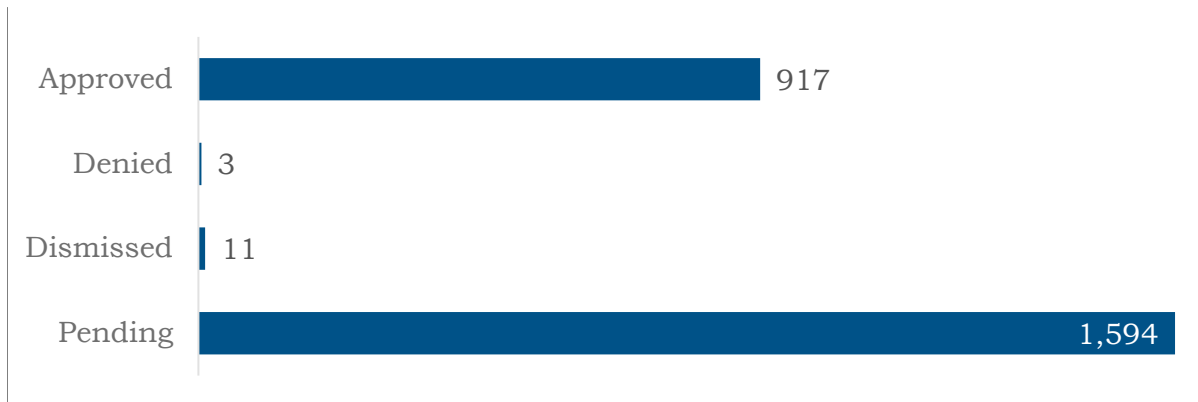


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Given our objective, we did not attempt to assess whether any of the completed adjudications that exceeded the Act's 150-day timeframe presented exceptional circumstances. Figure 3 shows a breakdown of adjudication decisions through October 2022.¹⁹

Figure 3. Adjudication Status for the OAW Population Filed through May 2022
(Total 2,525 Applicants)



Source: DHS OIG analysis of USCIS data

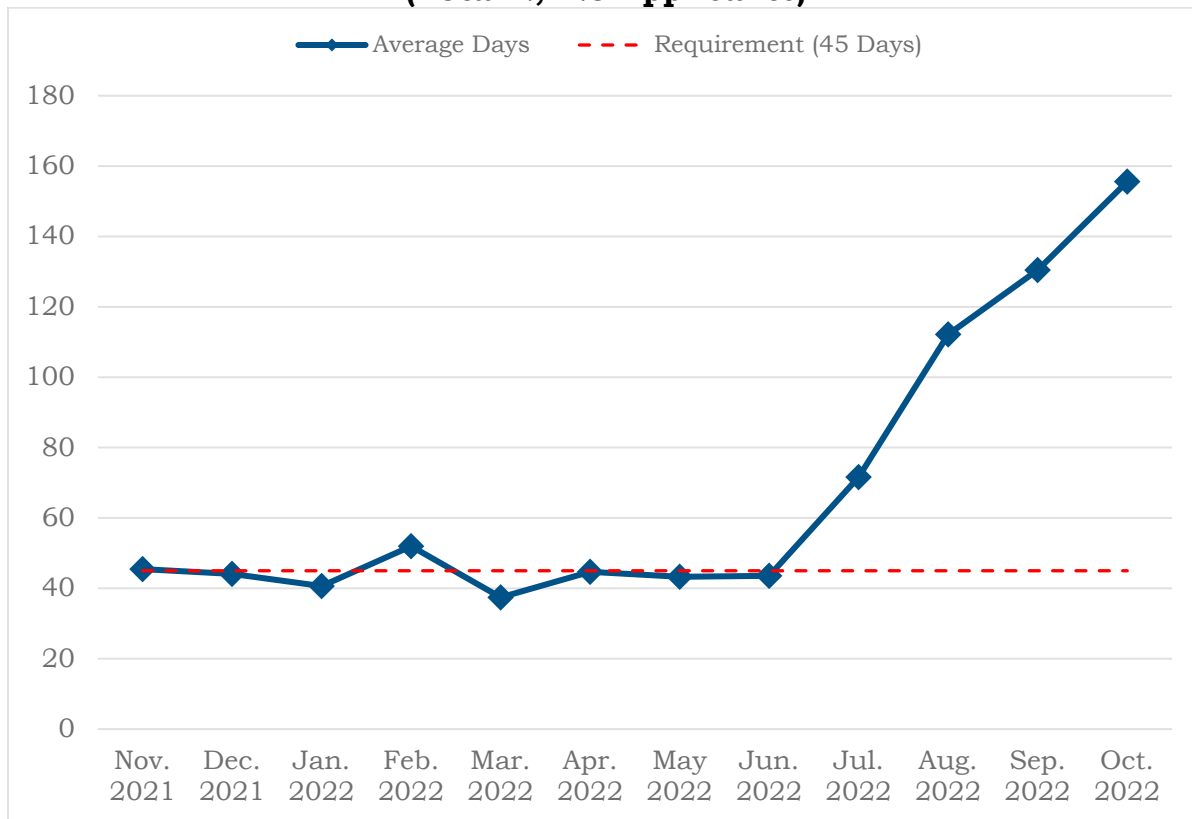
Our analysis showed, however, that processing times are trending higher. As shown in Figure 4, the average time to complete the interview has tripled since June 2022.

¹⁹ An asylum application may be dismissed if the applicant fails to appear for a scheduled interview without prior authorization or fails to comply with fingerprinting requirements without good cause. See 8 C.F.R. § 208.10. An applicant who is not granted asylum but possesses parole, TPS, or another immigration status is considered as being denied. An applicant who is not granted asylum and does not have immigration status may be referred by USCIS to an immigration judge through the issuance of a charging document. See 8 C.F.R. § 208.14.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Figure 4. Average Days from Asylum Application Receipt to Interview
(Total 2,425 Applicants)**



Source: DHS OIG analysis of USCIS data

The delays interviewing applicants followed delays entering application data.²⁰ As shown in Figure 5, average days from receipt by USCIS to file creation in the Asylum Division’s case management system more than tripled between June and October 2022.

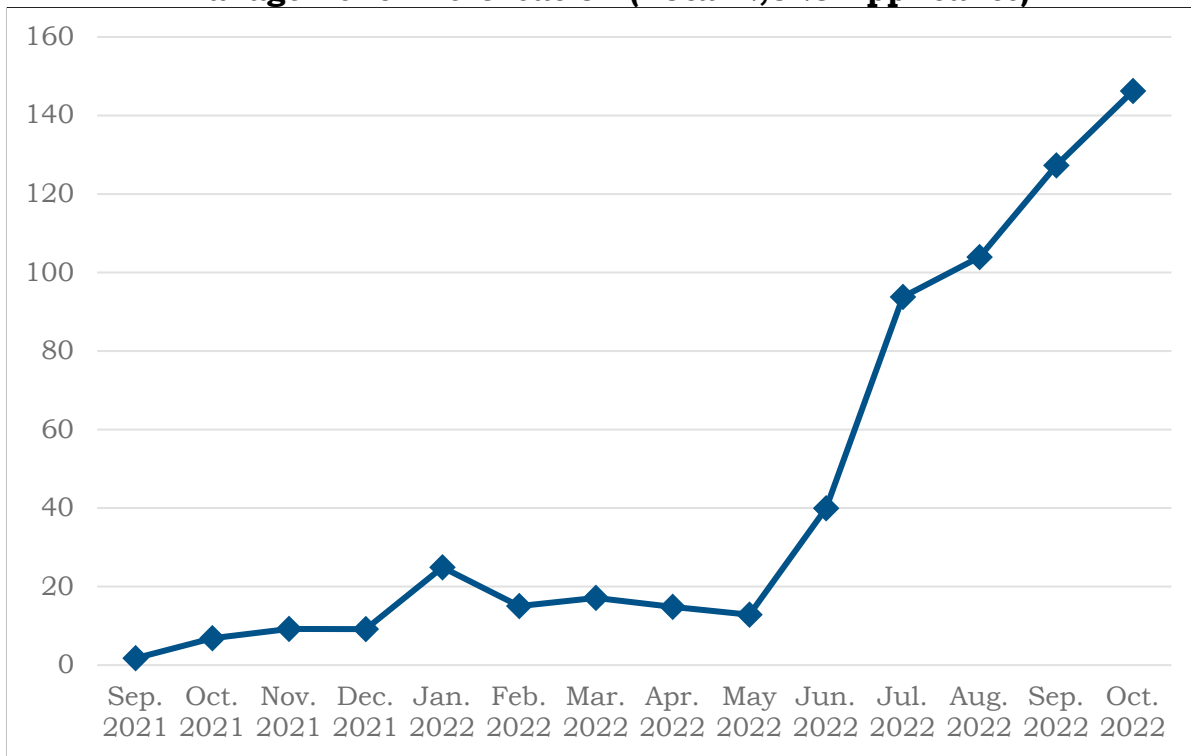
²⁰ As described in our methodology in Appendix A, we continued receiving asylum data through November 2022 for applications submitted as of May 31, 2022.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 5. Average Days from Asylum Application Receipt to Case Management File Creation (Total 2,525 Applicants)



Source: DHS OIG analysis of USCIS data

USCIS Has Adjusted Its Operations to Process Applications from the OAW Population

USCIS adjusted its operations in an effort to decrease processing times. These adjustments cover the entire asylum application process, and they include outreach prior to an application being submitted, application intake, language interpretation, and efforts to enhance workforce efficiency.

USCIS Tailored Outreach to the OAW Population

USCIS increased its introductory outreach to the OAW population to address confusion and limited understanding regarding applying for immigration benefits. Specifically, USCIS identified potential confusion within the OAW population regarding whether applying for asylum affected eligibility for other immigration benefits.²¹ USCIS officials also said some OAW applicants were unprepared to support their claim during their asylum interview. Although asylum applicants within the OAW population are provided expeditious

²¹ A USCIS official told us there was no impact, and individuals can apply for any immigration benefit for which they are eligible.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

processing, they still must support their asylum claim to the same degree as other asylum applicants. Applicants who are unable to support their claim during the interview cannot schedule a follow-up interview to provide additional support, but they may provide supporting information, including a declaration, prior to the asylum officer deciding on the application. If the asylum officer and the supervisor determine the applicant is ineligible for asylum, the applicant will receive a Notice of Intent to Deny. The Notice of Intent to Deny explains the reasons the applicant was found ineligible for asylum and provides the applicant an opportunity to respond, which is known as a rebuttal.

A USCIS official said that on average, an asylum officer adjudicates about two cases per day, but asylum officers have reported that OAW cases generally take longer to adjudicate. The official said this is a logical result of some applicants not being fully prepared to articulate their asylum claim. Another official said OAW cases take longer because some applicants have backgrounds, including military service, that require further elicitation.

USCIS also started performing more introductory outreach to the OAW population. USCIS held outreach sessions with organizations such as resettlement groups that are not typical asylum stakeholders. These engagements attempt to explain how asylum works, in contrast with the more process-focused discussion that typically occurs with traditional stakeholders. Furthermore, USCIS maintains a dedicated webpage²² with detailed information for the OAW population. USCIS officials noted that outreach diverts officers from adjudicating applications.

USCIS Made Adjustments to Application Intake

USCIS has made some process changes to improve the efficiency of receiving and entering applications from the OAW population into its case management system.

Asylum applications are mailed to SCOPS, which enters them into the case management system used by the Asylum Division for adjudication. Originally, USCIS did not request that OAW asylum applicants mark their envelopes to indicate their parole pursuant to OAW when mailing in their applications. Early asylum application envelopes from the OAW population were therefore indistinguishable from general asylum application envelopes. This resulted in OAW-related applications not being appropriately prioritized for data entry upon receipt, despite USCIS attempts to prioritize these applications due to the Act's timelines for conducting interviews. Consequently, the Asylum Division could not initiate adjudication activities more quickly for the OAW population.

²² See <https://www.uscis.gov/humanitarian/information-for-afghan-nationals>.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In response to this challenge, USCIS began instructing OAW applicants to mark their envelopes²³ to indicate their parole pursuant to OAW in an effort to facilitate faster identification and data entry by SCOPS. A USCIS official said exterior marking of envelopes is a method used for other applications as well, and it is helpful because applications are manually reviewed and sorted. However, not all OAW applicants followed the guidance to mark the envelope, and applications that were not marked as OAW would have been processed in timeframes associated with general asylum applications.

Delays in the initiation of OAW application processing were also caused by data entry delays in USCIS service centers. As of November 2022, SCOPS mainly used three service centers — in California, Nebraska, and Texas — to process Form I-589 asylum applications.²⁴ SCOPS' data entry contract requires data entry of non-fee forms, including Form I-589s, within 3 business days. In November 2022, the California and Nebraska service centers were operating with no delays and delays of 30–35 days, respectively. The Texas Service Center had a backlog of 30,000 asylum applications, resulting in a 5-month processing delay. A USCIS official said that although there are occasional delays in processing applications associated with events such as H-1B visa filings, which are accepted during a limited period, this was the first year of pervasive delays. This official said these delays resulted from high application volume and contractor staffing issues. The official said a new contract will be in place in February 2023. As of May 31, 2023, SCOPS no longer received asylum applications.

Although most asylum applications were paper-based, a USCIS official told us some asylum applications were submitted via an online filing option that was in testing during periods covered by our fieldwork and available on a limited basis.²⁵ Another official said these filings were processed quickly relative to paper applications, as they avoided any data entry delays associated with some paper-based applications. USCIS analysis also showed some of the online applications often appeared in the Asylum Division's case management system on the day of submission. In November 2022, online filing of the Form I-589 became generally available.²⁶ Based on processing times in data we reviewed, electronic filing should improve compliance with the Act's 45-day interview

²³ USCIS' website instructs OAW applicants to "mark 'Attn: OAW' anywhere on the front of the envelope." See <https://www.uscis.gov/humanitarian/information-for-afghan-nationals>.

²⁴ An official said the Potomac Service Center performed data entry. However, the service centers do not accept applications directly from applicants. Applicants were instructed to send applications to a specific service center based on their state of residence.

²⁵ We attempted to locate the electronic application during fieldwork but were unsuccessful. We did not confirm the option was available at the time we searched for it.

²⁶ See <https://my.uscis.gov/forms/application-for-asylum-withholding-removal/start/overview> or <https://www.uscis.gov/i-589>.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

requirement. For applicants who filed by May 31, 2022, USCIS has been completing interviews within an average of 30 days from the time the application was entered into the Asylum Division's case management system, indicating it may be able to meet statutory timelines if data entry times decrease.

USCIS Changed Its Practices for Interviews and Language Interpretation

USCIS also made changes to ensure availability of language interpretation services. Under DHS regulations, asylum applicants who are unable to interview in English are required to provide, at no expense to USCIS, interpreters who are fluent in both English and a language the applicant speaks.²⁷ As a result of the COVID-19 pandemic, DHS implemented a temporary final rule in September 2020 requiring applicants to use USCIS-provided interpreters if DHS' language contract covers a language an applicant speaks.²⁸ In September 2021, DHS extended the temporary final rule and added a provision allowing USCIS to accept an applicant-provided interpreter in the event a USCIS-provided interpreter is unavailable. Despite these changes, USCIS officials told us USCIS experienced challenges related to interpreter availability for the languages spoken by OAW applicants. One issue was related to dialect, with the contract providing interpretation for a Pashto dialect different from the dialect more commonly spoken by the OAW population. Based on USCIS analysis provided to us, a lack of interpreters was a cause for delay in approximately 2 percent of applications for which the interview was not held within 45 days. A USCIS official told us that to further address interpreter availability, the Asylum Division has signed its own contract for Pashto and Dari interpretation.

USCIS Made Operational Changes for Workforce Efficiency

Finally, USCIS created materials and conducted training to help its officers streamline the adjudication of many OAW applications. This initiative provided country condition information²⁹ and examples of factual and legal

²⁷ 8 C.F.R. § 208.9(g).

²⁸ *Asylum Interview Interpreter Requirement Modification Due to COVID-19*, 85 Fed. Reg. 59655 (Sept. 23, 2020). The September 2020 temporary final rule's period of amendment lasted 180 days. DHS has implemented multiple extensions, with the current period of amendment running through September 12, 2023, per *Asylum Interview Interpreter Requirement Modification Due to COVID-19*, 88 Fed. Reg. 16372 (Mar. 17, 2023).

²⁹ Country conditions are general conditions of the country from which the applicant is seeking asylum and may include "newspaper articles, affidavits of witness or experts, medical and/or psychological records, doctors' statements, periodicals, journals, books, photographs, official documents, or personal statement or live testimony from witnesses or experts." See I-589, Application for Asylum and for Withholding of Removal Instructions at <https://www.uscis.gov/sites/default/files/document/forms/i-589instr.pdf>.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

determinations specific to Afghans, for example those who worked for the U.S. Government, that an asylum officer can consult when considering asylum claims. The streamlining tool facilitates an asylum officer's establishment of country conditions, thereby relieving some effort by asylum officers for each OAW application.

A Surge of Asylum Applications May Challenge USCIS' Asylum Operations

The Asylum Division may be challenged to meet the Act's required timelines for interviewing and adjudicating asylum applications while still addressing other priorities if it receives a high volume of applications in a short period. Because the vast majority of the OAW population had not yet applied for long-term legal status in the period covered by our fieldwork, there could be a surge of asylum applications as the OAW population's initial period of parole potentially starts to expire in mid-2023.³⁰

Although the Act's deadlines likely require USCIS to prioritize OAW applications, a USCIS official said the Asylum Division also has other priorities. For example, during our fieldwork, Migrant Protection Protocols³¹ were another priority, as were cases where USCIS was subject to a mandamus action.³² In addition, USCIS is currently strained by a 7-year backlog³³ for existing, non-OAW asylum applications, and a surge of OAW applications would amplify the strain on Asylum Division resources.

Conclusion

Members of the OAW population had only filed a limited number of applications for asylum as of May 31, 2022, though they likely remain eligible to apply into 2024. USCIS has met timelines required by the Act for the

³⁰ In May 2023, DHS announced it was developing a process for members of the OAW population to request re-parole. See <https://www.uscis.gov/humanitarian/information-for-afghan-nationals/re-parole-process-for-certain-afghans>.

³¹ DHS created the Migrant Protection Protocols initiative in 2019, which required certain migrants to remain in Mexico for the duration of their U.S. immigration proceedings. In June 2021, DHS issued a memorandum rescinding the initiative. As of December 2022, the rescission effort remained the subject of litigation.

³² Mandamus actions are filed to ask a Federal court to compel the U.S. Government to take action that has been unreasonably delayed (per 28 U.S.C. § 1361). In the context of asylum cases, petitioners would ask the court to compel USCIS to adjudicate their asylum applications.

³³ As of September 30, 2022, USCIS had 605,027 pending asylum cases. Prior OIG work related to USCIS processing challenges can be found in [OIG-22-12, Continued Reliance on Manual Processing Slowed USCIS' Benefits Delivery during the COVID-19 Pandemic](#), and [OIG-18-07, DHS Needs a More Unified Approach to Immigration Enforcement and Administration](#)



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

majority of applications that have been filed, and it has adjusted its operations to expedite adjudications. A surge of applications in a short period of time may nevertheless strain the Asylum Division's operations, given the OAW-specific processing timelines and its preexisting backlog of non-OAW asylum cases.

Recommendation

We recommend that the Associate Directors of Refugee, Asylum, and International Operations and Service Center Operations:

Recommendation 1: Continue to evaluate their operations and ensure consistent compliance with statutory timelines for interviewing asylum applicants from the OAW population.

Management Comments and OIG Analysis

USCIS concurred with our recommendation and described corrective actions it has taken to address the issues identified in this report. Appendix B contains USCIS' management comments in their entirety. We also received technical comments on the draft report and revised the report as appropriate. We consider this recommendation resolved and open. A summary of USCIS' response to our recommendation and our analysis follows.

Recommendation 1: Continue to evaluate their operations and ensure consistent compliance with statutory timelines for interviewing asylum applicants from the OAW population.

USCIS' Response to Recommendation 1: USCIS concurred with the recommendation. It said it will continue to monitor and assess operations to ensure consistent compliance with statutory timelines for the OAW population, while also addressing demand for protection screening interviews at the Southwest Border. It also said it will continue to provide training and is developing tools to streamline interviewing and assessment writing. Finally, USCIS described initiatives it undertook to increase interviewing efficiency for applicants who reside far from an asylum office, as well as to conduct outreach that prepares potential OAW applicants for their asylum interviews and informs them of other immigration benefits. USCIS requested that we consider the recommendation resolved and closed.

OIG Analysis: We consider these actions, as well as those described in our report, such as offering electronic filing, responsive to the recommendation, which is resolved and open. We will close the recommendation upon our review of application processing data showing improvement of processing time trends.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107-296) by amendment to the *Inspector General Act of 1978*.

Our objective was to assess DHS' preparations to provide long-term legal status to paroled Afghan evacuees.

We defined long-term legal status as applying for asylum or lawful permanent resident status based on criteria that existed at the time the person arrived in the United States. Because obtaining a special immigrant visa likely relates to obtaining lawful permanent resident status, we included special immigrant visas in our scope. In the future, members of the OAW population who are granted asylum status will be able to apply to adjust to lawful permanent resident status by filing a Form I-485. These applications cannot be filed until the applicant has been physically present in the United States for at least 1 year after asylum was granted. Because these applications could not have been filed during our fieldwork, they are not within our scope. Similarly, although members of the OAW population may become eligible for long-term legal status through other means (e.g., employment- or family-based adjustments to status), we considered those avenues outside our scope. Although we considered lawful permanent resident status and special immigrant visa status in our scope, this report only discusses asylum applications.

Our evidence collection consisted of interviews with officials from relevant USCIS offices and a review of policies, data, and other documents. Our data analysis considers applications filed through May 31, 2022. For asylum applications, we received updated data as late as November 2022, which we included in our analysis if it related to an application filed by May 31, 2022. Our last special immigrant visa and lawful permanent resident data was collected in June 2022. USCIS provided data from its information systems in addition to its data collection methodology. We performed limited data assurance, generally to assess whether our analysis was accurate, and removed potentially erroneous data from our analysis. For example, although USCIS provided data on 2,532 asylum applicants, we excluded seven applicants where filing dates ended in years 0022 or 0222, likely in the place of 2022. As a result, we used a base of 2,525 applicants. For some analysis, we also removed events with future dates or conflicting information. For example, some applicants had future interview dates, which we interpreted as representing a scheduled but yet to be completed interview. Other applicants had past interview dates, but statuses indicating the interview had not



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

occurred, e.g., pending rescheduling. Based on this assessment, we removed 100 applicants from our analysis of interview timeliness, resulting in a population of 2,425 applicants. Although we performed analysis at the applicant level, a principal applicant may include his or her spouse and unmarried children under 21 who are present in the U.S. on his or her application. As a result, the number of applications from the OAW population is fewer than the number of applicants.

We conducted this review under the authority of the *Inspector General Act of 1978*, 5 U.S.C §§ 401-424, and in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

During this inspection, DHS provided timely responses to DHS OIG's requests for information and did not delay or deny access to information we requested.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
USCIS Comments to the Draft Report

U.S. Department of Homeland Security
U.S. Citizenship and Immigration Services
Office of the Director (MS 2000)
Camp Springs, MD 20588-0009



**U.S. Citizenship
and Immigration
Services**

July 7, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Ur M. Jaddou UR M. JADDOU  Signature of Ur M. Jaddou
20230707 10:18:00 AM
Director
U.S. Citizenship and Immigration Services

SUBJECT: Management Response to Draft Report: "USCIS Has
Generally Met Statutory Requirements to Adjudicate Asylum
Applications from Paroled Afghan Evacuees"
(Project No. 22-021-ISP-USCIS)

Thank you for the opportunity to comment on this draft report. U.S. Citizenship and Immigration Services (USCIS) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

USCIS leadership is pleased to note OIG's positive recognition that during the period of review, USCIS met Operation Allies Welcome (OAW) specific processing timelines established by the Afghanistan Supplemental Appropriations Act of 2022 for the majority of applications that were filed, and has adjusted its operations to expedite adjudications. USCIS also continuously explores ideas to identify solutions for efficient processing as areas of immediate need shift with competing priorities. In addition, USCIS recognizes the importance of continuing to process OAW asylum cases given the Congressionally mandated timelines and to ensure these applicants and their families can have their requests for asylum adjudicated in a timely manner. USCIS intends to continue prioritizing this OAW asylum caseload as much as operationally feasible and evaluating resources, as USCIS also navigates a higher volume of protection screenings at the Southwest Border. When USCIS is not able to timely adjudicate OAW asylum filings, USCIS is ensuring continuity of lawful presence and employment authorization through extending, on a case-by-case-basis, the parole periods of OAW parolee applicants for asylum by two years while their asylum applications are adjudicated.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The OAW Unified Coordination Group, composed of several federal partners, was created to support vulnerable Afghan nationals, including those who worked alongside the United States in Afghanistan for the past two decades, as they safely resettle in the United States. DHS was designated to lead OAW's efforts, and USCIS has played a key role in supporting OAW's critical mission, and has continued its commitment since the transition of OAW into Enduring Welcome. For example, as of June 7, 2023, USCIS received over 17,000 applications for asylum from the OAW population, representing over 33,000 individuals, and completed over 2,900 cases, representing 4,795 individuals. Of the adjudications completed, USCIS granted asylum in over 99 percent of those cases. USCIS also realigned resources to ensure that OAW asylum interviews and decisions are completed in a timely manner, which resulted in increased completion rates at the beginning of Fiscal Year 2023.

The draft report contained one recommendation with which USCIS concurs. Enclosed find our detailed response to the recommendation. USCIS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration.

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

Enclosure



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Enclosure: Management Response to Recommendation Contained in 22-021-ISP-USCIS

OIG recommends that the Associate Director of Refugee, Asylum and International Operations:

Recommendation 1: Continue to monitor and assess operations to ensure consistent compliance with statutory timelines for interviewing asylum applicants from the OAW population.

Response: Concur. USCIS will continue to monitor and assess operations to ensure consistent compliance with statutory timelines for interviewing asylum applicants from the OAW population. USCIS Refugee, Asylum, and International Operations (RAIO), as well as the Office of Performance and Quality, the Chief Financial Officer, and others, regularly monitors and assesses resources by reviewing staffing and receipt levels in order to dedicate staff to interview and adjudicate asylum applications for the OAW population timely, and meet higher demands for protection screening interviews at the Southwest Border. USCIS will also continue to provide training on complex legal and procedural issues and to develop tools to streamline the interview and assessment writing.

USCIS also explored creative ways to conduct interviews for Afghan parolees living far from an asylum office. For example, USCIS established a public-private partnership with Canopy Northwest Arkansas, a resettlement agency located in Fayetteville, Arkansas, to conduct 31 OAW asylum interviews at its location, as federal space was not available in that area. This partnership addressed the lack of federal space, and created efficiencies in interviewing and processing Afghan applicants and their families and saving them the time and cost of traveling 10 hours by car to the New Orleans Asylum Office.

To assist applicants with preparation for their asylum interviews, USCIS RAIO, as well as other USCIS offices, participated in multiple engagement and outreach sessions that communicated important information to potential Afghan applicants, Afghan nationals with pending asylum cases, legal service providers, and other stakeholders. USCIS also created a program with Cherokee Federal¹ to host Afghan Support Centers. This program brings together federal, state, and local organizations that provide assistance and information about the asylum process and other immigration benefits as well as available services to applicants or future applicants.

USCIS requests that the OIG consider this recommendation resolved and closed, as implemented.

¹ Cherokee Federal is a division of Cherokee Nation Businesses, a team of tribally owned federal contracting companies.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix C

Office of Inspections and Evaluations Major Contributors to This Report

John Shiffer, Chief Inspector
Brendan Bacon, Lead Inspector
Anthony Crawford, Senior Intelligence Officer
Rebecca McLain, Senior Inspector
Stephen Farrell, Independent Referencer



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix D

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary for Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
USCIS Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

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

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



OIG Hotline

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

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

CBP Could Do More to Plan for Facilities Along the Southwest Border





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

August 29, 2023

MEMORANDUM FOR: The Honorable Troy A. Miller
Senior Official Performing the Duties of the
Commissioner
U.S. Customs and Border Protection

FROM: Joseph V. Cuffari, Ph.D. **JOSEPH V. CUFFARI** Digitally signed by
Inspector General JOSEPH V CUFFARI
Date: 2023.08.28
17:55:30 -04'00'

SUBJECT: *CBP Could Do More to Plan for Facilities Along the
Southwest Border*

Attached for your action is our final report, *CBP Could Do More to Plan for Facilities Along the Southwest Border*. We incorporated the formal comments provided by your office.

The report contains two recommendations aimed at improving how U.S. Customs and Border Protection (CBP) plans for temporary and permanent facilities along the Southwest border. Your office concurred with both recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 and 2 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

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

Please contact me with any questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

CBP Could Do More to Plan for Facilities Along the Southwest Border

August 29, 2023

Why We Did This Audit

During fiscal year 2022, SWB crossings surged between ports of entry, resulting in more than 2.3 million encounters. The significantly elevated number of encounters strained CBP's resources. We conducted this audit to determine the extent to which CBP assessed and planned its needs for temporary and permanent facilities to process and hold migrants along the SWB.

What We Recommend

We made two recommendations to improve how CBP plans for temporary and permanent facilities along the SWB.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

Since 2019, U.S. Customs and Border Protection (CBP) has improved its response to migrant surges by deploying temporary facilities to increase its capacity to humanely process migrants along the Southwest border (SWB). However, CBP did not always document its planning decisions for both temporary and permanent facilities. Additionally, CBP did not consider alternatives before issuing contracts for temporary facilities. Finally, CBP did not document whether it continually reassessed the need for existing temporary facilities, including the cost-effectiveness of keeping those facilities.

These conditions occurred because CBP prioritized short-term response over long-term planning and does not have a comprehensive policy that incorporates planning for both temporary and permanent facilities. As a result, CBP may be spending money on facilities that are not cost effective and in the best interest of taxpayers. Additionally, CBP may not be well prepared for future migrant surges or for a higher steady state of migrants in custody.

CBP Response

CBP concurred with both recommendations. We consider these recommendations open and resolved.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background 1

Results of Audit 3

 CBP Has Made Progress in Facility Planning, But Additional Work Is Needed
 3

Conclusion..... 10

Recommendations..... 10

Management Comments and OIG Analysis 10

Appendixes

Appendix A: Objective, Scope, and Methodology 12

Appendix B: CBP Comments to the Draft Report..... 14

Appendix C: Comparative Analysis of Average Daily Subjects in Custody
to Sector Holding Capacity..... 16

Appendix D: Report Distribution..... 23

Abbreviations

CBP	U.S. Customs and Border Protection
SWB	Southwest border
U.S.C.	United States Code



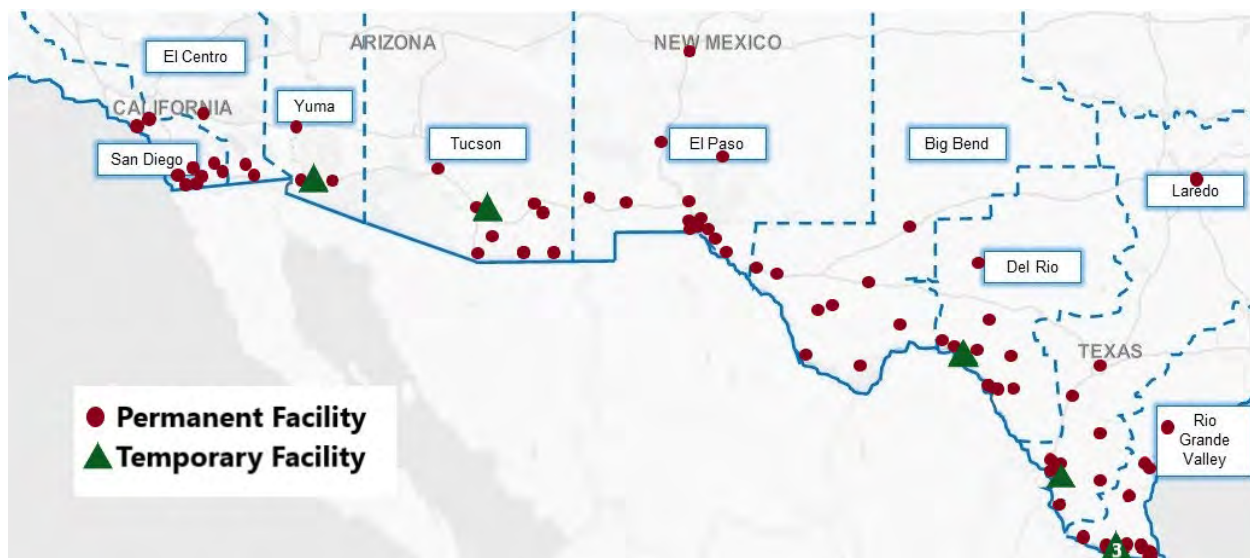
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

U.S. Customs and Border Protection (CBP) maintains 74 permanent facilities along the Southwest border (SWB) for short-term detention of people who are inadmissible to the United States or subject to criminal prosecution (see Figure 1). These facilities are only equipped for short-term detention; after CBP processes detainees, it may repatriate them, release them, or transfer them to other agencies. CBP standards require segregation for different demographics, such as adults, juveniles, family units, and at-risk populations, as well as separation based on gender.

Figure 1. Map of Permanent and Temporary Facilities Along the SWB



Source: Department of Homeland Security Office of Inspector General depiction based on information from CBP. Facility sites will not add up to total due to overlapping on map.

In fiscal year 2019, CBP faced a spike in encounters, an increasing proportion of which involved family units. To address the increased number of migrants and all demographics, CBP awarded contracts for temporary soft-sided facilities to supplement its existing facilities, some of which were over capacity. These temporary facilities are tent-like structures and include equipment necessary to make them livable, such as heating, ventilation, air conditioning, plumbing, electrical, and lighting systems (see Figure 2). From FY 2019 through FY 2022, CBP funded contract task orders totaling more than \$1.27 billion for temporary facilities, which also included support services such as meals, medical care, childcare, and janitorial services. As of June 20, 2022, within CBP's nine sectors along the SWB, U.S. Border Patrol had seven temporary soft-sided



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

facilities: three in the Rio Grande Valley sector, and one in each of the Laredo, Del Rio, Tucson, and Yuma sectors.

Figure 2. Soft-Sided Facility at Laredo, Texas



Source: CBP website as of February 3, 2023

Since 2019, the volume of migrants crossing the SWB has fluctuated. Starting in March 2020, the number of migrants entering the United States decreased significantly after the Centers for Disease Control and Prevention issued a public health order under Title 42¹ of the United States Code (U.S.C.). The order, which was issued in response to the COVID-19 public health emergency, prohibited entry into the United States by certain persons from foreign countries traveling from Canada or Mexico, regardless of their countries of origin. The order was issued to prevent the spread of COVID-19 into land ports of entry and Border Patrol facilities at the borders with Canada and Mexico, or into the interior of the country. During FY 2020, CBP encountered 458,088 migrants,² a 53 percent reduction from the number of encounters in FY 2019. However, in FYs 2021 and 2022, SWB crossings between ports of entry increased to more than 1.7 and 2.3 million encounters, respectively. The significantly elevated number of encounters strained CBP's resources.

In February 2022, DHS issued the *DHS Southwest Border Mass Irregular Migration Contingency Plan*, which outlines the actions DHS components and

¹ 42 U.S.C. § 265 - Suspension of entries and imports from designated places to prevent spread of communicable diseases.

² Encounter numbers include individuals processed under Title 8 and expelled under Title 42.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

their Federal partners should take to humanely prevent and respond to migrant surges across the SWB. The immediate goal of DHS' plan is to create an infrastructure to process migrants quickly, safely, and humanely at the SWB and in the interior. According to the plan, DHS' long-term priorities include developing sustainable capacity and capability. DHS' plan was developed based on lessons learned and best practices the Department collected from 2016 through 2022 to meet current and anticipated migration activities and surges.

To implement DHS' contingency plan, CBP developed the *CBP Integrated SWB Mass Irregular Migration Contingency Plan* (draft, dated February 2022) (CBP's plan). As of August 2023, CBP's plan is still in draft.

We conducted this audit to determine the extent to which CBP assessed and planned its needs for temporary and permanent facilities to process and hold migrants along the SWB.

Results of Audit

Since 2019, CBP improved its response to migrant surges by deploying temporary facilities to increase its capacity to humanely process migrants along the SWB. However, CBP did not always document its planning decisions for both temporary and permanent facilities. Additionally, CBP did not consider alternatives before issuing contracts for temporary facilities. Finally, CBP did not document whether it continually reassessed the need for existing temporary facilities, including the cost-effectiveness of keeping those facilities.

These conditions occurred because CBP prioritized short-term response over long-term planning and does not have a comprehensive policy that incorporates planning for both temporary and permanent facilities. As a result, CBP may be spending money on facilities that are not cost effective and in the best interest of taxpayers. Additionally, CBP may not be well prepared for future migrant surges or for a higher steady state of migrants in custody.

CBP Has Made Progress in Facility Planning, But Additional Work Is Needed

CBP has taken steps to improve its temporary facility planning process by drafting the *CBP Integrated SWB Mass Irregular Migration Contingency Plan*. CBP used lessons learned from prior migrant surges to formulate this plan.

When making informed facility planning decisions, CBP's *Cost-Wise Readiness Guidebook* requires the component to continually evaluate operations to ensure they are as efficient and cost effective as possible. According to the guidebook,



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

CBP defines cost-wise readiness as a strategic framework for establishing and maintaining material readiness at the best cost. Additionally, according to the U.S. Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government*, management should implement control activities through documented policies in the appropriate level of detail to effectively monitor the activity.

However, CBP did not always provide evidence to support whether it documented its decision-making process when planning for facilities. Additionally, CBP did not demonstrate that personnel analyzed alternatives before issuing contracts for temporary facilities or fully analyzed whether continuing to use the temporary facilities was cost effective.

CBP Did Not Always Document Its Facility Planning Decisions

CBP could not provide sufficient documentation to support the decisions it made regarding planning for facilities. The *Federal Records Act of 1950*³ requires agencies to make and preserve records that document the decisions, procedures, and essential transactions of the agency. Additionally, agencies must create and maintain records that document the formulation and execution of their decisions and make the records available for scrutiny by Congress or authorized Government agencies.⁴

Although CBP provided us with documentation it uses to help inform and support its decisions about facility needs, these documents did not show that CBP had examined migration data or conducted cost-benefit analyses to support its facility planning decisions. We determined that CBP collects migration and capacity data but did not document using the data when making decisions about its facilities.

We analyzed 35 months of CBP data from January 2020 through November 2022 on the daily average number of subjects in custody in all nine SWB sectors compared to CBP's holding capacities. We found that three sectors (Del Rio, El Paso, and Yuma) consistently exceeded their holding capacities and six sectors were regularly under their holding capacities. (Appendix C shows the results of our analysis for each of the nine SWB sectors.) For example, the Del Rio sector's average daily number of subjects in custody during this timeframe consistently exceeded its total holding capacity, as shown in Figure 3. Specifically, the Del Rio sector, which has a temporary facility, exceeded its total holding capacity for 13 of the 35 months that we reviewed.

³ 44 U.S.C. § 3101.

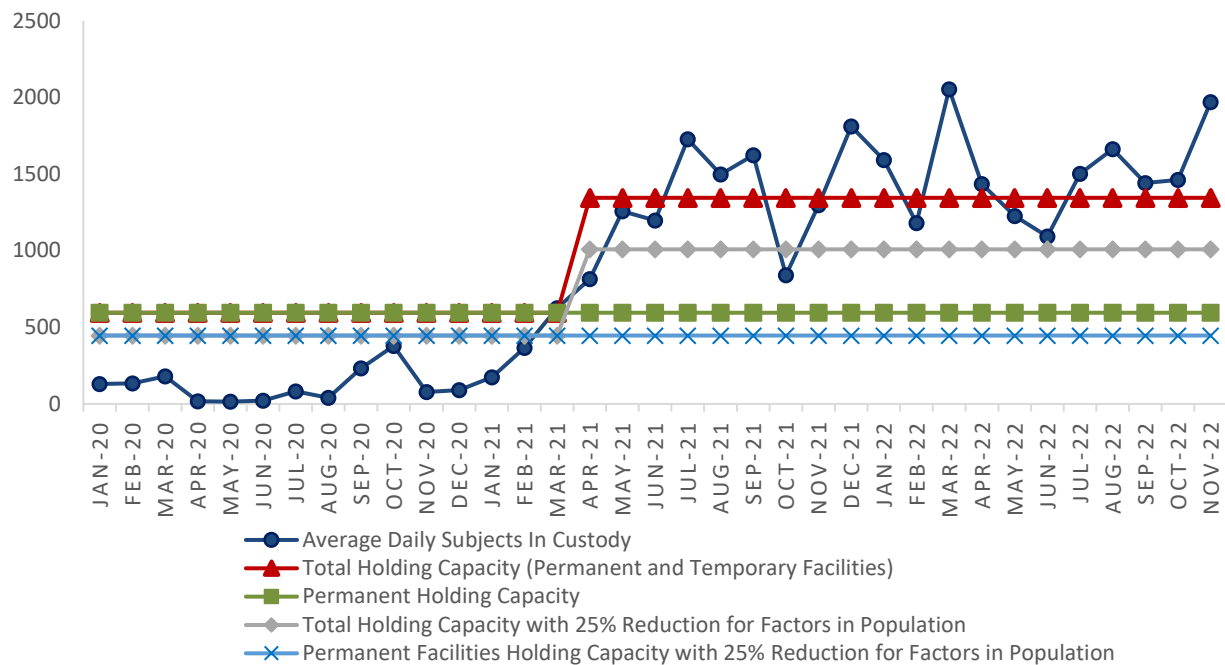
⁴ 36 Code of Federal Regulations § 1222.22; DHS Instruction 141-01-001, *Records and Information Management (Revision 01)*, September 2019.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 3. Comparative Analysis of Del Rio Average Daily Subjects in Custody to the Sector's Holding Capacities⁵



Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily number of subjects in custody from January 2020 through November 2022

Conversely, the Laredo Sector, which has a temporary facility, has regularly been under its permanent holding capacity. As shown in Figure 4, Laredo's average daily number of subjects in custody never exceeded its permanent holding capacity from January 2020 through November 2022.

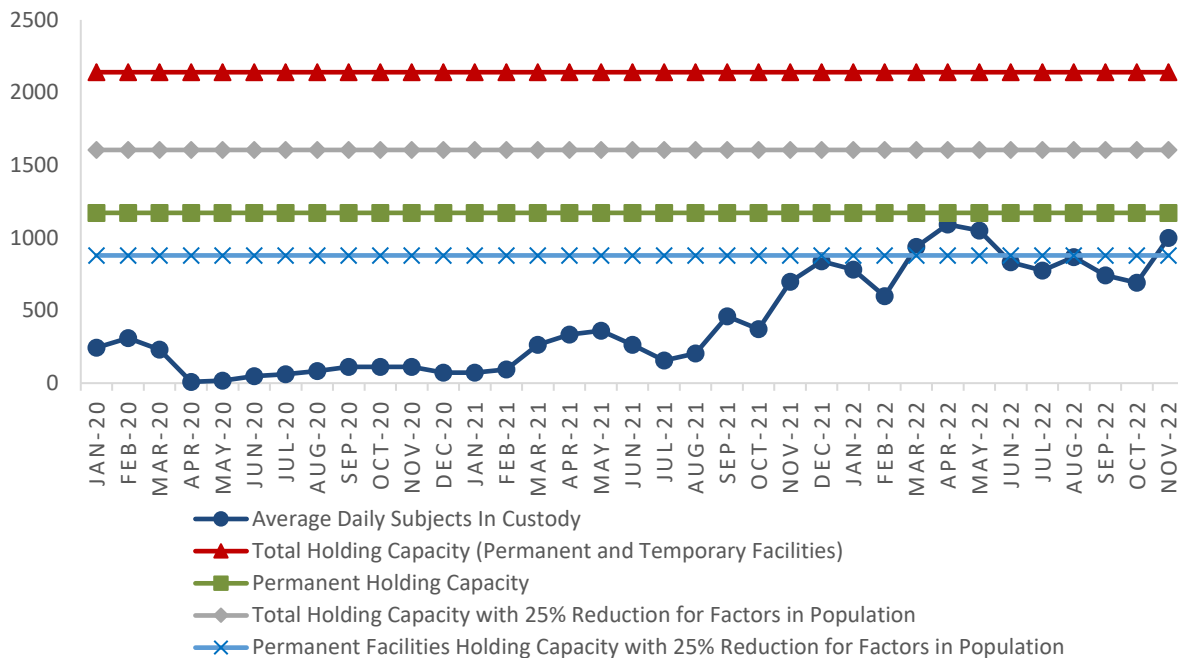
⁵ For Figure 3 and other figures showing holding capacities, we also included calculations showing what a sector's holding capacity would be when reduced by 25 percent. This is to account for factors in the population, such as demographics, gender, single adults, and family units, that may require separating or holding some individuals together, in effect, lowering the number of people who can be held in a facility.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 4. Comparative Analysis of Laredo Average Daily Subjects in Custody to the Sector's Holding Capacities



Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily number of subjects in custody from January 2020 through November 2022

In addition to not documenting a capacity analysis, CBP officials did not consistently document whether they performed cost-benefit analyses to make informed decisions when planning for facility needs. In May 2022, in response to a congressional request, CBP developed a cost comparison of the use of temporary soft-sided and permanent facilities. According to CBP officials, this was the component's first analysis of this type. It showed that temporary soft-sided facilities can be a cost-effective solution if they will be used for fewer than 6 years, at which point CBP could have funded a permanent facility. However, the cost-benefit analysis CBP performed in May 2022 was only done when needed for a specific purpose and is not a consistent part of CBP's facilities planning process.

CBP Did Not Always Consider Alternatives before Issuing Contracts for Temporary Facilities

CBP did not ensure the Rio Grande Valley and Yuma sectors analyzed alternative options and documented this analysis before issuing contracts for



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

temporary facilities. According to CBP, in FY 2022 it spent \$314 million on temporary soft-sided facilities in these sectors.

CBP provided documentation showing that, in response to migrant surges, Border Patrol recommended construction of temporary soft-sided facilities in Donna, Texas (in the Rio Grande Valley sector), due to factors such as its central location in the sector. The documentation to support this decision did not have a detailed explanation to justify temporary soft-sided facilities as the best solution. Border Patrol officials we interviewed confirmed they did not perform any analysis beyond analyzing custody numbers.

Although personnel in the Yuma sector conducted some analyses of alternatives before issuing an initial contract for a temporary soft-sided facility in Yuma, Arizona (see text box), these analyses could have been more thorough. For example, Yuma personnel considered leasing additional detention space. However, the documentation of their analysis did not include a direct comparison to the cost of operating a temporary facility for the same amount of time. Yuma's first temporary facility was in operation from June 2019 until May 2020, when it was taken down.

In March 2021, CBP awarded a contract for a new temporary soft-sided facility in Yuma. However, CBP did not revisit its review of the alternative solutions before issuing the new contract. CBP's documentation to justify this new temporary soft-sided facility did not include an examination of alternative solutions or a cost assessment. The documentation also described CBP's plans for supporting the new temporary soft-sided facility, which indicates that CBP already planned to move forward with the temporary facility without ensuring a complete analysis of alternatives.

Yuma Sector's Alternative Options Included:

Establish an **Inter-Agency Agreement** with the Yuma County Sheriff's Office to lease an annex detention facility in Yuma, Arizona, to ease capacity issues.

Establish a program allowing family units to be **released on their own recognizance** until they appear before a court.

Leverage U.S. Immigration and Customs Enforcement's Enforcement and Removal Operations to reduce the time between bed space requests, approvals, and transfers.

Source: DHS OIG analysis based on information provided by CBP

CBP Did Not Regularly Reassess the Continued Need for Existing Temporary Facilities

CBP continued to authorize contract extensions for temporary facilities without providing the contracting office with detailed analyses to support the need for these facilities. We analyzed contracting documentation from June 2019 through December 2022 for the temporary soft-sided facilities in Donna and

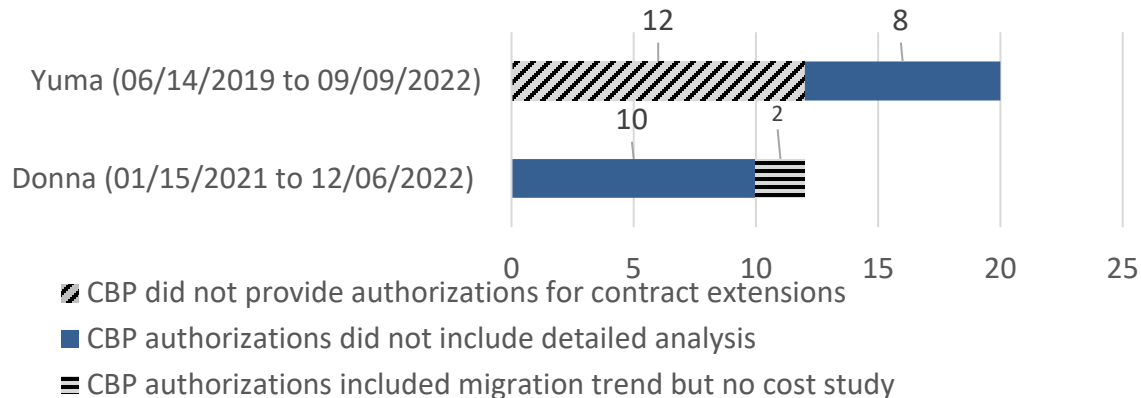


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

the Yuma⁶ sector to determine whether authorizations included CBP's documented analysis before awarding contract extensions. We found program officials could not provide authorizations to support 12 extensions to the contract for the Yuma temporary facility, and 8 of the authorizations did not have detailed analyses. Similarly, for the Donna temporary facilities, program officials provided authorizations for 10 contract extensions that did not have detailed analyses. Also, two Donna authorizations included migration trends but did not include a cost study (see Figure 5).

Figure 5. CBP Authorizations for Contract Extensions of Donna and Yuma Temporary Facilities



Source: DHS OIG analysis based on information provided by CBP

In addition, CBP did not provide support that it continually reassessed its need for one of the temporary soft-sided facilities in Donna while the facility was empty and not actively being used. In September 2022, the Rio Grande Valley sector⁷ recommended the Donna temporary facility be closed due to the unsustainably high cost and a drastic reduction in encounters. However, CBP leadership opted to keep the empty temporary facility on site and place it in a hold status. During a November 2022 interview, CBP officials confirmed they did not know or have a timeline for how long the temporary facility would remain on hold. However, CBP reopened the facility at the end of December 2022. CBP paid \$4.2 million to maintain the facility during the 3 months it was on hold.

CBP's decision to continue to pay for the facility when it was not in use was not supported by migration data. The average daily number of subjects in custody

⁶ Yuma's temporary facility was not operational from May 2020 through March 2021.

⁷ The Donna facility was used to support the Rio Grande Valley sector.

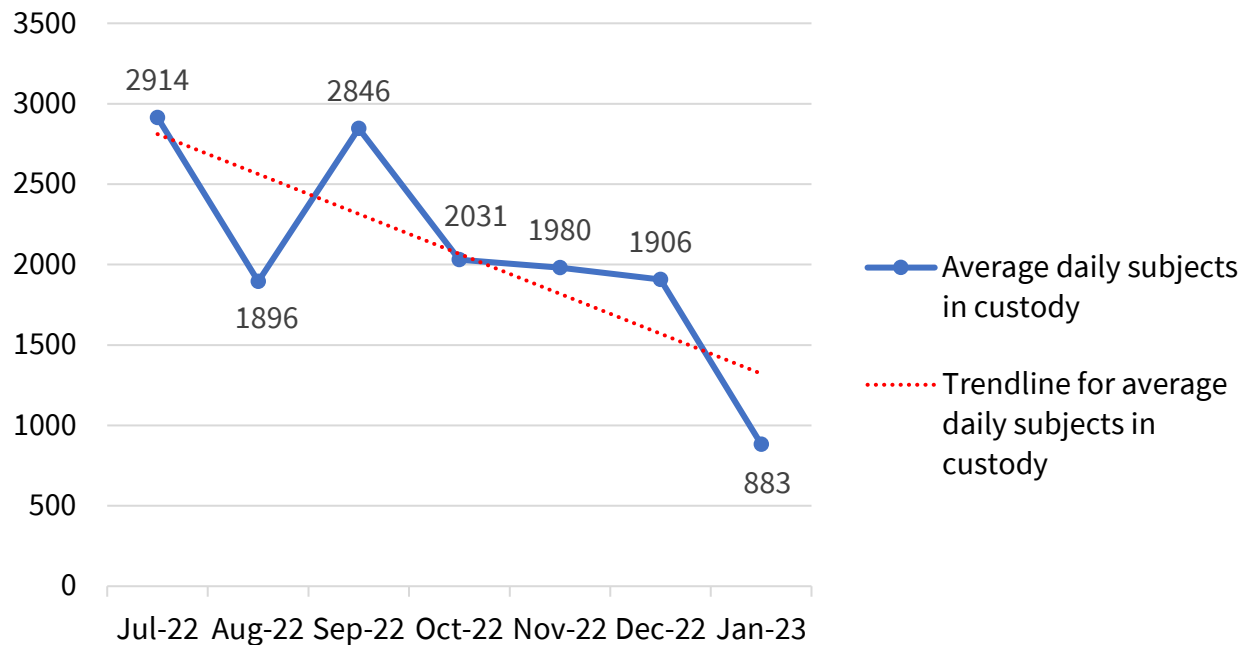


OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

in the Rio Grande Valley sector trended downward during the months the temporary facility was empty, as shown in Figure 6.

Figure 6. Average Daily Subjects in Custody in the Rio Grande Valley Sector and Corresponding Trendline



Source: DHS OIG analysis based on CBP's average daily subjects in custody from July 2022 through January 2023

CBP's Guidance for Planning Temporary and Permanent Facilities Is Not Comprehensive

The issues we identified occurred because CBP prioritized short-term response to migrant surges over long-term facility planning. To help with short-term response, CBP developed the *CBP Integrated SWB Mass Irregular Migration Contingency Plan* to quickly increase facility capacity. However, the plan remains in draft.

CBP does not have a comprehensive policy that incorporates planning for both temporary and permanent facilities along the SWB. Specifically, CBP does not require its personnel to document the use of all available migration information to make informed decisions regarding both temporary and permanent facilities. Also, CBP does not require sectors to identify and document analyses of all



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

possible alternatives before establishing temporary facilities, or to reassess regularly the need for existing temporary facilities, including their cost-effectiveness.

Conclusion

Although CBP has improved its planning processes for temporary facilities, the component continues to rely on a reactive approach instead of developing a more proactive approach. By developing a comprehensive policy, CBP can ensure it spends money on facilities that are cost effective and in the best interest of taxpayers. Additionally, CBP will be more prepared for strains on its facilities from future migrant surges and better positioned to avoid overcrowding and inhumane conditions.

Recommendations

Recommendation 1: We recommend that the Commissioner of CBP finalize the draft *CBP Integrated SWB Mass Irregular Migration Contingency Plan*.

Recommendation 2: We recommend that the Commissioner of CBP establish a comprehensive, formal policy to:

- consistently document the use of all available information to make informed facility planning decisions;
- conduct and document analysis of all possible alternative options before establishing temporary facilities; and
- regularly reassess the continued need for existing temporary facilities and evaluate the cost-effectiveness of maintaining existing temporary facilities.

Management Comments and OIG Analysis

CBP concurred with both recommendations. In its management response, CBP was pleased that our report acknowledged its improved response to migrant surges by deploying temporary facilities to increase its capacity to process migrants along the SWB. CBP also provided technical comments to our draft report. We made changes to incorporate these comments as appropriate. A summary of CBP's responses and our analysis follows. We included CBP's management comments in their entirety in Appendix B.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

CBP Response to Recommendation 1: Concur. CBP is in the process of finalizing the *CBP Integrated SWB Mass Irregular Migration Contingency Plan*, which will implement the *DHS Southwest Border Mass Irregular Migration Contingency Plan*, dated February 2022. Estimated Completion Date: March 29, 2024.

OIG Analysis: We consider these actions responsive to the recommendation, which will remain open and resolved until CBP provides documentation that the plan was approved and implemented.

CBP Response to Recommendation 2: Concur. CBP uses an established annual Capital Facility Investment Planning process to inform and prioritize investments to its permanent facility infrastructure. CBP is committed to reducing the component's reliance on temporary soft-sided facilities and is planning and constructing permanent processing facilities as part of this transition. To support this effort, CBP plans to evaluate current processes to identify areas of improvement and will document, via policy, how temporary facility planning decisions will be made. The resulting policy will standardize documentation requirements, formalize a repository for documentation, establish guidelines for alternatives analysis, and document procedures to regularly reassess the continued need for temporary facilities. Estimated Completion Date: September 30, 2024.

OIG Analysis: We consider these actions responsive to the recommendation, which will remain open and resolved until CBP provides us with a copy of its issued policy.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

The objective of this audit was to determine to the extent to which CBP assessed and planned its needs for temporary and permanent facilities to process and hold migrants along the SWB. To answer our objective, we interviewed multiple CBP officials to gain an understanding of how CBP plans for facilities. We interviewed personnel from:

- Office of the Chief Readiness Support Officer
- Border Patrol sectors:
 - San Diego
 - El Centro
 - Yuma
 - Tucson
 - El Paso
 - Big Bend
 - Del Rio
 - Laredo
 - Rio Grande Valley
- Office of Facilities and Asset Management
 - Border Patrol and Air and Marine Program Management Office
 - Office of Facilities Management and Engineering
- Border Patrol Law Enforcement Operations Directorate
- Office of Acquisition
- SWB Coordination Center

We analyzed DHS and CBP policies, procedures, and other documents related to planning for facilities, migrant surges, and migrant detention. We also reviewed prior DHS OIG and GAO reports, media articles, and congressional testimony.

To assess CBP's facility planning, we performed an assessment comparing the average daily number of subjects in custody to each sector's holding capacities from January 2020 through November 2022. To determine the individual holding capacities of the nine SWB sectors, we corroborated information obtained through CBP interviews with supporting documentation. To determine each sector's average daily in-custody counts, we used data from CBP's public website and corroborated it with daily in-custody information



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

pulled from the DHS Enforcement Integrated Database by DHS OIG's Office of Innovation. We found the data sufficient and reliable to support our analysis.

Additionally, we selected two locations with temporary facilities to assess whether CBP properly documented support for initially establishing the temporary soft-sided facilities and whether CBP assessed the continued need to use the soft-sided facilities. We judgmentally selected facilities in the Rio Grande Valley and Yuma sectors based on the location having a temporary facility that had been operational for more than a year or having more than one temporary facility. We obtained and analyzed documentation to determine how CBP used available data to plan for and make informed decisions regarding the use of the soft-sided facilities. We also reviewed documentation, such as contract agreements and issue papers,⁸ to confirm whether CBP performed analyses, reviewed alternatives, and justified continued use of the soft-sided facilities. Additionally, we requested documentation, such as project requirements documents⁹ and cost-benefit analyses toward the long-term planning process, regarding permanent facilities.

We assessed internal controls related to CBP's planning for permanent and temporary facilities used to process and hold migrants along the SWB. Our assessment revealed that CBP does not have adequate control activities and documentation for its policies and procedures as they relate to facility planning. However, because our internal control assessment was limited to the audit objective, it may not uncover other internal control deficiencies that potentially existed.

We conducted this performance audit between June 2022 and May 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG's Access to DHS Information

During this audit, CBP provided timely responses to DHS OIG's requests for information and did not delay or deny access to information we requested.

⁸ Issue papers are documents from the sector requesting a soft-sided facility.

⁹ Project requirements documents contain project details and authorizations for the construction of permanent facilities.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue, NW
Washington, DC 20229

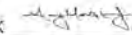


**U.S. Customs and
Border Protection**

August 9, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Henry A. Moak, Jr.
Senior Component Accountable Official
U.S. Customs and Border Protection

X 

8/9/2023

Approved by: HENRY A. MOAK JR.

SUBJECT: Management Response to Draft Report: "CBP Could Do
More to Plan for Facilities Along the Southwest Border"
(Project No. 22-046-AUD-CBP)

Thank you for the opportunity to comment on this draft report. U.S. Customs and Border Protection (CBP) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CBP is pleased to note the OIG's positive recognition of its improved response to migrant surges by deploying temporary facilities to increase CBP's capacity to humanely process migrants along the Southwest border (SWB). CBP secures the U.S. border against illegal entry, illicit activity, or other threats to uphold national sovereignty and promote national and economic security. In support of this mission priority, and as necessitated by the surge of migrants along the SWB, since 2019 CBP has deployed a series of temporary soft-sided facilities to provide short-term holding and support processing of migrants. CBP takes its role in providing care and ensuring health, safety, security, and welfare of each adult and child in its custody very seriously and remains committed to further strengthening its temporary and permanent facilities operations, while also being a good steward of the federal funds provided in support of its varied missions.

The draft report contained two recommendations with which CBP concurs. Enclosed find our detailed response to each recommendation. CBP previously submitted technical comments addressing several accuracy, contextual, sensitivity, and other issues under a separate cover for OIG's consideration.

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



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Enclosure: Management Response to Recommendations Contained in 22-046-AUD-CBP

OIG recommended that the Commissioner of CBP:

Recommendation 1: Finalize the draft “CBP Integrated SWB Mass Irregular Migration Contingency Plan.”

Response: Concur. CBP is in the process of finalizing the “CBP Integrated SWB Mass Irregular Migration Contingency Plan,” which will implement the “DHS Southwest Border Mass Irregular Migration Contingency Plan,” dated February 2022. Estimated Completion Date (ECD): March 29, 2024.

Recommendation 2: Establish a comprehensive, formal policy to:

- consistently document the use of all available information to make informed facility planning decisions;
- conduct and document analysis of all possible alternative options before establishing temporary facilities; and
- regularly reassess the continued need for existing temporary facilities and evaluate the cost effectiveness of maintaining existing temporary facilities.

Response: Concur. CBP utilizes an established annual Capital Facility Investment Planning (CFIP) process to inform and prioritize investments to CBP's permanent facility infrastructure. Given the urgent and unpredictable nature of migrant flow and associated U.S. Border Patrol (USBP) processing requirements on the SWB, temporary processing facility deployments do not follow the standard CFIP process. Instead, USBP determines capacity, sites, and priorities based on a comprehensive assessment, which considers current capacity, processing and transport operations, staffing, and proximity to partners.

CBP is committed to reducing the agency's reliance on temporary soft-sided facilities and is both planning, and constructing, permanent processing facilities as part of this transition. To support this effort, CBP will evaluate current processes to identify areas of improvement, and will document via policy, how temporary facility planning decisions will be made. The resulting policy will standardize documentation requirements, formalize a repository for documentation, establish guidelines for alternatives analysis, and document procedures to regularly reassess the continued need for temporary facilities. ECD: September 30, 2024.



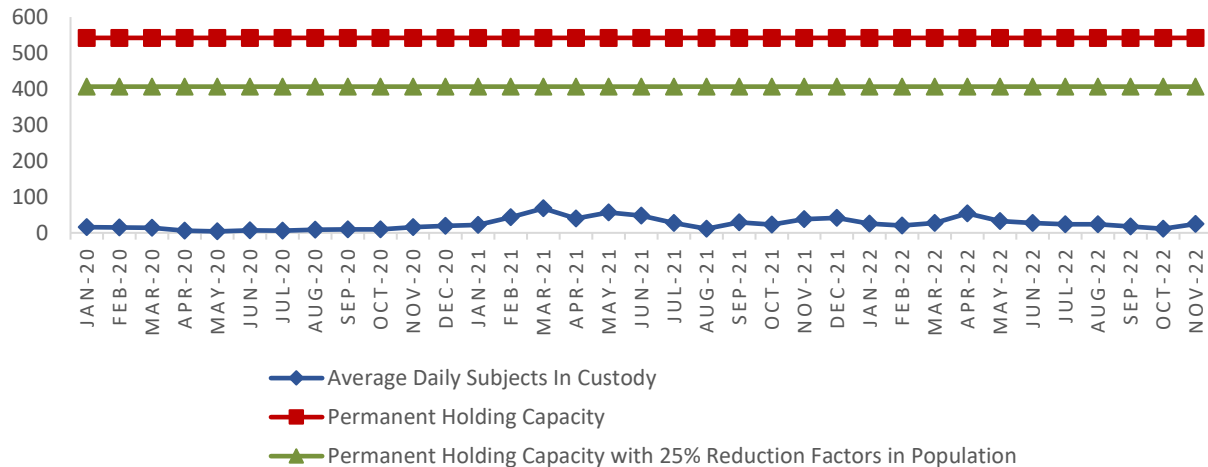
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix C

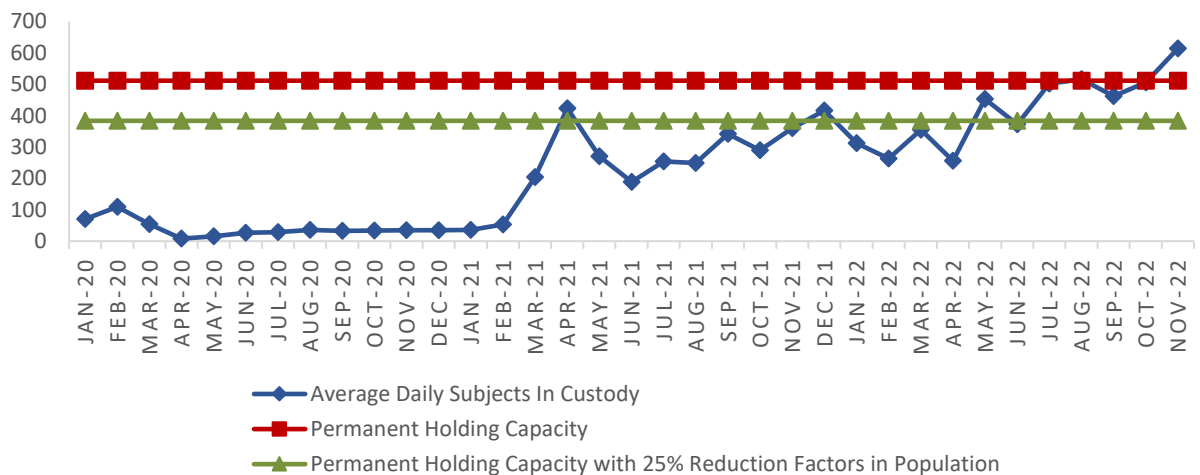
Comparative Analysis of Average Daily Subjects in Custody to Sector Holding Capacity

Figure 7. Comparative Analysis of Big Bend Average Daily Subjects in Custody to the Sector's Holding Capacities



Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily subjects in custody from July 2020 through November 2022

Figure 8. Comparative Analysis of El Centro Average Daily Subjects in Custody to the Sector's Holding Capacities



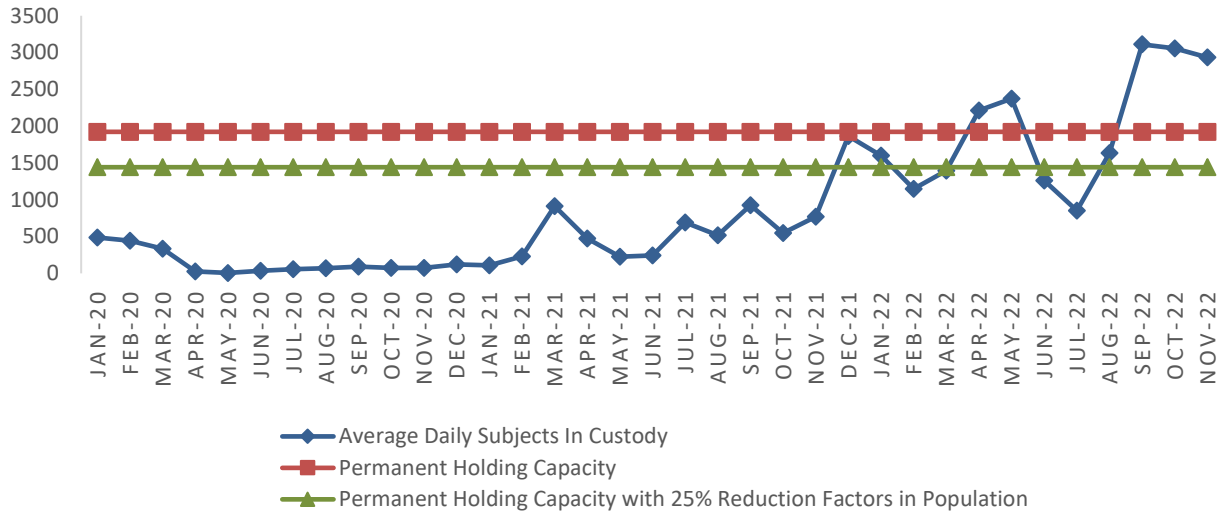
Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily subjects in custody from July 2020 through November 2022



OFFICE OF INSPECTOR GENERAL

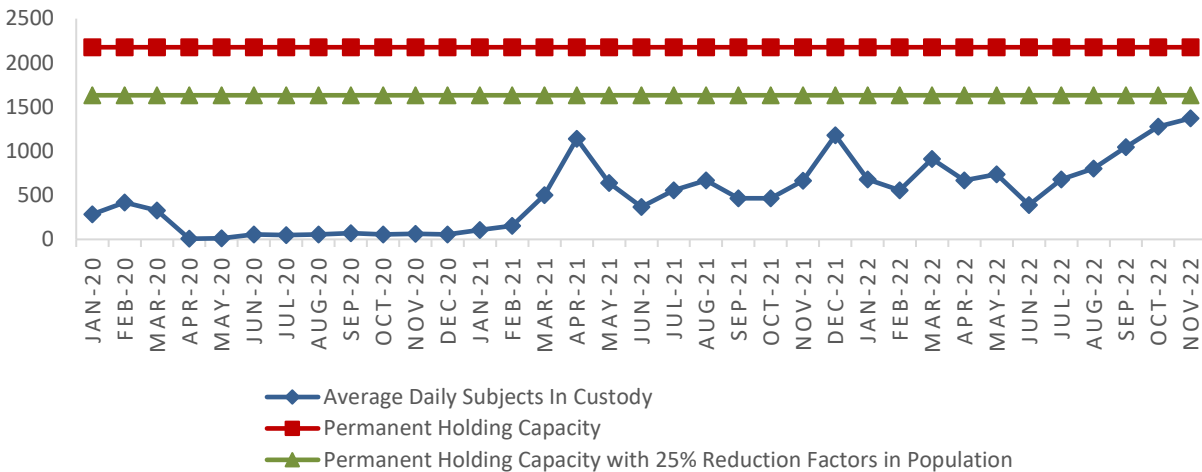
Department of Homeland Security

Figure 9. Comparative Analysis of El Paso Average Daily Subjects in Custody to the Sector's Holding Capacities



Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily subjects in custody from July 2020 through November 2022

Figure 10. Comparative Analysis of San Diego Average Daily Subjects in Custody to the Sector's Holding Capacities



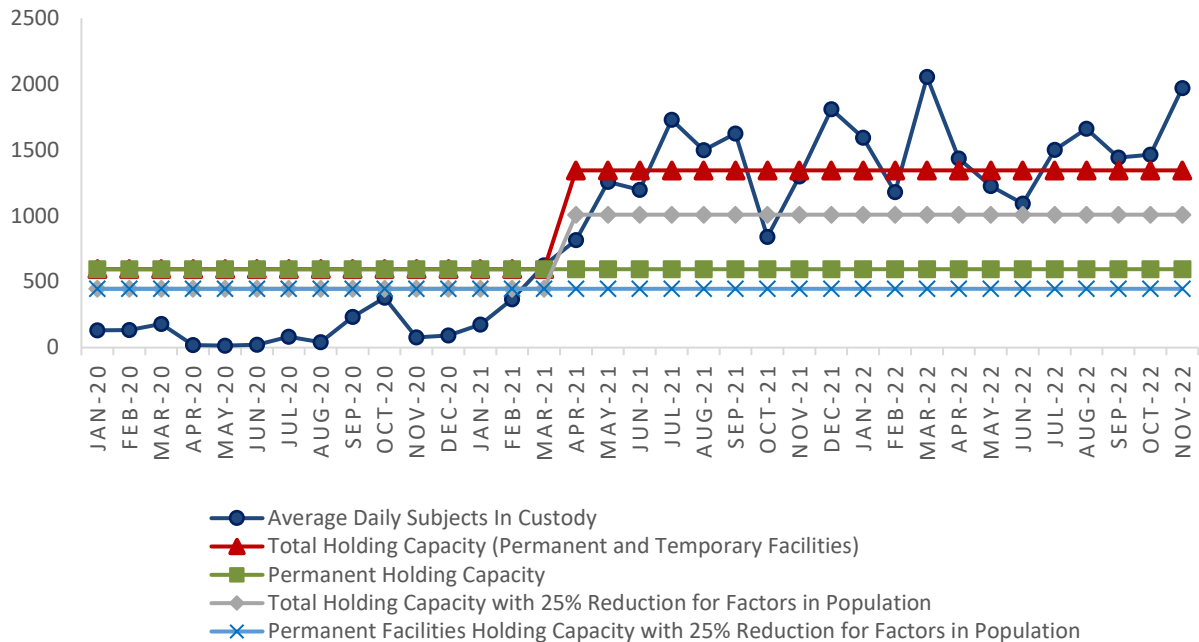
Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily subjects in custody from July 2020 through November 2022



OFFICE OF INSPECTOR GENERAL

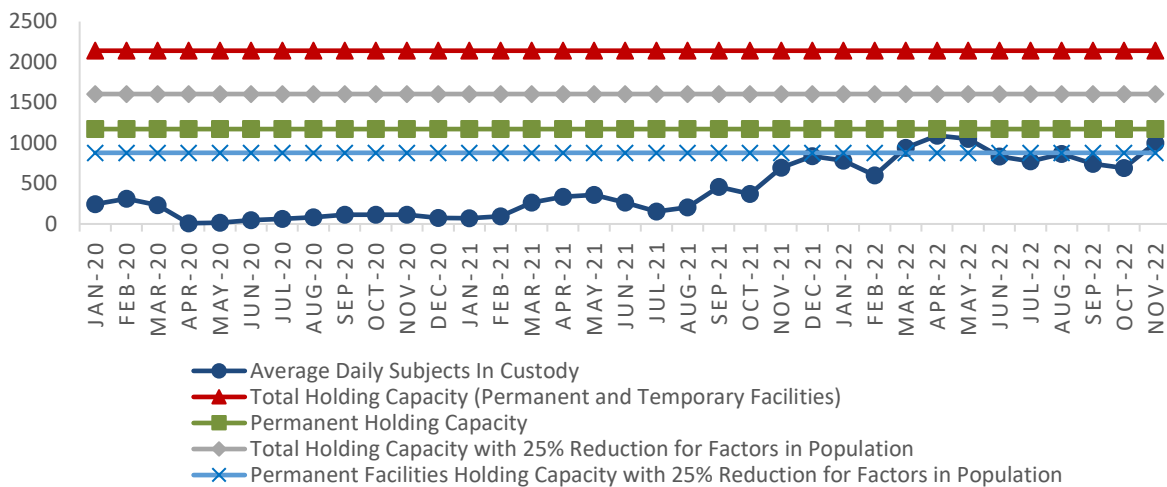
Department of Homeland Security

Figure 11. Comparative Analysis of Del Rio Average Daily Subjects in Custody to the Sector's Holding Capacities



Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily number of subjects in custody from January 2020 through November 2022

Figure 12. Comparative Analysis of Laredo Average Daily Subjects in Custody to the Sector's Holding Capacities



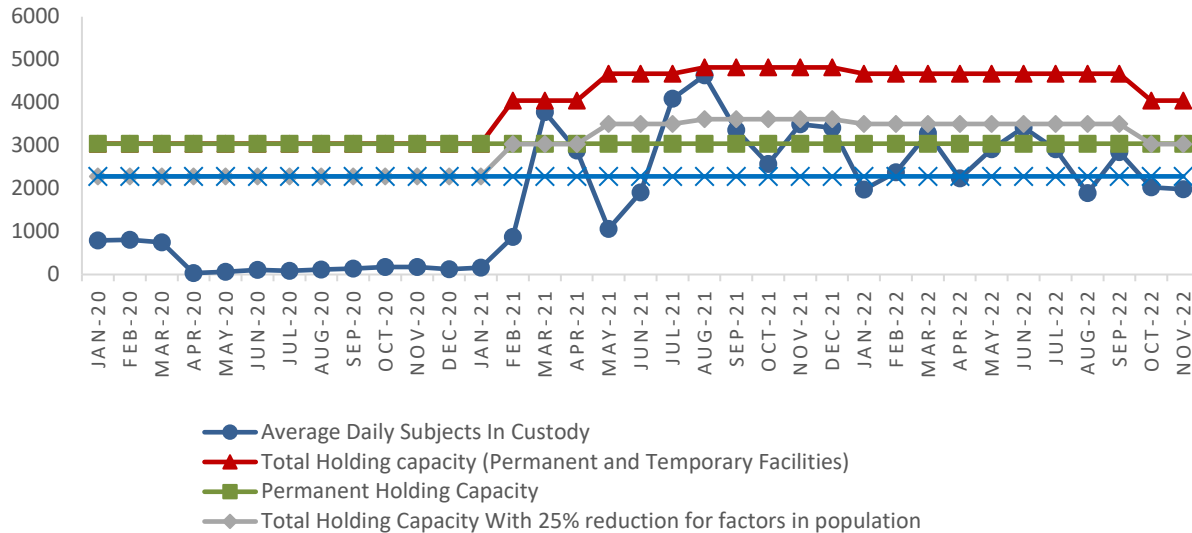
Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily number of subjects in custody from January 2020 through November 2022



OFFICE OF INSPECTOR GENERAL

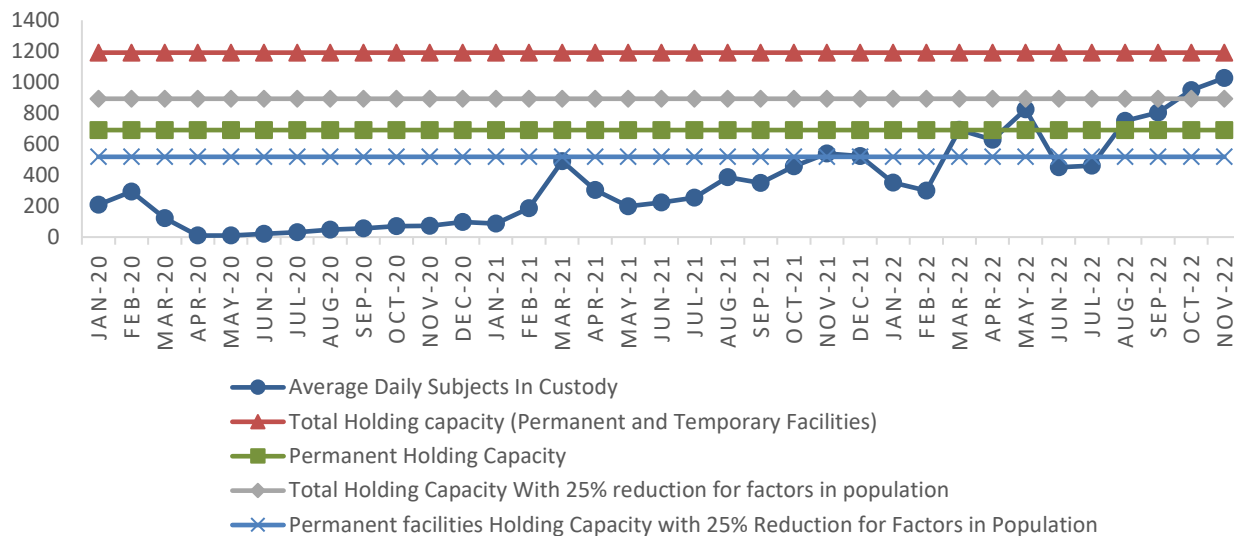
Department of Homeland Security

Figure 13. Comparative Analysis of Rio Grande Valley Average Daily Subjects in Custody to the Sector's Holding Capacities



Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily subjects in custody from July 2020 through November 2022

Figure 14. Comparative Analysis of Tucson Average Daily Subjects in Custody to the Sector's Holding Capacities



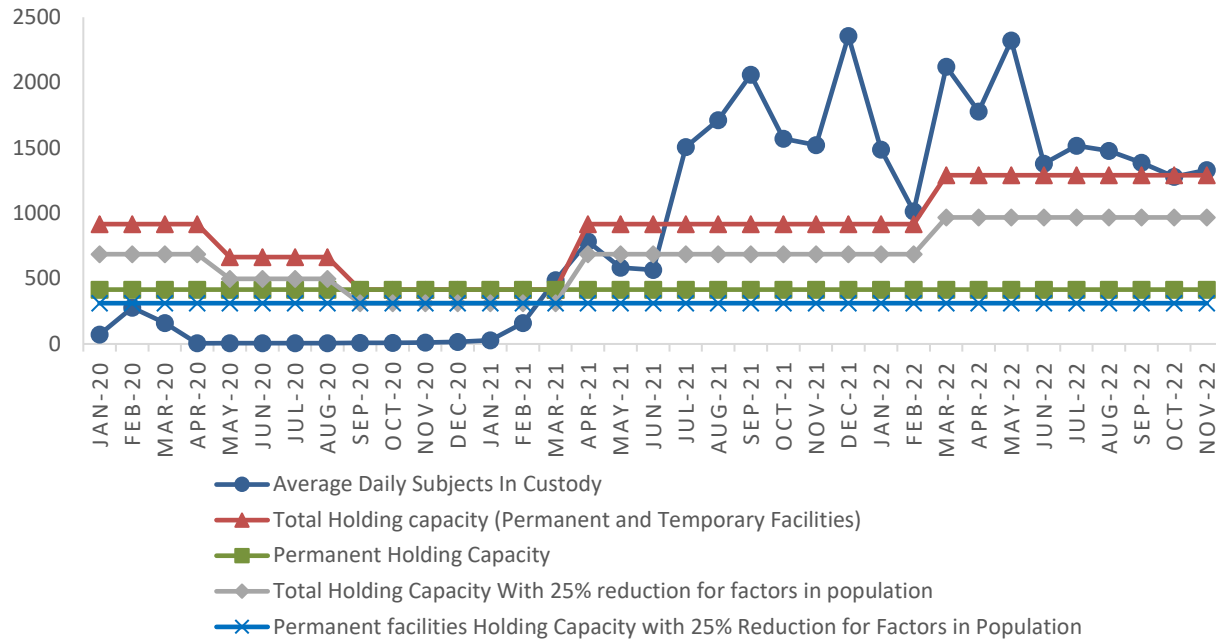
Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily subjects in custody from July 2020 through November 2022



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 15. Comparative Analysis of Yuma Average Daily Subjects in Custody to the Sector's Holding Capacities



Source: DHS OIG analysis based on CBP sector holding capacities and CBP's average daily subjects in custody from July 2020 through November 2022



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

U.S. Customs and Border Protection

Commissioner
CBP Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

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

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



OIG Hotline

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

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



September 2023

FACIAL RECOGNITION SERVICES

Federal Law
Enforcement
Agencies Should Take
Actions to Implement
Training, and Policies
for Civil Liberties

Why GAO Did This Study

Law enforcement may use facial recognition services provided by commercial and nonprofit entities to help solve crimes. For example, these services allow users to quickly search through billions of photos to help identify an unknown suspect in a crime scene photo.

GAO was asked to review federal law enforcement's use of facial recognition technology. This report examines, among other issues, the extent to which selected DHS and DOJ law enforcement agencies used facial recognition services to support criminal investigations; required staff to take training on facial recognition technology to use such services; and developed policies and guidance specific to facial recognition technology to help protect civil rights and civil liberties.

GAO selected seven law enforcement agencies within DHS and DOJ based on various factors, including the number of facial recognition technology systems used. GAO reviewed documents, such as training requirements and policies for using facial recognition services. GAO also analyzed training records and interviewed agency officials.

What GAO Recommends

GAO is making 10 recommendations, including that FBI implement a training requirement and clarify the status of its training requirement to stakeholders. GAO also recommends that DOJ develop a plan to issue a facial recognition technology policy addressing safeguards for civil rights and civil liberties. Agencies concurred with all 10 recommendations.

View [GAO-23-105607](#). For more information, contact Gretta L. Goodwin at (202) 512-8777 or goodwin@gao.gov.

September 2023

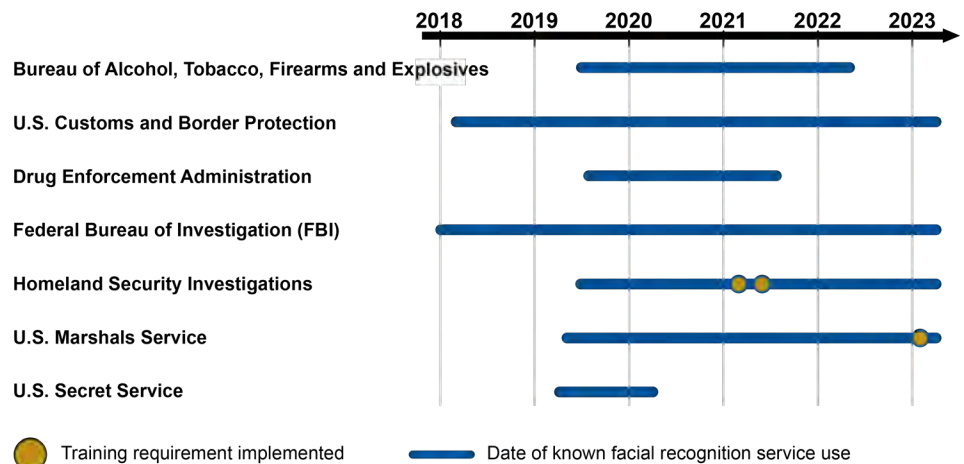
FACIAL RECOGNITION SERVICES

Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties

What GAO Found

Seven law enforcement agencies in the Departments of Homeland Security (DHS) and Justice (DOJ) reported using facial recognition services provided by commercial and nonprofit entities. The agencies reported using four services in total from October 2019 through March 2022 to support criminal investigations. All seven agencies initially used these services without requiring staff take facial recognition training. GAO found that six agencies had available data and cumulatively conducted about 60,000 searches when they did not have training requirements in place. As of April 2023, two agencies began to require training.

Facial Recognition Services, Use and Training for Selected Agencies, April 2023



Source: GAO analysis of agency information. | GAO-23-105607

Note: The figure shows when agencies used the four services covered by this review (services used from October 2019 through March 2022), and when, if at all, agencies implemented training requirements for facial recognition services. The figure provides use and training information as of April 2023. See figure 6 of the report for more detail.

FBI officials told key internal stakeholders that certain staff must take training to use one facial recognition service. However, in practice, FBI has only recommended it as a best practice. GAO found that few of these staff completed the training, and across the FBI, only 10 staff completed facial recognition training of 196 staff that accessed the service. FBI said they intend to implement a training requirement for all staff, but have not yet done so. Such a requirement would help FBI ensure its staff understand how to use these services. Also, clarifying the status of FBI's training requirement would allow stakeholders to fully evaluate use of the service against FBI ethical and privacy standards.

GAO also found that three of the seven agencies had policies or guidance specific to facial recognition technology that address civil rights and civil liberties. The other four agencies—three in DOJ and one in DHS—did not have such policies or guidance. DHS has plans to finalize a department-wide policy by December 2023. DOJ has taken steps to issue a department-wide policy, but has faced delays. Developing a plan with time frames and milestones would help DOJ ensure it issues a policy to support staff in safeguarding civil rights and civil liberties.

Contents

Letter		1
	Background	6
	Federal Law Enforcement Agencies Used Four Facial Recognition Services to Support Criminal Investigations	12
	Agencies with Available Data Reported Conducting About 60,000 Facial Recognition Searches Before Requiring Training	19
	Three of Seven Agencies Took Some Steps to Address Selected Privacy Requirements	30
	Most Agencies Did Not Have Policies Specific to Facial Recognition to Help Protect Civil Rights and Civil Liberties	36
	Conclusions	40
	Recommendations for Executive Action	42
	Agency Comments and Our Evaluation	43
Appendix I	Objectives, Scope and Methodology	46
Appendix II	Extent to Which Selected Federal Law Enforcement Agencies Took Steps to Address Selected Privacy Requirements	53
Appendix III	Comments from the Department of Homeland Security	61
Appendix IV	GAO Contact and Staff Acknowledgements	67
Tables		
	Table 1: Selected Privacy Requirements for Department of Homeland Security's (DHS) and Department of Justice's (DOJ) Use of Facial Recognition Services	9
	Table 2: Training Status of Homeland Security Investigations Staff That Conducted Facial Recognition Searches on Clearview AI from March 4, 2021 through March 31, 2022	24

Figures

Figure 1: Facial Recognition Technology Identification Search Process for Criminal Investigations	7
Figure 2: Facial Recognition Services Used by Selected Federal Law Enforcement Agencies to Support Criminal Investigations from October 2019 through March 2022	13
Figure 3: Reported Number of Searches That Federal Agencies Conducted Using Facial Recognition Services, Based on Available Data from October 2019 through March 2022	15
Figure 4: Selected Federal Law Enforcement Agencies' Reported Use of Facial Recognition Services	16
Figure 5: Homeland Security Investigations Agent Working to Identify Suspected Child Abusers and Victims	17
Figure 6: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023	20
Figure 7: Extent to which Selected Agencies Addressed Selected Privacy Requirements while Using Facial Recognition Services as of April 2023	31

Abbreviations

AI	artificial intelligence
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CBP	U.S. Customs and Border Protection
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
HSI	Homeland Security Investigations
ICE	U.S. Immigration and Customs Enforcement
PIA	privacy impact assessment
PII	personally identifiable information

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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.



September 5, 2023

Congressional Requesters

Facial recognition technology is a tool that the federal law enforcement community may use to help solve crimes. For example, facial recognition technology can allow users to quickly search through billions of photos to help identify an unknown suspect in a crime scene photo. A criminal investigator can also use this technology to help identify a victim in a photo or video. Federal agencies can own facial recognition technology or leverage technology owned by state and local governments. Federal agencies can also use facial recognition services offered by commercial and nonprofit entities.¹ While facial recognition services may support criminal investigations, members of Congress have raised questions about the extent to which federal law enforcement agencies use such services.

We have previously examined aspects of federal law enforcement agencies' use of facial recognition technology. For example, in June 2021, we found that 14 federal agencies that employed law enforcement officers used facial recognition technology, such as commercial services, to support criminal investigations. However, we found that 13 of these agencies did not have complete, up-to-date information on which facial recognition systems staff were using. We recommended that the 13 agencies—including agencies within the Department of Homeland Security (DHS) and the Department of Justice (DOJ)—track the use of such systems and assess the associated risks.²

You asked us to review federal law enforcement's use of facial recognition technology and its effects on privacy, civil rights, and civil

¹For the purposes of this report, the term facial recognition service includes services provided by nonprofit and commercial entities. Thus, the term facial recognition services does not include technology owned and operated by federal, state, and local government entities.

²As of July 2023, agencies have taken actions to fully or partially implement 11 of the 26 recommendations to track the use of facial recognition systems and assess the associated risks. See GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, [GAO-21-518](#) (Washington, D.C.: June 2021).

liberties.³ This report examines the extent to which selected DHS and DOJ law enforcement agencies have:

- (1) used facial recognition services to support criminal investigations from October 2019 through March 2022;
- (2) required staff to take training on facial recognition technology to use such services, and ensured compliance with requirements;
- (3) taken steps to address selected privacy requirements for using facial recognition services; and,
- (4) developed policies and guidance specific to facial recognition technology to help protect civil liberties and civil rights.

To address all four objectives, we selected seven agencies within DHS and DOJ that employ law enforcement officers (law enforcement agencies).⁴ We limited our selection to DHS and DOJ agencies because these two departments employ the highest number of law enforcement officers within the federal government, and cumulatively employ more than 80 percent of all federal law enforcement officers.⁵ From there, we identified DHS and DOJ law enforcement agencies that previously reported owning or using facial recognition technology systems in 2020.⁶

We then selected the seven agencies that reported owning or using the highest number of facial recognition systems to include in this review. Within the DHS, we selected U.S. Customs and Border Protection (CBP); U.S. Immigration and Customs Enforcement's (ICE) Homeland Security

³For the purposes of this review, we are defining "privacy" as individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information (PII), including data such as names, Social Security numbers, or photos. We are defining "civil rights" as due process protections and personal rights protected by the U.S. Constitution and federal laws, such as the Civil Rights Act of 1964; and "civil liberties" as the exercise of activities protected under the First Amendment.

⁴Consistent with our prior work, we define federal law enforcement officers as full-time employees with federal arrest authority who are authorized to carry firearms while on duty.

⁵Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016 – Statistical Tables*, NCJ 251922 (Washington, D.C.: October 2019).

⁶[GAO-21-518](#).

Investigations (HSI); and, the U.S. Secret Service.⁷ Within the DOJ, we selected the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); the Drug Enforcement Administration (DEA); the Federal Bureau of Investigation (FBI); and, the U.S. Marshals Service. The seven law enforcement agencies we selected are not representative of all law enforcement agencies.

Our review included agencies that used facial recognition services in support of criminal investigations, including sharing information (e.g., leads). For example, one agency—CBP—told us that it does not lead criminal investigations but has used facial recognition services to develop and share information in support of other agencies' criminal investigations.⁸ We focused exclusively on the use of facial recognition technology services offered by commercial and nonprofit entities (facial recognition services) to build upon our prior reports that reviewed technologies owned and operated by federal agencies.⁹

To address our first objective, we reviewed agency documentation and interviewed agency officials to identify commercial and nonprofit facial recognition services that agencies used from October 2019 through March 2022 to support criminal investigations.¹⁰ We then obtained and analyzed available data to determine the total number of searches that agency staff conducted using these services from October 2019 through March 2022. We assessed the reliability of these data by interviewing knowledgeable agency officials and representatives from each service that agencies reported using during this time period. In addition, we

⁷HSI is one of the investigative agencies within DHS responsible for investigating transnational crime and threats. HSI conducts federal criminal investigations into the illegal cross-border movement of people, goods, money, technology, and other contraband throughout the United States.

⁸CBP officials told us that the agency used facial recognition services primarily for immigration enforcement and border security purposes.

⁹See for example, [GAO-21-518](#); GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, [GAO-21-526](#) (Washington, D.C.: Aug. 2021); GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, [GAO-20-568](#) (Washington, D.C.: Sep 2020); and, GAO, *FACE Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, [GAO-16-267](#) (Washington, D.C.: May 2016, reissued Aug. 2016).

¹⁰We selected this timeframe to overlap with our prior work, and to extend to the most recent data available when we conducted our analysis. We previously reported on agencies' use of facial recognition technology from January 2015 through March 2020 (see [GAO-21-518](#)).

tested these data for outliers or obvious errors when possible. We determined that these data were sufficiently reliable for reporting on the minimum number of searches conducted by agencies during the period of our review.

To address our second objective, we reviewed agency documentation, including policies, guidance, and memorandums to determine the extent to which agencies required staff to take training on facial recognition technology to use such services.¹¹ In addition, we interviewed officials and reviewed available training materials to understand the nature and purpose of such training.¹² To understand the extent to which trained and untrained staff used facial recognition services, we then obtained and analyzed available data on staff training and facial recognition searches that staff conducted.

We assessed the reliability of these data by interviewing knowledgeable agency officials and company representatives, reviewing existing information about the data systems, and testing these data for outliers or obvious errors when possible. We determined that these data were sufficiently reliable for reporting on the number of trained and untrained staff who used facial recognition services. Finally, we compared the agencies' efforts to ensure compliance with training requirements to agency policy, our human capital guidance, and *Standards for Internal Control in the Federal Government*.¹³

To address our third objective, we reviewed relevant departmental privacy policies and guidance, such as DHS and DOJ guidance on implementing

¹¹We assessed the extent to which agencies had implemented training specifically required for using facial recognition services, and did not assess requirements for more general training that agency staff may receive, such as general privacy training. We considered a training requirement to be written instruction to staff mandating training as a condition of access to a facial recognition service.

¹²We did not evaluate the content of this training to ascertain its sufficiency or appropriateness because there are no national training standards for facial recognition technology, which we discuss later in this report.

¹³GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, [GAO-04-546G](#) (Washington, D.C.: March 2004), GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

aspects of the E-Government Act of 2002.¹⁴ Based on our review of these policies and guidance, we identified four privacy requirements that generally apply to agencies when using facial recognition services.¹⁵ To identify the extent to which agencies addressed selected privacy requirements for using facial recognition services, we analyzed agency documentation—such as initial privacy reviews, privacy impact assessments, sensitive information and privacy checklists, and contract documentation. We also interviewed cognizant agency officials. Finally, we compared agencies’ efforts to address selected privacy requirements for using facial recognition services to principles in the *Standards for Internal Control in the Federal Government*.¹⁶

To address our fourth objective, we reviewed agency documentation and interviewed agency officials to understand the extent to which agencies had existing policies and guidance that addressed civil rights and civil liberties in the context of facial recognition technology. We also reviewed a congressional report and executive order related to facial recognition technology policies.¹⁷ We then interviewed department officials to understand their efforts to develop and implement new department-wide guidance related to civil rights and civil liberties specific to facial recognition technology, and to address the congressional report and

¹⁴Department of Homeland Security, Privacy Office, *Privacy Impact Assessments: Privacy Office Official Guidance*, (Washington, D.C.: June 2010). Department of Justice, Office of Privacy and Civil Liberties, *Privacy Impact Assessments: Official Guidance*, (Washington, D.C.: Revised July 2015). The E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921 (2002).

¹⁵The specific requirements applicable to DHS’s and DOJ’s use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. The four key privacy requirements we selected are (1) conduct initial privacy review; (2) conduct privacy impact assessment; (3) assess privacy needs prior to acquisition, and (4) oversee privacy controls for contractor access to PII. In addition, not all listed privacy requirements may apply to an agency’s use of a facial recognition service. For example, an agency may conclude in its initial privacy review that a privacy impact assessment is not required.

¹⁶[GAO-14-704G](#).

¹⁷See H.R. Rep. No. 117-97 (2021) (accompanying Consolidated Appropriations Act, 2022, Pub. L. No. 117-103, 136 Stat. 49 (2022) and incorporated by reference in the explanatory statement for the Act, 168 Cong. Rec. H1772 (2022)); Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

executive order. We compared agencies' efforts to develop such policies and guidance to leading project management practices.¹⁸

Appendix I provides additional information on our scope and methodology for all four objectives.

We conducted this performance audit from January 2022 through September 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

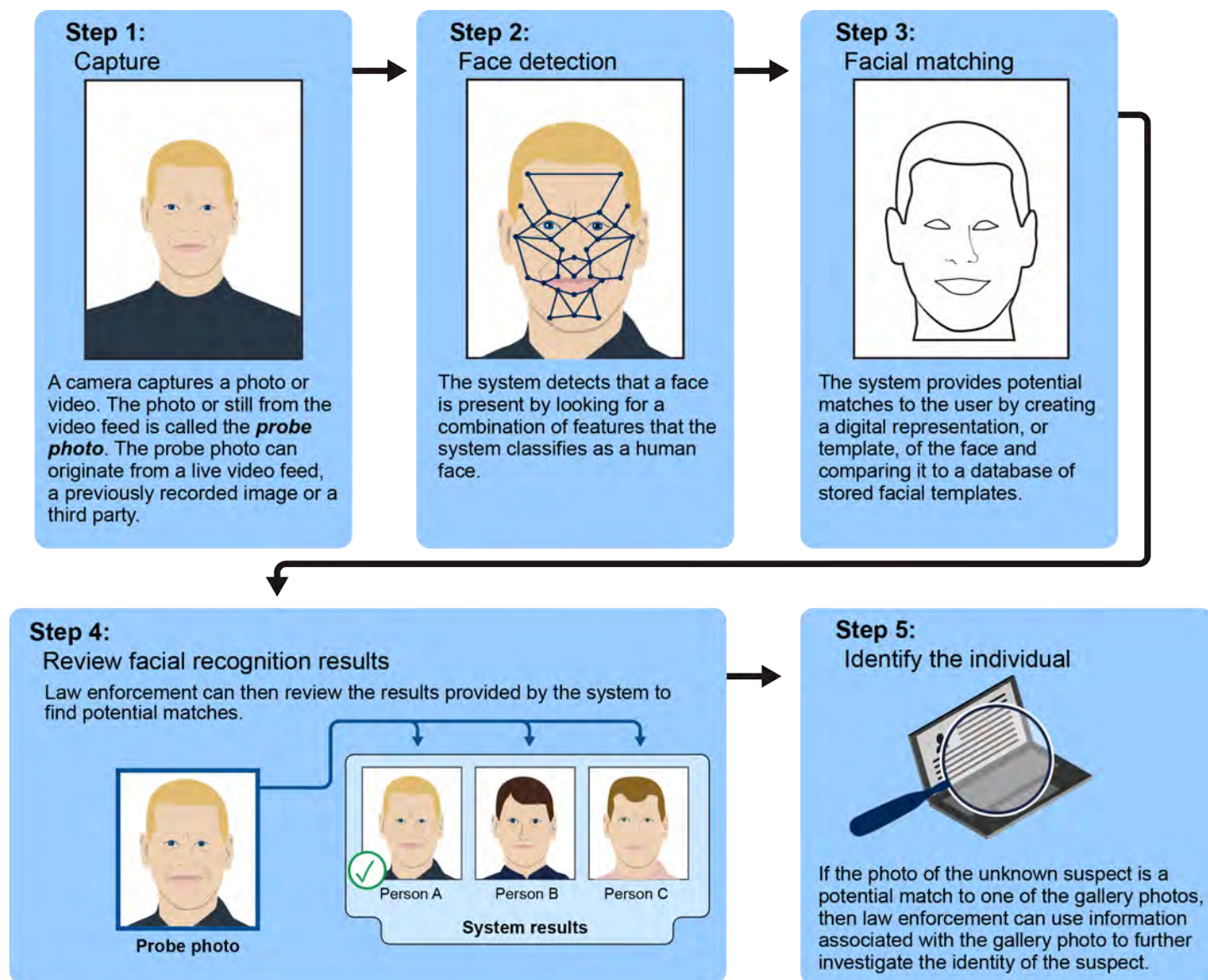
Facial Recognition Technology for Criminal Investigations

An identification search (or one-to-many search) is a type of facial recognition search used by the law enforcement community to support criminal investigations. Identification searches compare a photo of a single unknown individual against a gallery of photos to determine if there is a potential match (i.e., an investigative lead). For example, investigators may compare a photo of an unknown suspect from a crime scene against a facial recognition service's gallery of photos.¹⁹ If the photo of the unknown suspect is a potential match to one of the gallery photos, investigators can then use information associated with the gallery photo to investigate the identity of the suspect further. For example, a gallery photo may be linked to a public social media profile. Investigators can review details found in the profile, such as name and location, in conjunction with information gathered from other sources (e.g., information from witnesses, or evidence found at a crime scene) to potentially determine the identity of the suspect. Figure 1 shows how law enforcement may use a facial recognition identification search to support a criminal investigation.

¹⁸Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition* (2017). PMBOK is a trademark of Project Management Institute, Inc. The Project Management Institute is a not-for-profit association that, among other things, provides standards for managing various aspects of projects, programs, and portfolios.

¹⁹The photos in a facial recognition service's gallery may be drawn from various sources, including public web sites.

Figure 1: Facial Recognition Technology Identification Search Process for Criminal Investigations



Source: GAO analysis. | GAO-23-105607

Training Requirements to Use Facial Recognition Services in Criminal Investigations

There are no federal laws or regulations that require specific training for DHS or DOJ employees using facial recognition technology or services to support criminal investigations. A scientific working group that focuses on facial identification has developed training standards for using facial recognition technology, but federal agencies are not required to adopt these standards.²⁰ However, federal law enforcement agencies may establish their own training requirements for using facial recognition services, and we discuss the extent to which DHS and DOJ have done so later in this report.

Privacy Requirements for Using Facial Recognition Services

DHS and DOJ consider photos, such as those used for facial recognition services, as personally identifiable information (PII).²¹ The departments' guidance directs agencies to take certain steps to help prevent the inappropriate collection, use, and release of PII when acquiring or using services that collect such information. The requirements applicable to DHS's and DOJ's use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. Table 1 provides an overview of selected privacy requirements.²²

²⁰The Facial Identification Scientific Working Group, which includes DHS and DOJ representatives, aims to develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features and to provide recommendations for research and development activities necessary to advance the state of the science in this field. The working group participates in an ongoing initiative by National Institute of Standards and Technology and DOJ to strengthen forensic science in the United States.

²¹Department of Homeland Security, Privacy Office, *Privacy and Civil Liberties Policy Guidance Memorandum*, (Washington, D.C.: June 20009). Department of Justice, Office of Privacy and Civil Liberties, *Initial Privacy Assessment Instructions and Template, Revised 2019*. For the purposes of this report, we are defining PII as any information that can be used to distinguish or trace an individual's identity, such as a photo, name, date and place of birth, and Social Security number; or that otherwise can be linked to an individual, in accordance with DHS, DOJ, and Office of Management and Budget Guidance.

²²The privacy requirements that we selected for this review are from DHS and DOJ privacy guidance, including guidance on implementing the E-Government Act's Privacy Impact Assessment provision. There may be other privacy requirements that apply to federal agencies' use of services that collect PII that we do not discuss. E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921 (2002). The E-Government Act of 2002 addresses the protection of personal information in government information systems or information collections by requiring that agencies take certain steps to analyze how personal information is collected, stored, shared, and managed in a federal system.

Table 1: Selected Privacy Requirements for Department of Homeland Security’s (DHS) and Department of Justice’s (DOJ) Use of Facial Recognition Services

<i>Conduct Initial Privacy Review</i>	DHS and DOJ agencies are to complete initial privacy reviews when they intend to design, develop, or procure a project that will include personally identifiable information (PII), such as a facial recognition service. These reviews help agencies identify potential privacy issues related to the use of PII; assess whether additional privacy requirements apply; and ultimately, help ensure the agency’s compliance with applicable privacy laws and policies. Based on its initial privacy review, an agency may determine that use of a service requires a more comprehensive privacy assessment, known as a privacy impact assessment (PIA).
<i>Conduct Privacy Impact Assessment (PIA)</i>	DHS and DOJ agencies are to complete PIAs before developing or procuring information technologies that collect, maintain, or disseminate PII. A PIA is an analysis of how PII is handled to (1) ensure compliance with applicable privacy requirements; (2) determine the privacy risks associated with an information system or activity; and, (3) evaluate ways the agency can mitigate potential privacy risks. For example, in a PIA, an agency may identify staff conducting inappropriate facial recognition searches as a potential privacy risk. The agency may then identify a related mitigation—such as requiring all staff take training on the appropriate use of facial recognition technology—that will help manage the potential privacy risk.
<i>Assess Privacy Needs Prior to Acquisition</i>	DHS and DOJ guidance directs agencies to consider privacy needs in decisions concerning the acquisition of services that handle PII. For example, the DHS Acquisition Manual requires that staff complete a checklist of considerations for sensitive information (including PII) for all acquisitions regardless of dollar value. Additionally, DOJ guidance states that privacy should be considered in the beginning stages of a proposed project, whether that project necessitates an external acquisition or not, to ensure that privacy protections are built into the system from the start.
<i>Oversee Privacy Controls for Contractor Access to Personally Identifiable Information</i>	DHS and DOJ agencies must include certain terms related to privacy in contracts when contractors will have access to PII. DHS acquisition regulations require that when contractors have access to sensitive information, including PII, DHS contracts are to include terms to safeguard PII. ^a For example, such DHS contracts are to include a clause requiring contractors with access to sensitive information to sign non-disclosure agreements, and direct how contractors are to handle PII. Similarly, DOJ requires contracts to include terms requiring contractors with access to PII take privacy training, sign non-disclosure agreements, and report data breaches, among other privacy requirements.

Source: GAO analysis of DHS and DOJ privacy guidance. | GAO-23-105607

Note: These selected privacy requirements are from DHS and DOJ privacy guidance, including guidance on implementing the E-Government Act’s Privacy Impact Assessment provision. The specific requirements applicable to DHS’s and DOJ’s use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. Further, there are other privacy requirements that can apply to the departments’ use of these services that are not included in this table and that were not included in our review.

^aSee Department of Homeland Security, *HSAR Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information* (Washington, D.C., Mar. 2015); Homeland Security Acquisition Regulation § 3052.204-71(a).

Facial Recognition Technology, Civil Rights and Civil Liberties

The use of facial recognition technology for criminal investigations presents unique questions about civil rights and civil liberties. For example, civil liberties advocates have noted that the use of facial recognition at certain events—such as protests—could have a chilling

effect on individuals' exercise of their First Amendment rights.²³

Additionally, facial recognition technology, like all artificial intelligence (AI) technology, contains the potential for error and thus the potential to misidentify individuals.²⁴ As a result, civil rights advocates have cautioned that an over-reliance on facial recognition technology in criminal investigations could lead to the arrest and prosecution of innocent people, and in particular innocent people of certain racial and ethnic backgrounds.²⁵

Though not specific to facial recognition technology, both DOJ and DHS have longstanding guidance and policies that officials stated apply to the technology and can help safeguard civil liberties and civil rights during criminal investigations. For example, since 2003, DOJ has had guidance that limits the use of demographic characteristics by all federal law enforcement officers (including DHS law enforcement officers) during domestic law enforcement activities.²⁶ Additionally, in 2019, the DHS Secretary issued a memorandum to all employees emphasizing longstanding legal prohibitions on maintaining records that describe how U.S.

²³See, e.g., *Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties: Hearing Before the H. Comm. on Oversight and Reform*, 116th Cong. (2019) (statement of Neema Singh Guliani, Senior Legislative Counsel, American Civil Liberties Union).

²⁴Since 2018, the National Institute of Standards and Technology has tested facial recognition algorithms, and reported that performance differences varied by the algorithms tested, with some performing better than others. For a small number of the one-to-many algorithms, differences in false positives across demographic groups were undetectable. The extent of performance differences varied by the algorithm developer, type of error, and quality of the facial images. National Institute of Standards and Technology, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST Interagency or Internal Report 8280 (Dec. 19, 2019).

²⁵National Association of Criminal Defense Lawyers, *Letter to the White House Office of Science and Technology Policy*, January 15, 2022.

²⁶Department of Justice, *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, Gender Identity and Disability* (Washington, D.C.: 2023). Among other things, the current version of guidance notes that federal law enforcement officers may not use race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in making routine or spontaneous law enforcement decisions. This guidance is limited to domestic law enforcement activities and does not apply to U.S. military, diplomatic, or non-Department of Justice intelligence agencies and their activities. In addition, this Guidance does not apply to interdiction activities at the border or its functional equivalent (e.g., airports, seaports, and other ports of entry) and related traveler and cargo vetting activities or to protective and inspection activities.

citizens and certain other individuals exercise their First Amendment rights.²⁷

In addition, Congress and the President have directed certain federal departments to develop new policies to help ensure the protection of civil rights and civil liberties when using facial recognition technology. For example, a House committee report accompanying DOJ's fiscal year 2022 appropriations act directed DOJ to develop ethical policies for the use of facial recognition technology.²⁸

Additionally, in May 2022, the President issued Executive Order 14074, which directed DOJ and DHS to take actions related to facial recognition technology.²⁹ The executive order directed DOJ to enter into a contract with the National Academy of Sciences by November 2022, for the purposes of conducting a study on facial recognition technology that includes an assessment of privacy, civil rights, and civil liberties concerns. The executive order also calls for DOJ, DHS, and the White House Office of Science and Technology Policy to lead an interagency effort to identify best practices for law enforcement agencies using facial recognition technology, and issue a report describing any resulting policy changes by November 2023.

²⁷Department of Homeland Security, Acting Secretary, *Information Regarding First Amendment Protected Activities*, (Washington, D.C.: May 17, 2019). This memorandum notes that under the Privacy Act of 1974, all DHS personnel are prohibited from maintaining records that describe how a U.S. citizen or legal permanent resident exercises his or her First Amendment rights, "unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

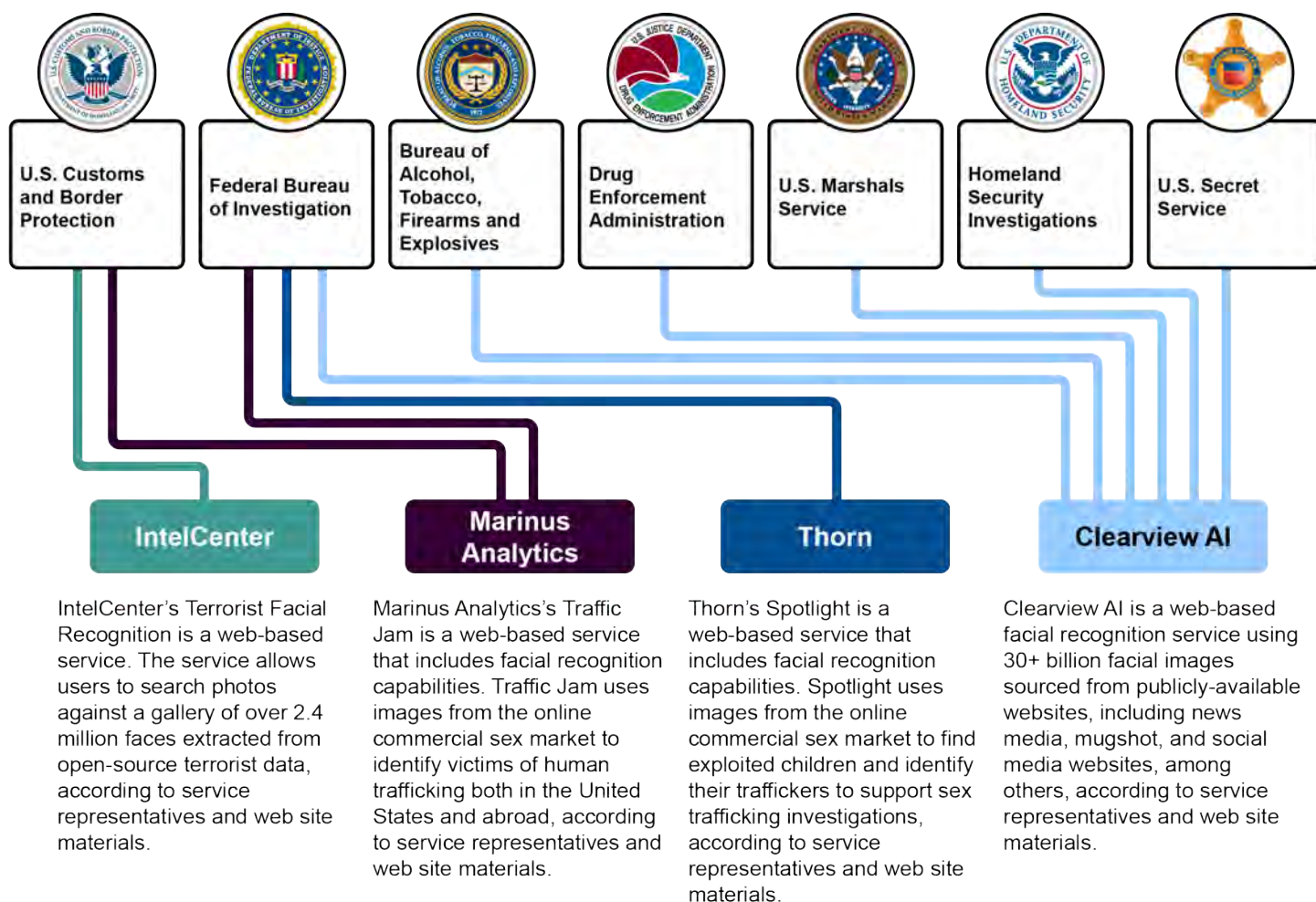
²⁸See H.R. No. 117-97, at 60 (2021) (accompanying Pub. L. No. 117-103, 136 Stat. 49 (2022) and incorporated by reference in the explanatory statement for the Act, 168 Cong. Rec. H1772 (2022)). The committee report directed DOJ to develop ethical policies and required that DOJ report not later than 90 days after the enactment of the Consolidated Appropriations Act on the status of establishing such policies, but did not specify a deadline for the completion of these policies.

²⁹Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

Federal Law Enforcement Agencies Used Four Facial Recognition Services to Support Criminal Investigations

The seven federal law enforcement agencies in our review—ATF, CBP, DEA, FBI, HSI, the Marshals Service, and the Secret Service—reported using four different facial recognition services in total to support criminal investigations from October 2019 through March 2022 (see figure 2). These services gather photos from various sources, such as social media and mugshot websites. In addition, some of these services support certain types of criminal investigations. For example, FBI told us it used Marinus Analytics’s Traffic Jam service to support human trafficking investigations. Figure 2 provides more information about the four services used by the law enforcement agencies in our review.

Figure 2: Facial Recognition Services Used by Selected Federal Law Enforcement Agencies to Support Criminal Investigations from October 2019 through March 2022



Source: GAO analysis of facial recognition service information. | GAO-23-105607

DHS and DOJ officials stated that, as of April 2023, these law enforcement agencies had limited their use of facial recognition services in criminal investigations to conducting identification searches to generate investigative leads, or to help identify potential victims in specific investigations such as human trafficking cases. Additionally, HSI officials told us that within ICE, only HSI has used Clearview AI to support criminal investigations, and that ICE has not used this service in immigration law enforcement or removal operations.

CBP officials told us the agency does not lead criminal investigations but may develop and share information in support of other agencies' criminal investigations. For example, CBP officials stated that they have used facial recognition services to identify potential terrorists, transnational criminals, and individuals who pose a higher risk of violating U.S. law. If CBP identifies something criminal in nature, officials stated that they would refer the information to other law enforcement agencies to conduct criminal investigations, such as HSI.

Six agencies with available data reported conducting approximately 63,000 searches using facial recognition services from October 2019 through March 2022 in aggregate—an average of 69 searches per day.³⁰ We refer to the number of searches as approximately 63,000 because the aggregate number of searches that the six agencies reported is an undercount.³¹ Specifically, the FBI could not fully account for searches it conducted using two services, Marinus Analytics and Thorn.³² Additionally, the seventh agency (CBP) did not have available data on the number of searches it performed using either of two services staff used.³³ Figure 3 provides information on the number of searches agencies reported conducting during this time period, to the extent this information was available.

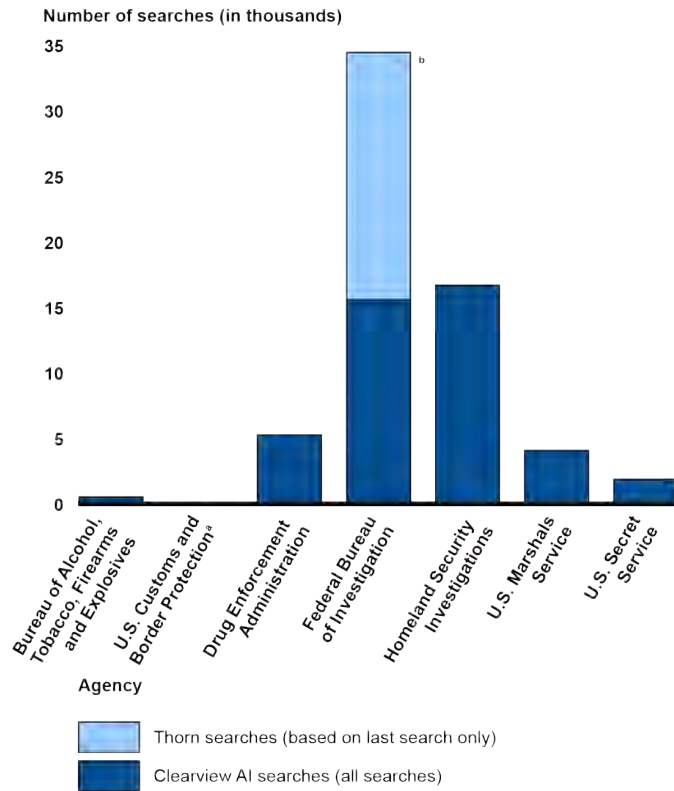
³⁰For this analysis, we defined a search as any instance of comparing a probe photo to a facial recognition service's gallery of photos. Additionally, when an agency searched the same probe photo multiple times but at different points in time, we included each individual search in our count. For instance, if an agency conducted three searches on the same probe photo at different times or dates, we included all three searches in our count.

³¹It is difficult to determine the overall extent to which agencies use facial recognition services, in part, because of variation in how facial recognition services and agencies using those services track the number of searches conducted by agency staff. Additionally, in 2021, we found that some agencies did not track what facial recognition systems staff used and therefore agencies may not have a complete list of facial recognition searches on untracked systems (see [GAO-21-518](#)).

³²Specifically, neither the FBI nor Marinus Analytics tracked the number of searches staff conducted during this time. Additionally, Thorn, only tracked the last time the agency searched using a specific probe photo, and not each time the agency searched using that same probe photo. Marinus Analytics representatives told us that the service did not track the number of facial recognition searches, but it would be able to establish the capability to track searches upon the request of a client organization.

³³CBP officials were unable to provide information on the number of facial recognition searches staff conducted during this time because neither the agency nor the services tracked this information.

Figure 3: Reported Number of Searches That Federal Agencies Conducted Using Facial Recognition Services, Based on Available Data from October 2019 through March 2022



Source: GAO analysis of data provided by agencies and facial recognition services. | GAO-23-105607

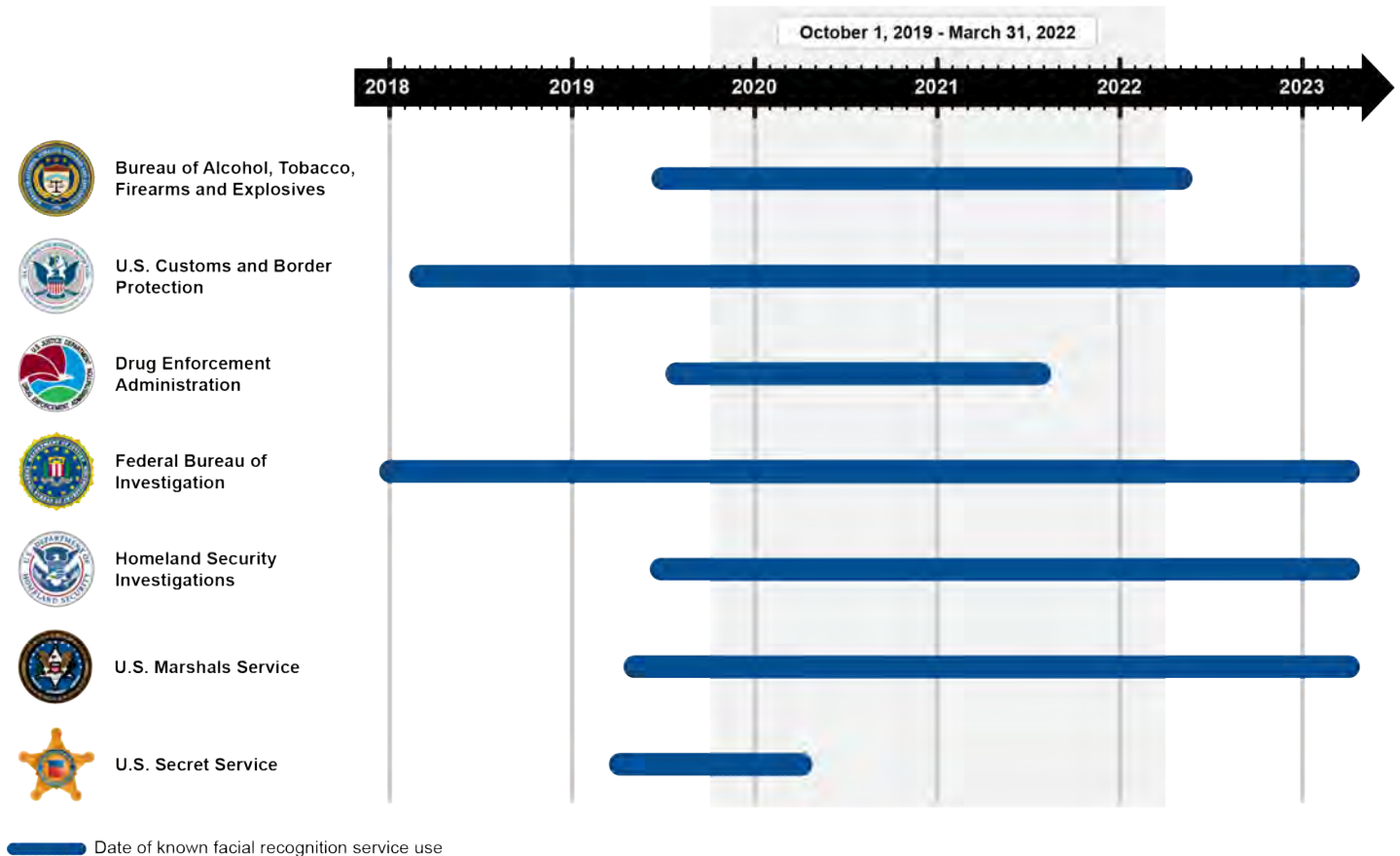
Note: For this analysis, we defined a search as any instance of comparing a probe photo to a commercial or nonprofit facial recognition service's gallery of photos. Additionally, when an agency searched the same probe photo multiple times but at different points in time, we included each individual search in our count. For instance, if an agency conducted three searches on the same probe photo at different times or dates, we included all three searches in our count. The number of searches conducted in this time period may be incomplete. For example, in 2021, we found that some agencies did not track what facial recognition systems staff used and therefore agencies may not have a complete list of facial recognition searches on untracked systems (see [GAO-21-518](#)).

^aCBP officials were unable to provide information on the number of facial recognition searches staff conducted on the two services it used during this time—IntelCenter and Marinus Analytics—because neither the agency nor the services tracked this information. CBP officials acknowledged that staff used two services with facial recognition capabilities.

^bThe number of searches that FBI reported conducting in this time period is an undercount. This is because the FBI could not fully account for searches it conducted using two services, Marinus Analytics and Thorn. Specifically, the figure does not include searches for Marinus Analytics because neither the FBI nor Marinus Analytics tracked the number of searches staff conducted on the service. Additionally, Thorn only tracked the last time the agency searched using a specific probe photo, and not each time the agency searched using that same probe photo.

Our review included facial recognition services that agencies used from October 2019 through March 2022, but some agencies began using these services before this period, and continued to use them after. For example, CBP began using IntelCenter services in 2018 and continued to use this service as of April 2023. Further, as of April 2023, four of the seven agencies in our review continued to use facial recognition services, including FBI, CBP, HSI, and the Marshals Service. However, as of April 2023, ATF, DEA, and the Secret Service reported that they had halted their use of such services. See figure 4.

Figure 4: Selected Federal Law Enforcement Agencies' Reported Use of Facial Recognition Services



Source: GAO analysis of agency information. | GAO-23-105607

Note: Our review only included commercial and nonprofit facial recognition services that agencies reported using from October 1, 2019 to March 31, 2022 (see gray shading in figure). Agencies reported using four services during this time period. The timeline ranges from January 2018 through April 2023 because agencies may have used these four services prior to October 1, 2019 and continued to use the services after March 31, 2022.

For agencies that continued to use selected services after March 31, 2022, we collected data through April 12, 2023, the most recent data available at the time of our review. Additionally, in 2021, we found that some agencies did not track what systems staff used, and not all agencies have taken actions to address this issue (see [GAO-21-518](#)). Further, the timeline does not include agencies' use of government-owned facial recognition services, or commercial and nonprofit services that agencies stopped using prior to October 1, 2019, or began using after March 31, 2022.

According to agency training materials and officials, law enforcement agencies have used facial recognition services during criminal investigations to help identify relevant individuals, including both suspects and victims. See figure 5.³⁴

Figure 5: Homeland Security Investigations Agent Working to Identify Suspected Child Abusers and Victims



Source: Josh Denmark/ U.S. Immigration and Customs Enforcement. | GAO-23-105607

³⁴ATF officials noted that as of April 2023, ATF staff were not directly accessing facial recognition services. However, these officials noted that ATF routinely partners with state and local law enforcement agencies who may use such services during a joint investigation. We discuss agencies' ongoing use of the technology in greater detail later in this report.

For example:

- ICE training material indicates that HSI staff worked on a task force that used facial recognition services to help identify an individual suspected of involvement in the production of child sexual abuse materials. Specifically, according to HSI training documents, HSI investigators in the Cyber Crimes Center first extracted an image of the suspect's face from the child sexual abuse materials. Task force investigators then uploaded this photo to a facial recognition service. One of the potential matches for this photo was linked to an image on a public social media profile. Using this information, in conjunction with other investigative efforts, task force investigators were able to identify, locate, and arrest the suspect. According to the U.S. Attorney's Office, this individual pled guilty to federal charges of sexual exploitation of children and possession of child pornography and was sentenced to 35 years in prison.³⁵
- ATF officials provided another example of the use of facial recognition services. According to the officials, an ATF task force investigated the suspected arson of a Pennsylvania State Police vehicle in Philadelphia. ATF investigators obtained video footage of a suspect, and uploaded images from this footage to a facial recognition service. One of the potential matches included a link to a public social media profile, which showed the individual was in Philadelphia on the day of the suspected arson. The profile also included the individual's cell phone number. ATF investigators obtained a search warrant to review location information from the individual's cellphone. Based on the location data, ATF investigators determined the suspect was at the location of the crime when it occurred. According to ATF officials, the individual was ultimately arrested, confessed to arson, and was sentenced to 364 days in jail.

³⁵Department of Justice, U.S. Attorney's Office for the District of Nevada, "Argentine Citizen Sentenced To 35 Years In Prison For Child Sexual Exploitation And Distribution Of Child Pornography Over The Dark Web," (Las Vegas, NV: Sept. 16, 2020).

Agencies with Available Data Reported Conducting About 60,000 Facial Recognition Searches Before Requiring Training

All seven agencies in our scope initially used facial recognition services without requiring staff to take training on topics such as how facial recognition technology works, what photos are appropriate to use, and how to interpret results. Some agencies required general privacy training for all staff, and made optional facial recognition training available to staff, both of which may have benefited staff using facial recognition services. However, we found that cumulatively, agencies with available data reported conducting about 60,000 searches—nearly all of the roughly 63,000 total searches—without requiring that staff take training on facial recognition technology to use these services.³⁶ While some agencies have since implemented training requirements, others have not assessed whether training would be beneficial. Additionally, although the FBI determined that training is needed, the agency has not yet implemented a training requirement, and did not provide clear documentation to stakeholders about the status of its training requirement. Finally, in our review of FBI records, we found that only about 5 percent of FBI staff that accessed one facial recognition service had taken training.³⁷

Two of Seven Agencies Have Implemented Training Requirements Specific to Facial Recognition Services

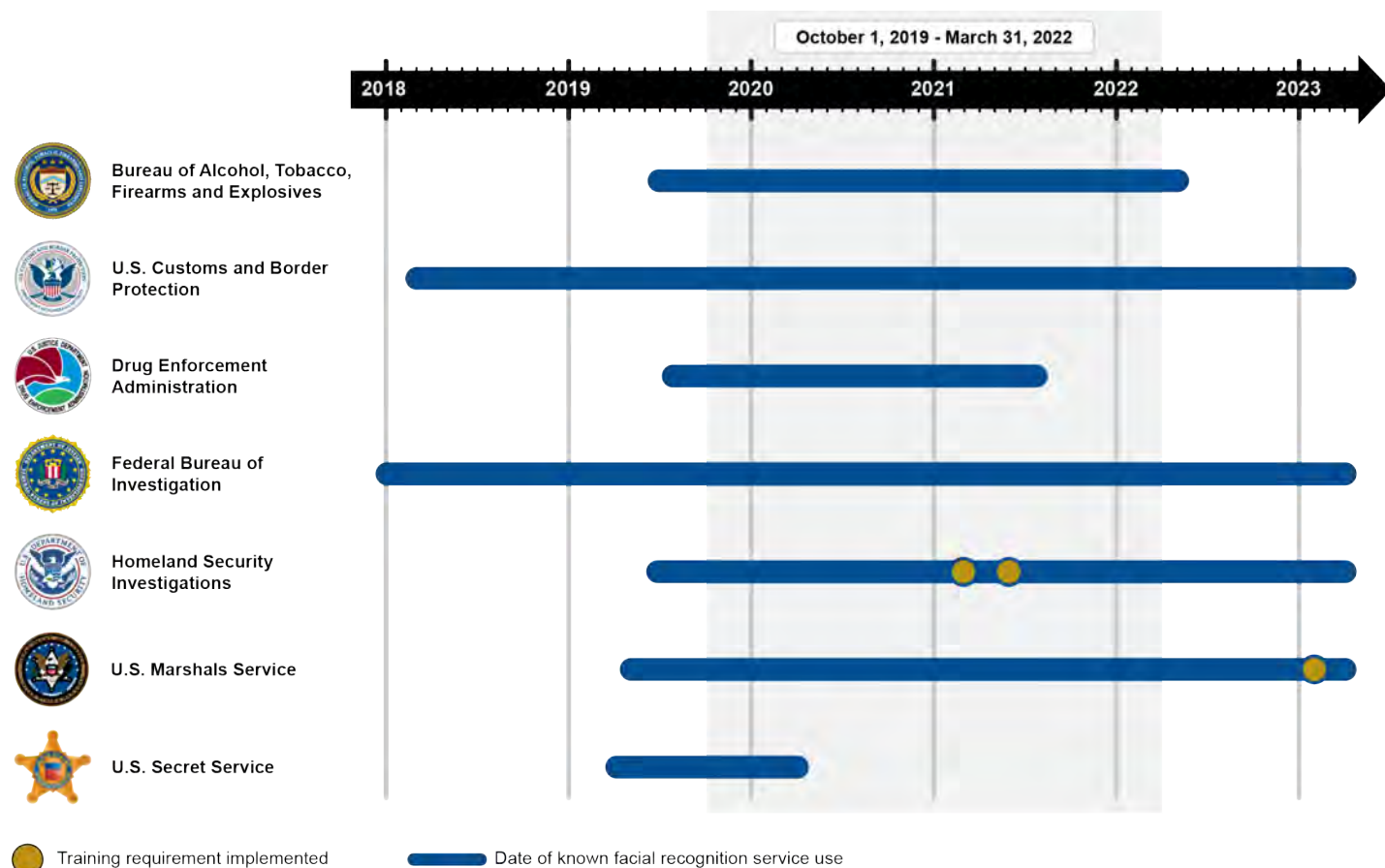
From October 2019 through March 2022, seven agencies used facial recognition services to support criminal investigations. During this time period, one agency—HSI—required staff to take facial recognition training prior to using services, while the other six agencies did not have requirements in place. In February 2023, the Marshals Service also implemented training requirements for staff. Among the remaining agencies that did not have training requirements, CBP and FBI continued to use the services and three agencies—ATF, DEA, and the Secret Service—as of April 2023 had halted their use of these services.³⁸ Figure 6 illustrates when agencies implemented training requirements, and when they began using the four facial recognition services mentioned earlier in this report.

³⁶As discussed earlier in this report, there are limitations associated with the number of searches agencies reported conducting.

³⁷The three remaining agencies in our review—ATF, DEA, and the Secret Service—did not require staff to complete training but had halted their use of facial recognition services at the time of our review (i.e., as of April 2023).

³⁸ATF, DEA and Secret Service officials told us that their headquarters officials were unaware that staff were using these services because staff were using free trial accounts. They said they directed staff to discontinue use of these services after discovery. We discuss this in greater detail later in this report.

Figure 6: Selected Law Enforcement Agencies' Implementation of Training Requirements to Use Facial Recognition Services, as of April 2023



Source: GAO analysis of agency information. | GAO-23-105607

Note: This timeline represents agencies' use of commercial and nonprofit facial recognition services and training requirements to use such services between October 1, 2019 through March 31, 2022 (see gray shading in figure). The timeline ranges from January 2018 to April 2023 because agencies may have used these four services prior October 1, 2019 and continued to use these services after March 31, 2022. For agencies that continued to use selected services after our scope ends, we collected data as of April 12, 2023, the most recent data available at the time of our review. We assessed the extent to which agencies had implemented training specifically required for using facial recognition services, and did not assess requirements for more general training that agency staff may receive, such as general privacy training.

HSI. In 2021, HSI implemented two training requirements that staff must complete prior to using Clearview AI. HSI began requiring the first course, *ICE Use of Facial Recognition Services*, in March 2021.³⁹ This course, which is about three and a half hours in length, covers ICE policies for using third party facial recognition services and best practices for using such services. According to HSI officials, this training also provides information on the capabilities and limitations of facial recognition technology more generally as well as safeguards to help reduce errors and misuse. In addition, the training covers HSI staff responsibilities for protecting individuals' privacy, civil rights and civil liberties when using these services. For example, according to course materials we reviewed, the training covers ICE's policies designed to help avoid discrimination and ICE's policy limiting the collection of probe photos in certain contexts, such as participation at events protected by the First Amendment (e.g., protests).⁴⁰

In addition, officials stated that HSI began requiring that staff using Clearview AI take a second course in July 2021. The *Clearview AI Facial Recognition Tool* course is a one-hour virtual training that provides information on how to use Clearview AI, including how to submit a probe photo and how to record the use of facial recognition searches in HSI tracking sheets and case files.⁴¹

³⁹ICE established this requirement when the agency issued its *Use of and Access to Third Party Facial Recognition Services* memo in January 2021. The memo states that all staff must take and electronically certify that they completed the training course prior to using facial recognition services. U.S. Immigration and Customs Enforcement, Acting Executive Associate Director, *Use of and Access to Third-Party Facial Recognition Services*, Memorandum to All Homeland Security Investigations Personnel (Washington, D.C.: January 15, 2021). HSI officials stated they began enforcing this requirement two months later, in March 2021, when ICE made staff aware of the training requirement.

⁴⁰In particular, the training notes that ICE may not collect probe photos based solely on an individual's religious, political, social views or activities, race, ethnicity, citizenship, place of origin, age, disability, gender identity, or sexual orientation. Additionally, the training reiterates ICE's policy that staff may not collect probe photos based solely on an individual's participation in a noncriminal organization or event protected by the First Amendment.

⁴¹For example, HSI staff are to log certain information on the use of any commercial service in agency tracking sheets. This information includes the name of the service used, the date it was searched, the case number associated with the search, the number of probe photos submitted, and the results of the search, among other things. In addition, staff are to record the results of all facial recognition searches in the relevant case file and the associated report of investigation. U.S. Immigration and Customs Enforcement, *Clearview AI Facial Recognition Tool* (Washington, D.C.: July 9 2021).

Marshals Service. The Marshals Service recommended staff complete training as a best practice, but has since made such training required. According to officials, in February 2021, the Marshals Service began recommending staff complete training to use facial recognition services, but did not require staff to do so. In February 2023, the Marshals Service implemented a training requirement for staff using facial recognition services.⁴² Specifically, staff must complete Clearview AI's virtual training session prior to initially using the service, and complete Clearview AI's refresher training annually.⁴³

Marshals Service officials stated that this training, which is about four hours in length, provides an overview of the functions of Clearview AI. For example, officials stated that the training provides information on how to navigate and interpret possible matches on the service.⁴⁴ Further, officials stated that as part of the training, the service runs example searches and reviews the results with staff to help them understand how to interpret search results appropriately.

The Marshals Service has also taken steps to limit the number of staff that use the service. Specifically, the Marshals Service reached out to Clearview AI to suspend accounts of staff that were no longer using or did not have a need for using the service. This reduced the number of staff with active accounts from 103 to three. Based on our review of training

⁴²In February 2023, the Marshals Service implemented training requirements and a process to help ensure compliance with these requirements. Given that the Marshals Service implemented these requirements as our audit was underway, we did not assess the agency's compliance process.

⁴³The Marshals Service implemented training requirements by issuing a memorandum in February 2023. The memorandum states that all staff that use Clearview AI must complete Clearview AI's initial virtual training session prior to using the service and complete the service's virtual refresher session annually. The memorandum also requires that staff take agency-provided general privacy training. Among other things, officials stated that this training provides a general overview of privacy and civil liberties, their historical abuses, and staff obligations to protect privacy and civil liberties. U.S. Marshals Service, *Clearview AI Training Requirements* (Washington, D.C. Feb. 6 2023).

⁴⁴Marshals Service officials stated that this includes training on how to interpret the degree of confidence the Clearview tool assigns to a potential match.

records, as of February 2023, all three staff that had access to Clearview AI completed the required training.⁴⁵

FBI. As of April 2023, FBI did not require staff to complete training to use any of the three facial recognition services it uses—Clearview AI, Thorn or Marinus Analytics. FBI officials stated that although the agency did not require staff to complete training prior to using facial recognition services, they intend to develop such a requirement. We discuss this later in our report. Although not a requirement, FBI officials said they recommend (as a best practice) that some staff complete FBI's *Face Comparison and Identification Training* when using Clearview AI. The recommended training course, which is 24 hours in length, provides staff with information on how to interpret the output of facial recognition services, how to analyze different facial features (such as ears, eyes, and mouths), and how changes to facial features (such as aging) could affect results.⁴⁶ However, the recommendation does not apply to other FBI units using Clearview AI, or to staff using Thorn or Marinus Analytics. According to FBI officials, the agency has been using the facial recognition capabilities of Thorn and Marinus Analytics since 2018, when the capabilities were added to both services.

CBP. CBP does not require staff to take facial recognition training to access the two services it uses: IntelCenter and Marinus Analytics' Traffic Jam. According to officials, this is in part because they believe staff rarely use the facial recognition capabilities of either service, and instead predominantly use other features available through these services.⁴⁷ Additionally, CBP officials stated that the agency requires all staff to complete privacy training, and that staff could have taken facial comparison training as part of training for identifying fraudulent documents.

⁴⁵We reviewed training records that showed all three staff completed the required trainings. Marshals Service officials stated all agency staff that would like probe photos searched against the Clearview AI gallery in support of an investigation must now work with one of the three trained staff. These three staff will conduct the searches and review results on behalf of the requestor, according to the agency officials.

⁴⁶Federal Bureau of Investigation, *Face Comparison and Identification Training* (Washington, D.C.: Revised Dec. 2020).

⁴⁷CBP officials stated that staff primarily use IntelCenter for its news alerts, and primarily use Marinus Analytics for its feature that aggregates online advertisements to help CBP gather information on certain criminal investigations. However, as we discuss later in the report, CBP does not track the extent to which the agency uses these services.

ATF, DEA, and Secret Service. ATF, DEA, and the Secret Service used Clearview AI during the period of our review, but did not require staff to complete training. Combined, these agencies conducted roughly 7,700 searches during the period of our review. Officials with all three agencies told us that, as of April 2023, they had halted their use of these services.

Most HSI Staff Completed Training, but HSI Could Better Monitor Whether Staff Take Training

Within ICE, HSI established a process to help ensure staff complete required training prior to using facial recognition services. We found that most staff completed this training before using facial recognition services. However, some staff did not complete the training. We reviewed training records from March 4, 2021—when HSI implemented its first training requirement—through March 31, 2022. We found that 106 HSI staff used Clearview AI, and 15 of those staff did not complete the required training prior to conducting searches (see table 2).⁴⁸

Table 2: Training Status of Homeland Security Investigations Staff That Conducted Facial Recognition Searches on Clearview AI from March 4, 2021 through March 31, 2022

Training Status	Number of Staff	Number of Searches Conducted by Staff	Percentage of Total Searches Conducted by Staff
Trained Staff	91	2,120	79%
Untrained Staff	15	569	21%
Total	106	2,689	100%

Source: GAO analysis of agency data. | GAO-23-105607

Note: We considered staff trained if they completed all required training prior to conducting searches, and untrained if they had not completed all training requirements prior to conducting searches. Of the 15 untrained staff, 11 completed the agency’s training requirements (though after conducting searches without such training), and four had not completed the training requirements as of March 31, 2022.

HSI officials told us that the official responsible for administering Clearview AI accounts is to review proof that staff complete the required training, and then provide the fully trained staff access to the service. HSI officials stated that they were unaware of any staff using Clearview AI without having completed the necessary training requirements. In January 2023, officials also told us HSI did not conduct periodic reviews to ensure that staff using Clearview AI had met training requirements. In addition,

⁴⁸We analyzed training records from March 4, 2021 through March 31, 2022 to determine the number of trained and untrained staff. Specifically, we reviewed the date each individual completed training. We considered staff trained if they completed all required training prior to conducting searches, and untrained if they had not completed all training requirements prior to conducting searches.

HSI officials stated that the agency had not evaluated the current approval process to ensure it is working as intended.

As previously described, ICE issued a memorandum that established a training requirement for staff using facial recognition services. *Standards for Internal Control in the Federal Government* states that management should design and implement controls to help achieve agencies' objectives, which, in this case, is to ensure only trained staff use facial recognition services. Further, the internal control standards state that management should periodically monitor the internal control system and evaluate results to help ensure controls are working as intended.⁴⁹

Since we conducted our initial audit work, HSI officials have taken steps to improve staff adherence to training requirements. Specifically, HSI officials told us that the agency conducted a one-time review of all staff using Clearview AI to determine whether staff received required training and whether staff should still have access to the service. As a result of this one-time review, HSI officials reported that they were able to ensure that all staff using Clearview AI as of July 2023 had completed training. Officials also stated that they intend to conduct additional reviews, but had not established or implemented a process for periodically monitoring whether staff have completed training requirements.

ICE has highlighted the importance of its training to help reduce errors and inappropriate use of facial recognition technology by staff. For example, the *ICE Use of Facial Recognition Services* training course teaches staff about common issues in probe photos (e.g., photos with poor resolution or with part of the face obstructed) that could cause errors when using them, and how to reduce these errors. The agency has developed a process to help ensure staff take the required training, and we found that many staff followed this process. However, HSI has not established or implemented a process to periodically review whether all staff with access to facial recognition services received required training. For example, as noted earlier, our review found that 15 staff had conducted over 500 searches before completing the required training. HSI officials took the positive step of conducting a one-time review of staff training and access to Clearview AI. However, without establishing and implementing a process to periodically monitor whether staff using facial recognition services have completed training, HSI faces a continued risk that untrained staff may use facial recognition services.

⁴⁹[GAO-14-704G](#).

Key FBI Stakeholders Were Not Given Clear Documentation on Training Requirements

Federal government officials and others have emphasized the importance of training to help prevent potential abuse of facial recognition technology and increase public confidence in the technology. For example, the FBI has emphasized the importance of facial recognition training, and FBI officials told key internal stakeholders, including the AI Ethics Council and the Privacy and Civil Liberties Unit, that certain staff must take training to use one facial recognition service (Clearview AI).⁵⁰ However, FBI officials told us that while the agency recommends that staff in one unit take training to use a facial recognition service, it does not require any staff that use facial recognition services to take training, and we found that few staff did so. Additionally, FBI officials told us they intend to implement a training requirement, but the agency has not yet done so.

In February 2022, program officials provided documentation to the FBI AI Ethics Council to review the use of Clearview AI by a specific FBI unit.⁵¹ The documentation stated that staff in the unit must take training to use Clearview AI.⁵² In particular, the AI Ethics Council Intake Questionnaire—used by the Council to help it holistically evaluate an AI use case against ethical principles—notes that these staff must receive training to ensure they understand how to use AI systems, like facial recognition services, and the limitations of such systems. In response to this questionnaire, FBI program officials reported that staff in this one unit take the agency’s

⁵⁰See, e.g., *The Use Of Facial Recognition Technology By Government Entities and the Need for Oversight of Government Use of this Technology Upon Civilians: Hearing before H. Comm. on Oversight and Reform*, 116th Cong. (2019) (statement of Kimberly J. Del Greco, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation). In this testimony, FBI stated that every facial recognition search—including facial recognition results received from partners—is reviewed and evaluated by trained FBI examiners to ensure the results are consistent with FBI standards. FBI officials told us that this testimony focused on FBI’s Criminal Justice Information Services use of facial recognition services, which does not include Clearview AI.

⁵¹According to FBI officials, the agency’s AI Ethics Council helps the FBI identify, review, and assess new and existing AI deployed and operating in support of agency missions. FBI’s Privacy and Civil Liberties Unit within the Office of General Counsel is responsible for, among other things, providing legal advice and counsel on compliance with federal law protecting individual privacy, and best practices to achieve an appropriate balance between protecting civil liberties and facilitating FBI activities. Officials stated that the AI Ethics Council evaluated whether FBI’s AI use cases and systems comply with ethical principles in accordance with Executive Order 13960. Exec. Order No. 13960, § 3(a)-(i), 85 Fed. Reg. 78,939 (Dec 3, 2022).

⁵²FBI officials told us that this documentation only relates to staff in one operational unit of the FBI. However, we found that staff on other FBI units used the service, which we discuss later in this section.

Face Comparison and Identification Training course, in addition to training provided by the service. Additionally, the initial privacy review, completed by program officials and submitted to FBI's Privacy and Civil Liberties Unit, similarly states that training is required for staff in this one unit using Clearview AI. However, FBI communicated to staff in this unit that training to use Clearview AI is a best practice, rather than a requirement. Additionally, FBI officials told us that the agency did not have a training requirement for any staff using any facial recognition service.

Standards for Internal Control in the Federal Government states that agencies should internally communicate the necessary quality information to achieve its objectives.⁵³ The AI Ethics Council found one unit's use of Clearview AI to be ethical in part based on documentation that staff in this unit were required to take training to use the service, when no such requirement exists. Similarly, the Privacy and Civil Liberties Unit approved an initial privacy review for Clearview AI that erroneously stated that training requirements were in place. However, as of April 2023, FBI officials had not provided clear documentation to these key internal stakeholders on the status of the training requirement. By clarifying the status of the agency's training requirement for staff using Clearview AI to the AI Ethics Council and the Privacy and Civil Liberties Unit, the FBI would allow these stakeholders to fully evaluate whether the use of this service complies with FBI ethical and privacy standards.

FBI officials recommended training as a best practice for staff in one unit of the FBI; however, multiple units used facial recognition services without either a requirement or recommendation of training. As we discussed earlier, according to records we analyzed, only 10 of 196 staff from across FBI who accessed Clearview AI had completed training.⁵⁴ Further, we found that the 186 untrained staff included staff in the FBI unit where training was recommended as well as other FBI units.

⁵³[GAO-14-704G](#).

⁵⁴We obtained and analyzed available data on training and FBI Clearview AI accounts to determine the number of trained and untrained staff. Specifically, we reviewed training records for each staff person that completed facial recognition training, and compared that to a list of staff that accessed the facial recognition service. We considered staff trained if they accessed the service and completed the training, and untrained if they accessed the service but did not complete training at all. Further details on our analysis are in Appendix I. FBI officials stated that since we conducted our analysis, additional FBI users of the service had completed training.

FBI officials told us that training would be beneficial for staff and that they intend to make training a requirement for all staff using facial recognition services. However, FBI staff have used facial recognition services included in our review since 2018 and have conducted tens of thousands of searches. In addition, staff continue to use the services without a training requirement in place. *Standards for Internal Control in the Federal Government* state that management should design control activities to achieve objectives and respond to risks.⁵⁵ Implementing a training requirement for staff using facial recognition services could help prevent potential abuses and increase the public's confidence in the agency's use of the technology. Additionally, doing so would help ensure that all staff that use these services understand how to use facial recognition services and their limitations.

CBP Has Not Assessed Whether Staff Would Benefit from Training for Facial Recognition Services

CBP provides staff access to two facial recognition services—IntelCenter and Marinus Analytics. However, CBP does not require staff to complete training on facial recognition technology to access these services, does not know the extent staff use such services for facial recognition searches, or whether training on facial recognition would benefit staff.

CBP officials told us they do not require staff to complete facial recognition training as a condition of receiving access to IntelCenter or Marinus Analytics, because they believe that staff rarely use the facial recognition capabilities of either service. Instead, agency officials stated that staff predominantly use other aspects of these services. For example, officials said staff mainly use IntelCenter for the news alerts, and mainly use Marinus Analytics for its feature that aggregates online advertisements to help CBP gather information on certain criminal investigations. However, CBP officials also acknowledged that staff use the facial recognition capabilities of the services to develop and share information in support of other agencies' criminal investigations. For example, CBP used the facial recognition capability of IntelCenter as part of a joint federal law enforcement task force.

Additionally, the agency does not have information on the number of staff that used the facial recognition capabilities available in either service, or how many facial recognition searches staff conducted from October 2019

⁵⁵[GAO-14-704G](#).

through March 2022.⁵⁶ According to officials, neither the agency nor the services tracked this information. As a result, CBP could not determine the extent that staff used these facial recognition services.⁵⁷

Although there is no specific training required for staff to access either service, CBP told us it requires all staff throughout the agency to complete certain training courses that could benefit users of facial recognition services. For example, CBP requires all staff to complete courses on protecting personal information and records management.⁵⁸ Further, CBP officials told us that staff could have taken face comparison training as part of their general training upon entering the agency. CBP officials also told us it has optional training resources available to staff with accounts.⁵⁹ However, CBP officials told us the agency has not assessed whether staff have the appropriate skills and competencies to use facial recognition services, and whether they would benefit from training beyond the general training required for all CBP staff.

According to our human capital guidance, agencies should assess the skills and competencies a workforce needs to address agency objectives, and identify gaps in those skills and competencies, including gaps that training and development strategies can help address.⁶⁰ This guidance further notes that valid and reliable data are the starting point for such assessments. Similarly, *Standards for Internal Control in the Federal Government* states that management should ensure that information it uses to achieve its objectives is appropriate, current, complete, and accurate.⁶¹

⁵⁶Representatives from both services told us that developing a feature to allow agencies to monitor how many staff use the facial recognition capability would be possible.

⁵⁷In addition, we confirmed with representatives from each service that they could not provide this information either.

⁵⁸CBP officials stated that some staff must also take agency training on integrity awareness and ethics. Further, CBP officials stated that staff could have taken training specific to use of other services, and a three-hour photo comparison training.

⁵⁹For example, Marinus Analytics provides trainings to assist with law enforcement investigations on human trafficking using information from adult services websites, among other topics. Additionally, according to company representatives from IntelCenter, they offer training to help users understand its facial recognition capability, but do not require it.

⁶⁰GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, [GAO-04-546G](#) (Washington, D.C.: March 2004).

⁶¹[GAO-14-704G](#).

Assessing whether training would benefit staff using facial recognition services to develop and share information in support of other agencies' criminal investigations could help CBP obtain assurance that its staff have the skills and competencies to address agency objectives. In addition, CBP could better support such an assessment by determining the extent to which staff use facial recognition services to develop and share information in support of other agencies' criminal investigations (such as number of CBP staff that use the services, and how often they do so).

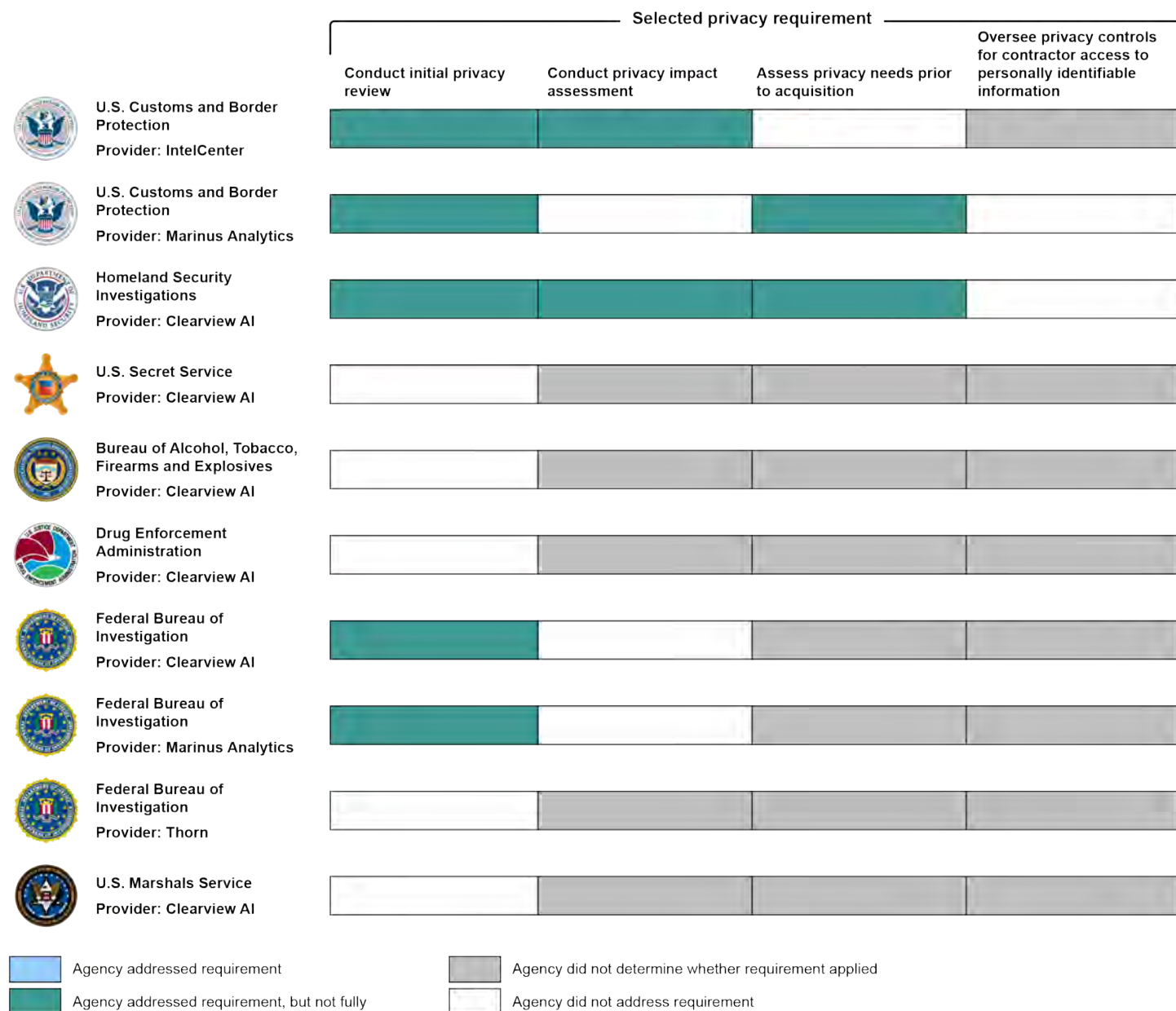
Three of Seven Agencies Took Some Steps to Address Selected Privacy Requirements

We found that three of the seven agencies in our review addressed some privacy requirements related to facial recognition services, which helped them identify privacy risks and develop related mitigation strategies. However, we also found several instances where these agencies did not address privacy requirements. For example, two of these agencies did not complete privacy impact assessments for facial recognition services they used, or only completed them after years' of using the service. Additionally the remaining four agencies did not fully address any privacy requirements. In addition, we found that most agencies had yet to make determinations about whether certain privacy requirements apply to their use of a facial recognition service.

As discussed earlier, DHS and DOJ have requirements generally applicable to the use of facial recognition services to help prevent the inappropriate collection, use, and release of PII including: (1) conducting an initial privacy review prior to acquiring the service; (2) conducting a privacy impact assessment (PIA) prior to acquiring the service; (3) assessing privacy needs prior to acquisition; and (4) overseeing privacy controls for contractor access to PII. We reviewed the extent to which the seven agencies followed these four privacy requirements before sending photos of individuals to facial recognition services.⁶² Figure 7 (below) and appendix II provide a detailed summary of the extent to which agencies addressed these four privacy requirements.

⁶²Our review focused on the facial recognition services used by the seven agencies from October 1, 2019 through March 31, 2022. As discussed previously, both DHS and DOJ guidance identify photos of people as PII, potentially subject to privacy requirements. In addition, not all listed privacy requirements may apply to an agency's use of a facial recognition service. For example, an agency may conclude in its initial privacy review that a privacy impact assessment is not required.

Figure 7: Extent to which Selected Agencies Addressed Selected Privacy Requirements while Using Facial Recognition Services, as of April 2023



Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

Note: For each agency, we reviewed the use of facial recognition services from October 2019 through March 2022. In addition, we determined the extent to which these agencies had addressed the four selected requirements as of April 2023. We considered an agency to have completed a selected privacy requirement if it completed the requirement in accordance with departmental policy. We were

unable to evaluate the extent to which agencies executed certain privacy requirements if the agency had not yet determined whether such requirements applied when we conducted our audit work.

Appendix I provides more information on how we evaluated privacy requirements and appendix II provides additional information on whether each agency met the four selected privacy requirements.

As shown in the figure above, three of the seven agencies in our review—CBP, HSI, and FBI—undertook efforts to address some of the requirements we reviewed. Specifically, CBP and HSI each completed an initial privacy review and associated PIA for facial recognition services they used. In addition, FBI finalized initial privacy reviews for two services it uses. By carrying out these activities, these agencies identified some privacy risks, and developed mitigation strategies to address those risks. For example, in its PIA, HSI identified as a potential privacy risk that HSI staff may submit probe photos to a facial recognition service that are not directly relevant to an ongoing criminal case.⁶³ HSI identified a mitigation strategy that included training HSI staff on the appropriate uses of the technology, requiring staff to document the source of probe photos and the use of facial recognition services in investigative case files, and requiring supervisory review of investigative case files.

In addition, the remaining four agencies in our review—ATF, DEA, the Marshals Service and the Secret Service—did not address the requirement to conduct an initial privacy review and did not determine the applicability of other privacy requirements we reviewed.

As shown in figure 7 above, we found that agencies:

- **Did not address a requirement.** None of seven agencies in our review completed all privacy requirements. For example, both CBP and FBI have determined a need for a PIA for facial recognition services they used; but, despite years of using these services, neither agency had completed the PIAs as of April 2023.
- **Did not determine the applicability of a requirement.** Six agencies—all but HSI—did not determine whether certain privacy requirements applied to their use of facial recognition services. For example, five of the six agencies did not complete initial privacy reviews for services they used—reviews intended to assess whether additional privacy requirements are applicable to the agency's use of a service. Without completing these reviews, the agencies were

⁶³U.S. Immigration and Customs Enforcement, *Privacy Impact Assessment for the ICE Use of Facial Recognition Services (DHS/ICE/PIA- 054)*, (Washington, D.C.: May 13, 2020).

unable to determine the applicability of the remaining privacy requirements.

- **Addressed a requirement, but not fully or in a timely manner.** Three agencies took actions toward addressing a requirement (CBP, HSI, and FBI); however, we found that the agencies did not address these requirements in accordance with departmental policy and guidance. For example, CBP completed the initial privacy review for IntelCenter's services prior to use, in accordance with DHS policy, but did not include a discussion of the service's facial recognition capabilities. Additionally, the initial privacy review indicated that CBP would only download IntelCenter data but we confirmed with both CBP officials and IntelCenter representatives that users must upload photos of individuals to the service to use the facial recognition capabilities. In addition, DHS and DOJ guidance calls for agencies to complete initial privacy reviews and PIAs prior to acquiring and using services that handle PII. We found that only CBP completed these reviews prior to acquiring and using one of its two facial recognition services. HSI and FBI addressed some privacy requirements for certain services they used, but addressed these requirements after they had already begun to use the services.

The four DHS and DOJ agencies that continued to use facial recognition services as of April 2023, had begun to take some, but not all, of the necessary steps to address outstanding privacy requirements. For example, according to CBP officials, CBP intends to publish the Marinus Analytics' PIA before the end of fiscal year 2023. In addition, FBI officials told us that they submitted a PIA for the services it uses to DOJ's Chief Privacy and Civil Liberties Officer for final approval in April 2023. Additionally, the three agencies that used free trials of facial recognition services—ATF, DEA, and the Secret Service—told us they have all taken actions to prohibit staff use of free trials, and had halted their use of these services as of April 2023.

Across the seven agencies we reviewed, program officials told us they did not fully address the privacy requirements, in part, because they (1) did not initially recognize the photos used as PII, (2) did not realize staff transmitted photos to facial recognition services, or (3) did not fully coordinate with privacy officials while acquiring these services. For example, CBP program officials stated they did not consider transmitted photos to facial recognition service providers as PII. ATF headquarters officials stated they were initially unaware ATF staff sent photos to Clearview AI. Additionally, HSI acquisition officials did not incorporate privacy officials' perspectives when making acquisition decisions with

potential privacy implications. Privacy officials we met with stated that they were unaware that some privacy compliance documentation was not fully complete, and stated that they relied on program officials to understand the extent to which PII is used in facial recognition services.

Multiple agency and department offices share the responsibility for ensuring agencies address privacy requirements. For example, program officials are to notify privacy officials when they seek to procure potentially privacy-sensitive technology and work with them to complete initial privacy reviews and privacy impact assessments. Acquisition officials are to coordinate with privacy officials to ensure that required privacy terms are included in contracts, and ultimately implemented. In addition, DHS and DOJ each have department officials responsible for helping their respective agencies and staff comply with laws and policies for protecting privacy, including the requirements we reviewed. Further, DHS and DOJ guidance states that program, privacy, and acquisition officials should coordinate prior to using privacy sensitive technology.⁶⁴ DHS and DOJ officials also emphasized that program officials should coordinate with relevant offices on privacy concerns, even when it may not be initially clear whether PII is directly involved.

Standards for Internal Control in the Federal Government state that management should evaluate and remediate deficiencies.⁶⁵ While most of the agencies continuing to use facial recognition services have begun to take steps to address the outstanding privacy requirements we identified in Figure 7, many of these efforts are incomplete. Additionally, agencies have not updated privacy documentation (initial privacy reviews, privacy impact assessments) that do not include full or correct information on the extent to which contractors may have access to PII. At a broader level, DHS and DOJ privacy offices have yet to work with other relevant offices (e.g., acquisition offices) to determine why agencies did not adhere to

⁶⁴Department of Homeland Security, *Privacy Impact Assessment: The Privacy Office Official Guidance* (Washington, D.C.: June 2010). Department of Justice, Office of Privacy and Civil Liberties, *Initial Privacy Assessment Instructions and Template* (Washington, D.C.: Revised May 2022).

⁶⁵[GAO-14-704G](#).

their respective privacy compliance processes for facial recognition services.⁶⁶

Both DOJ and DHS have noted the importance of adhering to privacy requirements. For example, DOJ has noted that timely completion of privacy impact assessments ensures that privacy protections are built into systems from the start, and not after the fact when they could be far more costly or affect the viability of the project.⁶⁷ Further, DOJ noted that timely completion of these assessments help promote trust between the public and the federal government by increasing transparency of the department's systems and missions. More broadly, DHS has noted that as stewards of data on the citizens it serves it must strive to ensure privacy protection and awareness remain fundamental to its operations.⁶⁸

By taking actions to ensure that agencies continuing to use facial recognition services address outstanding privacy requirements for facial recognition services, and updating existing privacy documentation as appropriate, DHS and DOJ can better ensure that PII shared with facial recognition services (such as probe photos), are not inappropriately disclosed or compromised. Further, DHS and DOJ Privacy Officers could help ensure agencies better comply with privacy requirements in the future by collaborating with agency program, acquisition, and privacy officials to evaluate why agencies did not adhere to their respective privacy compliance processes for facial recognition services—taking into account the results in this report. Conducting such an evaluation and remediating any deficiencies identified through the process could help DHS and DOJ increase transparency of the departments' use of facial recognition services.

⁶⁶Appendix II provides detailed information of the extent to which each of the seven agencies included in our review addressed selected privacy requirements.

⁶⁷Department of Justice, Office of Privacy and Civil Liberties, *Privacy Impact Assessments: Official Guidance*, (Washington, D.C.: Revised July 2015).

⁶⁸Department of Homeland Security, *Privacy Impact Assessments: The Privacy Office Official Guidance*, (Washington, D.C.: June 2010).

Most Agencies Did Not Have Policies Specific to Facial Recognition to Help Protect Civil Rights and Civil Liberties

Of the seven agencies in our review, three had policies specific to facial recognition technology intended to help protect civil liberties and civil rights, and four did not. In addition, DHS has plans to issue new department-wide guidance that, according to the department, will help ensure the protection of civil rights and civil liberties while staff use facial recognition technology. Finally, DOJ officials told us that they also intend to issue a department-wide policy, and have taken steps to do so. However, DOJ has also faced delays in its efforts, and officials told us they did not have a plan with time frames and milestones to issue such a policy.

Officials with HSI, the Marshals Service, and the Secret Service all identified policies or guidance that helped staff ensure the protection of certain civil rights and civil liberties. HSI's policy, first established in January 2021, includes requirements such as limiting the use of such technology to certain criminal investigations.⁶⁹ Specifically, this memorandum states that HSI will use a facial recognition service only for authorized law enforcement purposes relevant and necessary to an ongoing investigation relating to HSI's statutory authorities; or as part of an established HSI program or task force whose use of facial recognition is assessed for its impacts on privacy, civil rights, and civil liberties. Additionally, HSI's policy places explicit limits on the collection of probe photos taken while individuals are exercising their First Amendment rights (such as at protests), among other things.

In addition, the Marshals Service has guidance to staff that limits the use of facial recognition technology to ongoing criminal investigations. For example, the Marshals Service guidance states that all searches conducted in Clearview AI must have a direct nexus to an active fugitive investigation or other authorized criminal investigation, and that possible matches will require further research and investigation.

Finally, the Secret Service had halted its use of facial recognition services in April 2020. However, in April 2023 the Secret Service issued a directive which provides general guidance on using facial recognition services. For example, the directive limits the use of facial recognition services to subjects and victims in established Secret Service investigations under laws the Secret Service has the authority to enforce. In addition, this

⁶⁹U.S. Immigration and Customs Enforcement, Acting Executive Associate Director, *Use of and Access to Third-Party Facial Recognition Services*, Memorandum to All Homeland Security Investigations Personnel (Washington, D.C.: January 15, 2021).

policy only permits the use of facial recognition services that are pre-approved by the agency's Criminal Investigative Division.

The remaining four agencies (FBI, CBP, ATF, and DEA) did not have guidance or policies specific to facial recognition technology that addressed civil rights and civil liberties. However, officials with FBI and CBP told us staff must abide by more general guidance that helps ensure the protection of civil rights and civil liberties during investigatory activities, including when using facial recognition technology. For example, FBI officials noted that the Attorney General's Guidelines for Domestic FBI Operations and the FBI's Domestic Investigations and Operations Guidelines provide overarching guidance for all FBI activities, including addressing civil rights and civil liberties during investigatory activities.⁷⁰ Additionally, CBP officials identified a DHS memorandum on protecting First Amendment rights as a source of guidance for staff using facial recognition technology.⁷¹ Among other things, this memorandum notes that DHS personnel are only permitted to collect, maintain, or use information protected by the First Amendment in certain circumstances.⁷²

ATF and DEA had halted their use of facial recognition services at the time of our review. However, these officials noted the agency has general departmental and agency guidance to help ensure the protection of civil rights and civil liberties applicable to all criminal investigatory activities.⁷³

Additionally, DHS officials reported that beginning in May 2022, the DHS Chief Information Officer initiated a working group to develop a department-wide policy to establish responsibilities and requirements for

⁷⁰Additionally, FBI officials noted that one unit in the FBI had identified best practices for their staff to use one facial recognition service, which included practices to help protect civil rights. FBI officials also told us they were working on developing agency-wide policy specific to the use of facial recognition technology.

⁷¹Department of Homeland Security, Acting Secretary, *Information Regarding First Amendment Protected Activities*, (Washington, D.C.: May 17, 2019).

⁷²In particular, this memorandum notes that DHS personnel are not permitted to collect, maintain, or use information protected by the First Amendment unless (1) an individual has expressly granted their consent for DHS to collect, maintain, and use that information; (2) maintaining such information is expressly authorized by a federal statute or (3) the information is relevant to a criminal, civil, or administrative activity relating to a law DHS enforces or administers.

⁷³Because our review focused on the extent to which agencies had developed policies and guidance specific to facial recognition technology to help protect civil liberties and civil rights, we did not evaluate general guidance agencies have to protect civil rights and civil liberties.

the authorized, responsible, and ethical use of face recognition technology, including protections for individual rights. For example, DHS officials told us that they anticipated the policy would (1) address safeguarding privacy, civil rights, civil liberties, (2) identify authorized uses of facial recognition technology, and (3) provide guidelines to help ensure individuals are not targeted based on protected characteristics or protected activities (e.g., First Amendment activities). In May 2023, DHS officials provided us a project plan highlighting anticipated milestones to finalize the policy, including that they anticipated issuing this policy by June 2023. In August 2023, DHS officials stated that DHS Office of General Counsel was reviewing the policy but that they expected the policy to be completed by the end of December 2023. It will be important that DHS has focused attention on completing and implementing the policy by the newly established timeframe.

DOJ has also begun to develop a department-wide facial recognition policy addressing civil rights and civil liberties. In February 2022, DOJ formed a working group charged with determining a need for, and developing, policy on law enforcement's use of facial recognition technology.⁷⁴ DOJ officials stated that this working group was drafting a department-wide facial recognition policy that would include safeguards for civil rights and civil liberties. Officials also stated that they intended to use this policy to address the related congressional report from March 2022.⁷⁵ DOJ officials told us that they did not have a project plan with time frames and milestones for issuing this policy. Previously, in November 2022, they stated they expected to implement the policy in the following months, and in March 2023, DOJ officials stated they expected to finalize the policy shortly.

In April 2023, DOJ officials told us that although they had developed a draft policy, they had changed course, and intended to wait for the study and interagency effort required by Executive Order 14074 to complete before issuing the policy.⁷⁶ As discussed earlier, Executive Order 14074, issued in May 2022, directed DOJ to contract with the National Academy

⁷⁴DOJ officials also said the department formed the working group in part due to our reports since 2016 that have highlighted potential risks and benefits of facial recognition technology.

⁷⁵See H.R. No. 117-97 (2021) (accompanying Pub. L. No. 117-103, 136 Stat. 49 (2022) and incorporated by reference in the explanatory statement for the Act, 168 Cong. Rec. H1772 (2022)). As previously discussed, Congress directed DOJ to develop ethical policies for the use of facial recognition technology.

⁷⁶Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

of Sciences to study facial recognition technology and assess related privacy, civil rights, and civil liberties concerns. Additionally, the executive order calls for DOJ and others to lead an interagency effort to identify best practices for using facial recognition technology, and describe any resulting policy changes for federal law enforcement.

DOJ officials stated that they have begun to take some steps to address the facial recognition directives found in Executive Order 14074. For example, DOJ officials told us that representatives from DOJ, DHS, the White House's Domestic Policy Council, and the Office of Science and Technology Policy held three meetings from October 2022 through February 2023 to address the executive order requirements.

However, some efforts called for in the executive order have been delayed. DOJ officials told us that they had identified funding to address the requirement to develop a study on facial recognition technology, but had not yet awarded the funding to the National Academy of Sciences.⁷⁷ The executive order called on DOJ to enter into the contract by November 2022, and it had not done so as of April 2023. Additionally, the executive order called on the interagency effort to issue a report—using the results of the National Academy of Sciences study—by November 2023. However, as of April 2023, the funding for the study had not yet been awarded, the study had not yet begun, and it is unclear what impact this may have on DOJ's ability to issue their facial recognition policy in a timely manner.

Leading project management practices include that organizations direct and manage project work by developing a project management plan and a project schedule, which notes work activities, their durations, resources, and planned start and finish dates.⁷⁸

DOJ officials have stated that they intend to wait for the completion of the study and interagency effort before issuing department policy on facial recognition technology, which will allow them to leverage information gained during that process. However, without a department-wide facial recognition policy, we found that selected DOJ law enforcement agencies

⁷⁷Specifically, DOJ stated that the department would fund the study through a grant from the National Institute of Justice's fiscal year 2023 appropriations. As of April 2023, the National Institute of Justice was undertaking administrative tasks prior to awarding funding for the study.

⁷⁸Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition* (2017).

continued to use facial recognition technology. DOJ also lacks an implementation plan to ensure it issues its policy upon completion of the Executive Order activities, and has faced delays in those activities.

DOJ officials stated that the department has existing general guidance and policies that apply to the use of facial recognition technology; however, there may also be unique issues raised by the technology that DOJ has not yet addressed through existing policy. For example, in September 2022, DOJ officials told us that they were considering including in their policy guidance on whether a potential match result from a facial recognition system alone would constitute sufficient basis to apply for a search warrant.

Leveraging information gained through the interagency process may help DOJ improve policy on how to safeguard civil rights and civil liberties while using facial recognition technology. However, given uncertainties about when this process will complete, DOJ risks a delay in meeting its own goal of providing a policy to law enforcement on the use of facial recognition technology—a goal that predates the actions required by Executive Order 14074. Developing a plan with time frames and milestones would better position DOJ to issue its policy in a more timely manner upon completion of the executive order activities, thereby supporting staff in safeguarding civil rights and civil liberties while using facial recognition technology.

Conclusions

Facial recognition services offered by commercial and nonprofit entities are tools that DHS and DOJ used to support criminal investigations. While these services may support such investigations, federal government officials and others have also emphasized the importance of training to help prevent potential abuses and increase the public's confidence in the technology. While some agencies have developed training requirements, we found that HSI, FBI, and CBP could take additional steps to help ensure that staff are sufficiently trained.

HSI has a process to ensure staff take required training, but our analysis found that some staff did not complete these requirements. HSI has taken the positive step of undertaking a one-time review of staff adherence to training requirements. However, without establishing and implementing a process to periodically monitor whether staff using facial recognition services complete training requirements, HSI faces a continued risk that untrained staff may use facial recognition services.

The FBI does not require any staff to take training to use facial recognition services, but told key internal stakeholders that training is required for certain staff. Clarifying the status of its training requirement for staff using Clearview AI to the AI Ethics Council and the Privacy and Civil Liberties Unit would better enable the FBI to fully evaluate whether the use of these services follows FBI ethical and privacy standards. In addition, FBI officials said they intend to make training a requirement for all staff using facial recognition services, but have not yet done so. Implementing a training requirement for all staff using facial recognition services to support criminal investigations would better position FBI to help ensure staff understand how to use these services and their limitations.

CBP provides staff access to facial recognition services but does not have information on the number of staff that use the facial recognition services or how often. Further, CBP has not assessed whether staff using facial recognition services to develop and share information in support of other agencies' criminal investigations could benefit from training on facial recognition technology. Such an assessment can help provide CBP assurance that staff have skills and competencies needed to address agency objectives. In addition, determining the extent that staff use facial recognition services to develop and share information in support of other agencies' criminal investigations would provide key information to help CBP conduct the assessment.

All seven agencies in our review sent photos to facial recognition services without fully addressing privacy requirements. Addressing the outstanding privacy requirements identified in this report, and updating existing privacy documentation, would better enable DHS and DOJ to determine whether appropriate privacy safeguards are in place for agencies that continue to use facial recognition services. Further, ensuring privacy, program, and acquisition officials collaborate on an evaluation of components' adherence to the department's privacy compliance process for facial recognition services could help ensure DHS and DOJ better address privacy requirements in the future, thereby increasing transparency in the departments' use of facial recognition services.

Finally, DOJ has taken steps to develop a department-wide facial recognition policy that includes a focus on civil rights and civil liberties, but has not issued it, and some DOJ law enforcement agencies continue to use this technology without specific guidance. DOJ lacks a plan with time frames and milestones for issuing its facial recognition technology

policy. Developing such a plan would better position DOJ to safeguard civil rights and civil liberties while using facial recognition technology.

Recommendations for Executive Action

We are making a total of 10 recommendations, including one to ICE, two to FBI, two to CBP, three to DOJ, and two to DHS:

The Director of ICE should establish and implement a process to periodically monitor whether HSI staff using facial recognition services to support criminal investigations have completed training requirements. (Recommendation 1)

The Director of the FBI should clarify the status of its training requirement for staff using Clearview AI to FBI's AI Ethics Council and the Privacy and Civil Liberties Unit. (Recommendation 2)

The Director of the FBI should implement a training requirement for staff using facial recognition services to support criminal investigations. (Recommendation 3)

The Commissioner of CBP should determine the extent that staff use facial recognition services to develop and share information in support of other agencies' criminal investigations (such as number of CBP staff that use the services and how often they do so). (Recommendation 4)

The Commissioner of CBP should assess whether training would benefit staff using facial recognition services to develop and share information in support of other agencies' criminal investigations, incorporating information on the extent to which staff use such services. (Recommendation 5)

The Attorney General should ensure the Chief Privacy and Civil Liberties Officer works with DOJ components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate. (Recommendation 6)

The Attorney General should ensure the Chief Privacy and Civil Liberties Officer collaborates with component program, acquisition, and privacy officials to evaluate components' adherence to the department's privacy compliance process for facial recognition services—taking into account the results of this report—and to remediate any deficiencies identified during their evaluation. (Recommendation 7)

The Secretary of Homeland Security should ensure the Chief Privacy Officer works with DHS components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate. (Recommendation 8)

The Secretary of Homeland Security should ensure the Chief Privacy Officer collaborates with component program, acquisition, and privacy officials to evaluate components' adherence to the department's privacy compliance process for facial recognition services—taking into account the results of this report—and to remediate any deficiencies identified during their evaluation. (Recommendation 9)

The Attorney General should develop a plan with time frames and milestones for issuing its facial recognition technology policy that addresses safeguards for civil rights and civil liberties. (Recommendation 10)

Agency Comments and Our Evaluation

We provided a draft of this report to DOJ and DHS for review and comment. DOJ concurred with our recommendations and provided technical comments, which we incorporated as appropriate.

DHS provided formal, written comments, which are reproduced in appendix III. In its comments, DHS concurred with our recommendations and described actions taken and planned to address them. Additionally, DHS provided technical comments, which we incorporated as appropriate. In its technical comments, DHS pointed out that our draft recommendations 4 and 5 did not specify that the recommendations were about the extent that CBP staff use facial recognition services to develop and share information in support of other agencies' criminal investigations. We adjusted the language of these recommendations accordingly.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until one week from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Attorney General, and the Secretary of the Department of Homeland Security. In addition, this report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-8777 or goodwing@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink, reading "Gretta L. Goodwin". The signature is written in a cursive style with a large, stylized "G" and "L".

Gretta L. Goodwin
Director, Homeland Security and Justice

List of Requesters

The Honorable Richard J. Durbin
Chair
Committee on the Judiciary
United States Senate

The Honorable Jerrold Nadler
Ranking Member
Committee on the Judiciary
House of Representatives

The Honorable Jamie Raskin
Ranking Member
Committee on Oversight and Accountability
House of Representatives

The Honorable Cory A. Booker
United States Senate

The Honorable Christopher A. Coons
United States Senate

The Honorable Edward J. Markey
United States Senate

The Honorable Ron Wyden
United States Senate

Appendix I: Objectives, Scope and Methodology

This report examines the extent to which selected Department of Homeland Security (DHS) and Department of Justice (DOJ) law enforcement agencies have:

- (1) used facial recognition services to support criminal investigations from October 2019 through March 2022;
- (2) required staff to take training on facial recognition technology to use such services, and ensured compliance with requirements;
- (3) taken steps to address selected privacy requirements for using facial recognition services; and,
- (4) developed policies and guidance specific to facial recognition technology to help protect civil liberties and civil rights.

To address all four objectives, we selected seven agencies within DHS and DOJ that employ law enforcement officers (i.e., law enforcement agencies).¹ We limited our selection to DHS and DOJ agencies because these two departments employ the highest number of law enforcement officers within the federal government, and cumulatively employ more than 80 percent of all federal law enforcement officers.² From there, we identified DHS and DOJ law enforcement agencies that previously reported owning or using facial recognition technology systems in 2020.³

We selected seven agencies that reported owning or using the highest number of systems to include in this review. Within DHS, we selected U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), and the U.S. Secret Service. Within the DOJ, we selected the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), and the U.S. Marshals Service. The seven law enforcement agencies we selected are not representative of all law enforcement agencies.

¹Consistent with our prior work, we define federal law enforcement officers as full-time employees with federal arrest authority who are authorized to carry firearms while on duty.

²Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016 – Statistical Tables*, NCJ 251922 (Washington, D.C.: October 2019).

³GAO, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks*, [GAO-21-518](#) (Washington, D.C.: June 2021).

Our review included agencies that used facial recognition services in support of criminal investigations, including sharing information (e.g., leads). For example, one agency—CBP—told us that it does not lead criminal investigations but has used facial recognition services to develop and share information in support of other agencies' criminal investigations.⁴ We focused exclusively on the use of facial recognition technology services offered by commercial and nonprofit entities (facial recognition services) to build upon our prior reports that reviewed technologies owned and operated by federal agencies.⁵

To address our first objective, we reviewed agency documentation and interviewed agency officials to identify commercial and nonprofit facial recognition services that agencies used from October 2019 through March 2022 to support criminal investigations. We then obtained and analyzed available data to determine the total number of searches that agency staff conducted using these services from October 2019 through March 2022.

We selected this timeframe to overlap with our prior work, and extend to the most recent data available at the time of our analysis. We included reported searches conducted through March 31, 2022, as it was the most recent data available when we conducted our analysis. We previously reported on agencies' use of facial recognition technology from January 2015 through March 2020.⁶ We assessed the reliability of these data by interviewing knowledgeable agency officials and representatives from each service that agencies reported using during this time period. In addition, we tested these data for outliers or obvious errors when possible. The data on the number of searches agencies reported is an undercount. For example, the FBI could not fully account for searches it

⁴CBP officials told us that the agency used facial recognition services primarily of immigration enforcement and border security purposes.

⁵See for example, [GAO-21-518](#); GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, [GAO-21-526](#) (Washington, D.C.: Aug. 2021); GAO, *Facial Recognition: CBP and TSA Are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, [GAO-20-568](#) (Washington, D.C.: Sep 2020); and, GAO, *FACE Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, [GAO-16-267](#) (Washington, D.C.: May 2016, reissued Aug. 2016).

⁶See [GAO-21-518](#).

conducted using two services, Marinus Analytics and Thorn.⁷ Additionally, CBP officials were unable to provide information on the number of searches staff conducted during this time because neither the agency nor the services tracked this information. Therefore, we determined that these data were sufficiently reliable for reporting on the minimum number of searches conducted by agencies during the period of our review.

To address our second objective, we reviewed agency documentation, including policies, guidance, and memorandums, to determine the extent to which agencies required staff to take training on facial recognition technology to use such services.⁸ For agencies with training requirements, we interviewed relevant officials to learn more about the requirements, and how the agency ensures compliance with these requirements. In addition, for these agencies, we reviewed agency documentation such as memorandums of agency policy and training materials.⁹ In addition, because FBI recommended training as a best practice for one unit in the agency, we also reviewed relevant FBI documents.¹⁰

⁷Specifically, neither the FBI nor Marinus Analytics tracked the number of searches staff conducted during this time. Additionally, Thorn, only tracked the last time the agency searched using a specific probe photo, and not each time the agency searched using that same probe photo.

⁸We assessed the extent to which agencies had implemented training specifically required for using facial recognition services, and did not assess requirements for more general training that agency staff may receive, such as general privacy training. We considered a training requirement to be written instruction to staff mandating training as a condition of access to a facial recognition service.

⁹U.S. Immigration and Customs Enforcement, Acting Executive Associate Director, *Use of and Access to Third-Party Facial Recognition Services* (Washington, D.C.: Jan. 15 2021); U.S. Immigration and Customs Enforcement, *Clearview AI Facial Recognition Tool Training* (Washington, D.C.: July 9 2021); U.S. Marshals Service, *Clearview AI Training Requirements* (Washington, D.C.: Feb. 6 2023). We did not evaluate the content of training to ascertain its sufficiency or appropriateness because there are no national training standards for facial recognition technology.

¹⁰Federal Bureau of Investigation, *Face Comparison and Identification Training* (Washington, D.C.: Revised Dec. 2020).

We then evaluated the extent agencies ensured compliance with requirements or recommended best practices.¹¹ Specifically, we compared training records maintained by the agency to a list of staff that used facial recognition services.¹² We considered staff trained if they completed all required or recommended training in place prior to conducting searches, and untrained if they had not completed all training requirements or recommended training prior to conducting searches. Due to limited data available for the FBI, we considered staff trained if they completed training and accessed the service, and untrained if they did not complete training but accessed the service.¹³ We compared the agencies' efforts to ensure compliance with training requirements against agency policies requiring training and *Standards for Internal Control in the Federal Government*, including standards for designing and implementing controls activities, establishing and operating monitoring activities, and internally communicating quality information.¹⁴

If an agency did not require staff to take training but continued to use facial recognition services at the time of our review, we interviewed officials to understand the agency's rationale. We compared agencies' efforts against our human capital guidance and *Standards for Internal Control in the Federal Government*, including the standard for ensuring that information the agency uses to achieve its objectives is appropriate,

¹¹One agency—the Marshals Service did not implement its training requirement until February 2023. Given the short amount of time that has passed since the agency implemented its requirements, we did not assess the agency's compliance process for this training requirement.

¹²To compare HSI training records to Clearview AI search records, we matched record-level training data (staff first and last names and email addresses) to record-level Clearview AI search records (staff first and last names, and each date they conducted a search in our time frame).

¹³To compare FBI training records to search records, we matched record-level training data as of September 30, 2022 (staff first and last names) to summary-level Clearview AI records of staff that accessed the service (staff first and last names) as of August 2022.

¹⁴Specifically, Principle 10 states that management should design control activities to achieve objectives and respond to risks. Principle 12 states that management should implement control activities through policies. Principle 14 states management should internally communicate the necessary quality information to achieve the entity's objectives. Principle 16 states that management should establish and operate monitoring activities to monitor the internal control system and evaluate results. GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

current, complete, and accurate.¹⁵ In addition, we interviewed officials about their intention to implement a training requirement for all staff and compared agencies' efforts against *Standards for Internal Control in the Federal Government*, including the standard that management should design control activities to achieve objectives and respond to risks.¹⁶ We did not assess training requirements for agencies that reported they were not using facial recognition services at the time we conducted our audit work.

For all of the data we used in this objective, we assessed the reliability of the data by interviewing knowledgeable agency officials and company representatives, reviewing existing information about the data systems, and testing these data for outliers or obvious errors. We determined that these data were sufficiently reliable for reporting on the number of trained and untrained staff using facial recognition services during the period of our review.

To address our third objective, we reviewed departmental privacy guidance and agency documentation, such as the DHS and DOJ guidance on implementing aspects of the E-Government Act of 2002.¹⁷ We also reviewed DHS and DOJ acquisitions regulations and policies. Based on our review of these documents, we selected four privacy requirements generally applicable to systems and services that collect personally identifiable information (PII).¹⁸ The four privacy requirements we selected include conducting an initial privacy review, conducting a

¹⁵GAO, *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government*, [GAO-04-546G](#) (Washington, D.C.: March 2004). Specifically, Principle 13 states that management should use quality information to achieve its objectives. [GAO-14-704G](#).

¹⁶Specifically, Principle 10 states that management should design control activities to achieve objectives and respond to risks. [GAO-14-704G](#).

¹⁷Department of Homeland Security, Privacy Office. *Privacy Impact Assessments: Privacy Office Official Guidance*. (Washington, D.C., June 2010). Department of Justice, Office of Privacy and Civil Liberties. *Privacy Impact Assessments: Official Guidance*. (Washington, D.C.: Revised July 2015). The E-Government Act of 2002, Pub. L. No 107-347, § 208, 116 Stat. 2899, 2921 (2002).

¹⁸The specific requirements applicable to DHS's and DOJ's use of facial recognition services can depend on a number of factors, such as legal requirements, departmental policy, privacy risks that agencies identify, and the sensitivity level of PII involved. In addition, there may be other privacy requirements that apply to federal agencies' use of services that collect PII that we did not include in our review.

privacy impact assessment (PIA), assessing privacy needs prior to acquisition, and overseeing privacy controls for contractor access to PII.

We then determined whether agencies addressed the four selected privacy requirements for each facial recognition service used from October 2019 through March 2022. For each requirement, we gathered relevant agency documentation and compared them to agency guidance and policies. Specifically, we reviewed available initial privacy reviews, PIAs, privacy checklists for acquisition, and contract documentation.¹⁹ We also interviewed cognizant agency officials and representatives from facial recognition services to understand the extent to which PII may be transmitted during a facial recognition search.

We considered an agency to have addressed the requirements if the agency completed initial privacy reviews and PIAs in a timely manner (e.g. prior to acquisition) and with correct information on data transmission, data retention, and training. If the agency addressed the requirement late or without full information, we determined that the agency did not fully address the requirement.

We considered an agency to have assessed privacy needs prior to acquisition as required if the agency completed required privacy checklists on time and with accurate information and if contract documentation, such as terms of agreements reflected privacy needs identified during the acquisition process. We considered an agency to have overseen privacy controls for contractor access to PII as required if the agency executed selected terms in contracts with facial recognition service providers.

If an agency did not address a requirement that would help them determine whether other privacy requirements applied, then we could not evaluate the extent to which the agency addressed the remaining requirements. If an agency did not address, or did not fully address privacy requirements, we interviewed agency officials to determine why. Finally, we compared this information to principles in the *Standards for*

¹⁹We also requested relevant documentation from agency officials illustrating the extent to which they executed selected privacy requirements in contracts, such as requiring contractor employees to sign non-disclosure agreements and implement training requirements.

Internal Control in the Federal Government that state that management should evaluate and remediate deficiencies on a timely basis.²⁰

To address our fourth objective, we reviewed a congressional report and executive order related to policies for facial recognition technology.²¹ We also interviewed agency officials and reviewed agency documentation to understand the extent to which agencies had existing policies and guidance that addressed civil rights and civil liberties in the context of facial recognition technology. Specifically, we asked agency officials to identify guidance, memorandums or policies that addressed civil rights and civil liberties in the context of facial recognition technology, or that applied to the use of facial recognition technology.²²

We then interviewed department officials to understand their efforts to develop and implement new department-wide guidance related to civil rights and civil liberties specific to facial recognition technology, and to address the congressional report and executive order. We compared their efforts to leading project management practices.²³

We conducted this performance audit from January 2022 to September 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

²⁰Specifically, Principle 16 states that management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. Principle 17 states that management should remediate identified internal control deficiencies on a timely basis. [GAO-14-704G](#).

²¹See H.R. No. 117-97 (2021) (accompanying Pub. L. No. 117-103, 136 Stat. 49 (2022)); Exec. Order No. 14074, § 13(d)-(e), 87 Fed. Reg. 32,945 (May 25, 2022).

²²We are defining “civil rights” as due process protections and personal rights protected by the U.S. Constitution and federal laws, such as the Civil Rights Act of 1964; and “civil liberties” as the exercise of activities protected under the First Amendment.

²³Project Management Institute, Inc., *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition* (2017). PMBOK is a trademark of Project Management Institute, Inc. The Project Management Institute is a not-for-profit association that, among other things, provides standards for managing various aspects of projects, programs, and portfolios.

Appendix II: Extent to Which Selected Federal Law Enforcement Agencies Took Steps to Address Selected Privacy Requirements

The seven federal law enforcement agencies in our review addressed four selected privacy requirements to varying extents while using facial recognition services.¹ This appendix details the extent to which each agency addressed the four selected privacy requirements.

As discussed earlier, when using facial recognition services, agencies may need to: conduct an initial privacy review; conduct a privacy impact assessment (PIA); assess privacy needs prior to acquisition; and oversee privacy controls for contractor access to personally identifiable information (PII). If an agency determined that a privacy requirement applied, we analyzed the extent to which the agency addressed the requirement. Our review included facial recognition services used between October 2019 and March 2022.

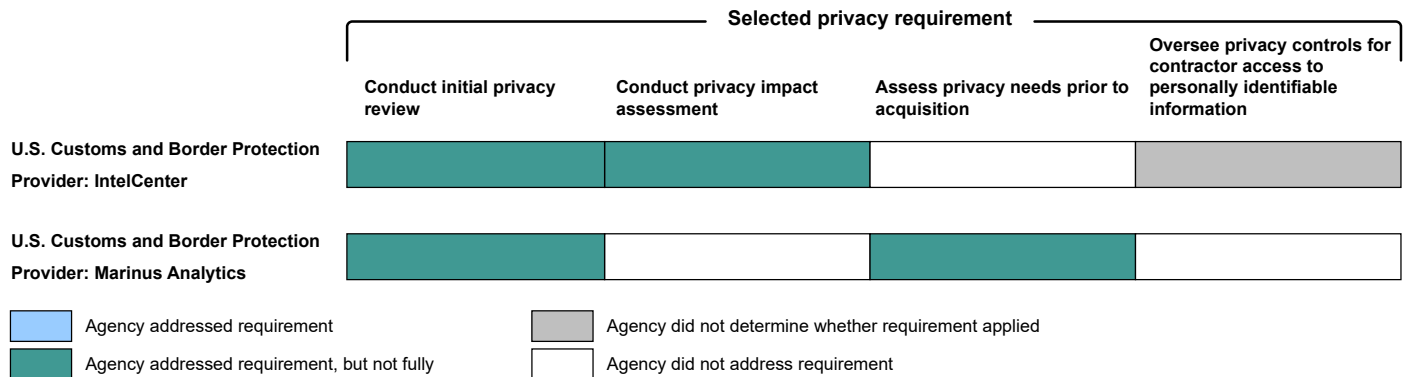
We evaluated the extent to which the agencies addressed these requirements on time (e.g., prior to using the service for criminal investigations). We also evaluated the extent to which agencies' privacy documentation included full and correct information on training requirements and whether PII is transmitted to, or retained by, contractors or contractor systems.

In some instances, an agency did not determine whether a requirement was applicable. For example, if an agency did not complete an initial privacy review, the agency could not determine whether it was required to complete a PIA. In instances where an agency did not determine the applicability of a requirement, we did not evaluate the extent to which the agency addressed the requirement. Appendix I contains additional information on our methodology.

¹The agencies we evaluated are the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), U.S. Customs and Border Protection (CBP), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), the U.S. Marshals Service, and the U.S. Secret Service.



U.S. Customs and Border Protection



Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

INITIAL PRIVACY REVIEW

U.S. Customs and Border Protection (CBP) completed initial privacy reviews for facial recognition services it uses. However, we found CBP completed one review without full and correct information on transmission and retention of personally identifiable information (PII), and completed the other review after it began using the service.

- We found CBP completed the initial privacy review for IntelCenter's services prior to use, in accordance with Department of Homeland Security (DHS) policy. However, we found the review did not discuss CBP's use of IntelCenter's facial recognition capabilities and presented some incorrect information about transmission and retention of PII. For example, CBP's initial privacy review states that CBP would only download IntelCenter data. However, we confirmed with CBP officials and IntelCenter representatives that users upload photos of individuals to IntelCenter to use the service's facial recognition capabilities.
- CBP completed an initial privacy review for Marinus Analytics' service. However, CBP completed it after staff had begun to use the service. Specifically, CBP told us it acquired and began using the service in September 2020 and completed the initial privacy review in January 2021, four months later.

PRIVACY IMPACT ASSESSMENT (PIA)

CBP completed a PIA for IntelCenter. However, we found it included some incorrect information. Additionally, CBP had not completed the PIA for Marinus Analytics as of April 2023.

- We found that CBP completed the PIA for IntelCenter prior to using the service, in accordance with policy. However, the PIA included some incorrect information about the service. For example, in the PIA, CBP stated that no information—PII or otherwise—would be transmitted to IntelCenter. However, we confirmed with CBP officials that CBP transmitted PII to use the facial recognition service. Further, the PIA did not discuss IntelCenter's facial recognition capabilities and therefore did not consider the potential privacy risks or mitigation strategies.
- In its January 2021 initial privacy review for Marinus Analytics' services, CBP determined a need for a PIA. However, of April 2023, CBP had yet to complete it. Officials stated that they hoped to complete the PIA by October 2023.

ASSESS PRIVACY NEEDS PRIOR TO ACQUISITION

CBP did not complete the required DHS privacy checklist for one service (IntelCenter). CBP partially completed this checklist for the second service (Marinus Analytics).^a

- CBP did not complete the required privacy checklist for its acquisition of IntelCenter. CBP privacy officials stated that CBP acquired the service in 2018, before privacy officials routinely reviewed contract documentation.
- CBP partially completed the privacy checklist for Marinus Analytics. For example, CBP completed the first page of Marinus Analytics' checklist, but did not address pages of the checklist related to, among other things, privacy terms and data retention requirements.

OVERSEE PRIVACY CONTROLS FOR CONTRACTOR ACCESS TO PII

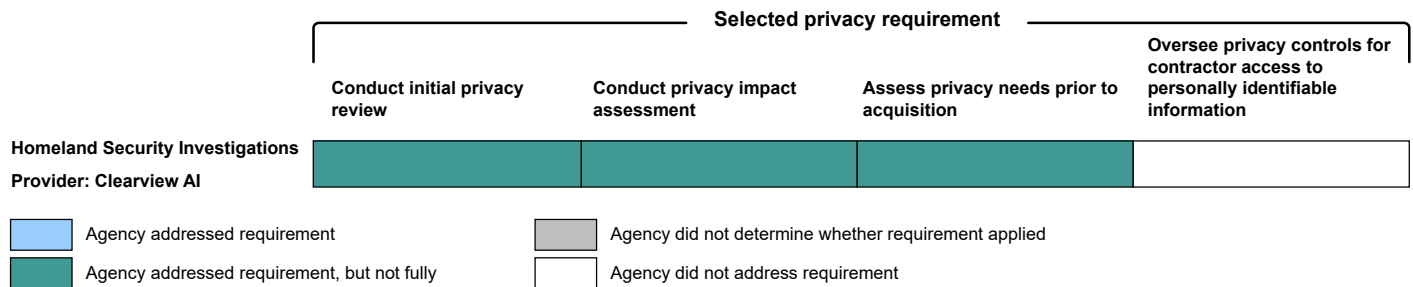
We were unable to assess the extent to which CBP addressed this requirement for one service it used (IntelCenter). CBP did not complete certain DHS requirements to oversee privacy controls for contractor access to PII for the other service it used (Marinus Analytics).

- Because CBP did not complete the DHS privacy checklist for IntelCenter that would have identified appropriate privacy controls, we could not evaluate the extent to which the agency oversaw privacy controls for contractor access to PII.
- CBP's contract with Marinus Analytics states that contractor staff who have access to sensitive information (including PII) are to sign non-disclosure agreements and receive training on protecting such information. However, CBP officials told us they did not enforce these terms because they did not initially consider the photos transmitted to Marinus Analytics to be PII, and so did not think contractor staff had access to CBP's PII. However, CBP's initial privacy review indicated that CBP would share PII with Marinus Analytics, and company representatives confirmed that a limited number of staff could access uploaded photos.

^aThe DHS Acquisition Manual requires that staff complete a checklist of considerations for sensitive information (including PII) for all acquisitions regardless of dollar value.



Homeland Security Investigations



Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

INITIAL PRIVACY REVIEW

Homeland Security Investigations (HSI) completed an initial privacy review for Clearview AI. However, it did so after using the service. Additionally, the review included some incorrect statements about Clearview AI's data retention features. In particular, the review states that Clearview AI will immediately delete uploaded photos in its database as soon as the facial recognition search is complete. However, according to Clearview AI representatives, the service retains search photos for audit purposes.^a

PRIVACY IMPACT ASSESSMENT (PIA)

According to its initial privacy review, HSI determined a need for a PIA for Clearview AI. In May 2020, HSI completed the PIA and in it, identified privacy risks and mitigations.^b However, HSI completed the PIA after acquiring and utilizing the service.^c Although the PIA was not complete until May 2020, HSI officials stated that many of the risk mitigations identified in the PIA were in place prior to that time.

ASSESS PRIVACY NEEDS PRIOR TO ACQUISITION

HSI completed the required Department of Homeland Security (DHS) privacy checklist to assess privacy needs and also had the Privacy Office review the draft contract and ensure the contract addressed HSI's privacy needs. However, HSI did not fully address issues raised by the agency's Privacy Office during the acquisition process. Specifically, the agency's Privacy Office conducted a review of HSI's proposed contract with Clearview AI before its execution. As part of this review, the Privacy Office evaluated privacy terms in the draft contract, and recommended that additional privacy terms be included in their entirety in the final contract. For example, these terms included identifying all records and data as federal government records and requiring a privacy point of contact to support HSI in completing privacy compliance documentation. However, the contracting officer removed these terms, among others, from the final contract and noted that it was within their discretion to do so. However, the contracting officer did not notify privacy officials of these changes, which left privacy officials unaware of the privacy controls of the service.

OVERSEE PRIVACY CONTROLS FOR CONTRACTOR ACCESS TO PII

We found that HSI did not complete certain DHS requirements to oversee privacy controls for contractor access to PII. HSI's contract with Clearview AI states that contractor staff who have access to sensitive information (e.g., PII) are to sign non-disclosure agreements and receive training on protecting such information.^d Acquisition officials stated they did not obtain signed non-disclosure agreements from Clearview AI staff or ensure Clearview AI staff received the training because they did not think Clearview AI staff had access to transmitted photos. However, we confirmed with Clearview AI representatives that a limited number of Clearview AI staff could access transmitted photos.^e

^aIn particular, in an addendum to HSI's contract with Clearview AI, (Attachment 5-Other Terms and Conditions), HSI required that the contractor "ensure that all queries of probe images submitted by U.S. Immigration and Customs Enforcement are maintained by Clearview AI for audit purposes only."

^bU.S. Immigration and Customs Enforcement, Privacy Impact Assessment for the ICE Use of Facial Recognition Services, DHS/ICE/PIA-054 (Washington, D.C.: May 13, 2020).

^cSpecifically, HSI began using Clearview AI in June 2019 and completed the PIA in May 2020.

^dSpecifically, the contract states that "all contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement, as a condition of access to such information" and that "all contractor and subcontractor employees that will have access to PII and/or sensitive PII are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or sensitive PII."

^eAdditionally, the privacy checklist for Clearview AI indicates that Clearview AI contractors would have access to PII. Clearview AI representatives noted that the company has cybersecurity and internal controls in place to protect probe photos in its system. These representatives also noted that the data are only retained for auditing purposes, and that staff would only access such data if they had with a valid legal reason.



U.S. Secret Service

	Selected privacy requirement			Oversee privacy controls for contractor access to personally identifiable information
	Conduct initial privacy review	Conduct privacy impact assessment	Assess privacy needs prior to acquisition	
U.S. Secret Service Provider: Clearview AI				
Agency addressed requirement Agency addressed requirement, but not fully	Agency did not determine whether requirement applied Agency did not address requirement			

Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

INITIAL PRIVACY REVIEW

The U.S. Secret Service did not complete an initial privacy review for Clearview AI. Specifically, the Secret Service told us that staff used Clearview AI between April 2019 and April 2020 on a free trial basis without the knowledge of headquarters officials. Officials told us that since headquarters officials, including relevant privacy officials, were unaware of this use, the agency did not conduct an initial privacy review. The Secret Service has since taken steps to ensure staff do not engage in future free trials. For example, the Secret Service published guidance and requirements prohibiting staff use of Clearview AI and future free trials.^a Further, as of April 2023, the Secret Service reported that the agency had halted its use of the service.

OTHER SELECTED PRIVACY REQUIREMENTS

Because the Secret Service did not conduct an initial privacy review, we could not evaluate the extent to which the agency addressed the three remaining privacy requirements.

^aThe guidance, emailed to staff on June 18, 2020, prohibits staff from conducting searches using Clearview AI because of possible government ethics concerns. It also reminds staff that they should only disclose personally identifiable information (i.e., photos) to an internet service when the Secret Service has an agreement in place regarding the confidentiality and security of that information.



Bureau of Alcohol, Tobacco, Firearms and Explosives

Bureau of Alcohol, Tobacco, Firearms and Explosives Provider: Clearview AI	Selected privacy requirement			
	Conduct initial privacy review	Conduct privacy impact assessment	Assess privacy needs prior to acquisition	Oversee privacy controls for contractor access to personally identifiable information

Agency addressed requirement

Agency addressed requirement, but not fully

Agency did not determine whether requirement applied

Agency did not address requirement

Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

INITIAL PRIVACY REVIEW

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) did not complete an initial privacy review for Clearview AI. Specifically, ATF told us that one Field Division used Clearview AI to conduct searches on a free trial basis between March and May 2022. Agency officials also said that ATF headquarters officials, including relevant privacy officials, were unaware of this use, and that the agency did not conduct an initial privacy review. ATF has since taken steps to ensure staff do not engage in future free trials, according to the agency. For example, ATF officials notified staff in July 2022 that use of free trials of facial recognition services is prohibited. As of April 2023, ATF officials told us that the agency had halted its use of the service.

OTHER SELECTED PRIVACY REQUIREMENTS

Because ATF did not conduct an initial privacy review, we could not evaluate the extent to which ATF addressed the three remaining privacy requirements.



Drug Enforcement Administration

	Selected privacy requirement			Oversee privacy controls for contractor access to personally identifiable information
	Conduct initial privacy review	Conduct privacy impact assessment	Assess privacy needs prior to acquisition	
Drug Enforcement Administration Provider: Clearview AI				

Agency addressed requirement

 Agency addressed requirement, but not fully

Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

INITIAL PRIVACY REVIEW

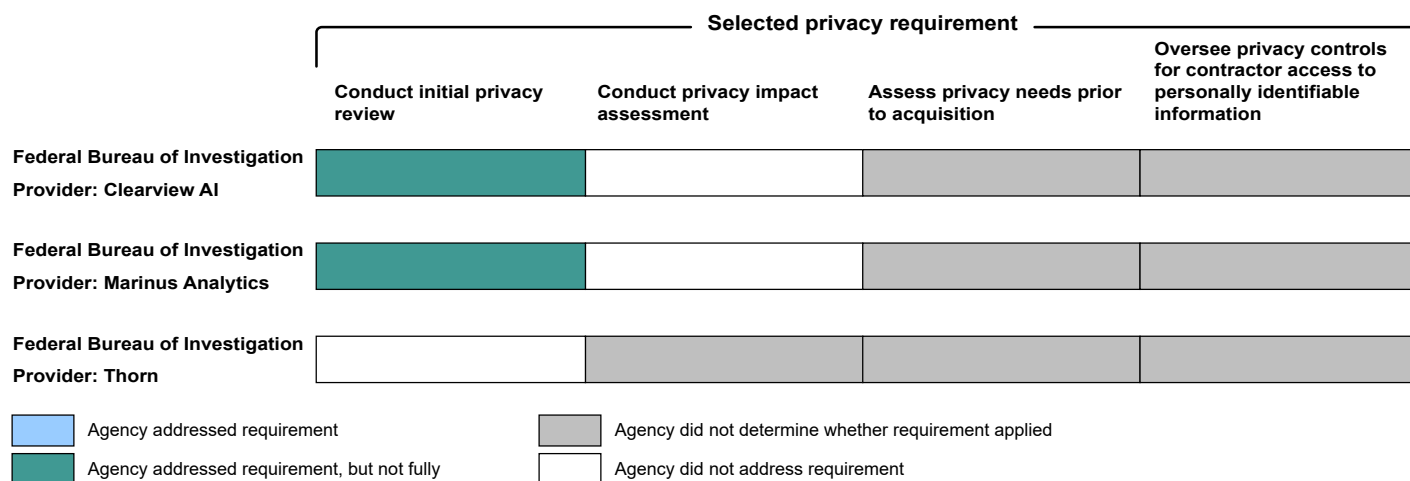
The Drug Enforcement Administration (DEA) did not complete an initial privacy review for Clearview AI. Specifically, DEA staff in at least 37 field offices used Clearview AI free trials over a two-year period, from August 2019 to August 2021, according to the agency. DEA officials told us that headquarters officials, including relevant privacy officials, were unaware of this use, and therefore the agency did not conduct an initial privacy review. DEA officials told us that the agency has since taken steps to ensure staff do not engage in future free trials. For example, DEA officials contacted Clearview AI in August 2021 to discontinue DEA accounts. Agency officials also told us that they notified relevant staff that DEA investigators were unauthorized to use facial recognition technology. Further, as of April 2023, DEA officials told us that the agency had halted its use of the service.

OTHER SELECTED PRIVACY REQUIREMENTS

Because DEA did not conduct an initial privacy review, we could not evaluate the extent to which DEA addressed the three remaining privacy requirements.



Federal Bureau of Investigation



Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

INITIAL PRIVACY REVIEW

The Federal Bureau of Investigation (FBI) completed initial privacy reviews for Clearview AI and Marinus Analytics, but not as required by departmental policy. As of April 2023, FBI had not completed an initial privacy review for Thorn.

- FBI completed an initial privacy review for Clearview AI; however, it did not do so before sending photos to the service in August 2019. FBI completed the review in June 2022—over two and a half years after the agency began using the service. In addition, the review presented some incorrect information about required training. Specifically, the review states that FBI requires staff in one specific unit to complete training to use Clearview AI. However, no such requirement exists.
- FBI completed an initial privacy review for Marinus Analytics; however, it did not do so before sending photos to the service beginning in 2018. FBI completed the review in November 2022—years after the agency began using the service. In addition, the review did not discuss the facial recognition capabilities of the service.
- Additionally, FBI determined a need for an initial privacy review for Thorn. However, as of April 2023, FBI had yet to complete it after more than four years of using the service.^a

PRIVACY IMPACT ASSESSMENT (PIA)

- As of April 2023, FBI had not completed a PIA for Clearview AI. Specifically, FBI officials told us that they submitted a PIA for its use of Clearview AI to DOJ's Chief Privacy and Civil Liberties Office for final approval in April 2023.
- As of August 2023, FBI had not completed a PIA for Marinus Analytics. Specifically, FBI determined a need for a PIA in its November 2022 initial privacy review but, as of August 2023, FBI officials told us that the agency had not completed it.

OTHER SELECTED PRIVACY REQUIREMENTS

Because FBI did not conduct a PIA for Clearview AI or Marinus Analytics and did not complete an initial privacy review for Thorn, we could not evaluate the extent to which the agency addressed the remaining privacy requirements.

^aAccording to FBI officials, Thorn is a free service. Therefore FBI did not go through an acquisition process to obtain this service and does not have a contract with the service.



U.S. Marshals Service

	Selected privacy requirement			Oversee privacy controls for contractor access to personally identifiable information
	Conduct initial privacy review	Conduct privacy impact assessment	Assess privacy needs prior to acquisition	
U.S. Marshals Service Provider: Clearview AI				

Agency addressed requirement

Agency addressed requirement, but not fully

Agency did not determine whether requirement applied

Agency did not address requirement

Source: GAO analysis of agency data and selected key privacy requirements. | GAO-23-105607

INITIAL PRIVACY REVIEW

The U.S. Marshals Service had not completed an initial privacy review for Clearview AI as of April 2023. Specifically, according to documentation we reviewed, Marshals Service officials began using Clearview AI in May 2019, and officials told us that the agency started to draft its initial privacy review in April 2021. Marshals Service officials told us the agency submitted the initial privacy review to DOJ's Office of Privacy and Civil Liberties in February 2023 but, as of April 2023, the agency had yet to complete this review—four years after it began using the service.

OTHER SELECTED PRIVACY REQUIREMENTS

Because the Marshals Service did not conduct an initial privacy review, we could not evaluate the extent to which the agency addressed the three remaining privacy requirements.

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

August 10, 2023

Gretta L. Goodwin
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-105607, "FACIAL RECOGNITION SERVICES: Federal Law Enforcement Agencies Should Take Actions to Implement Training, and Policies for Civil Liberties"

Dear Ms. Goodwin:

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

DHS leadership is pleased to note GAO's positive recognition that DHS is currently finalizing and plans to issue new Department-wide guidance to ensure the protection of civil rights and civil liberties while staff use facial recognition technology. Specifically, the DHS Office of the Chief Information Officer, in coordination with the DHS Privacy Office, drafted the Face Recognition Directive and Instruction which will establish requirements for the responsible and authorized use of facial recognition technology. The Directive and Instruction are in final review and expected to be issued by December 29, 2023. DHS remains committed to embedding and enforcing privacy, civil rights, and civil liberties protections, and enhancing transparency, in all DHS activities and programs, as appropriate.

The draft report contained ten recommendations, including five for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing accuracy, contextual, and other issues under separate cover for GAO's consideration.

Appendix III: Comments from the Department
of Homeland Security

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

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2023.08.10 07:31:37 -0400

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

**Enclosure: Management Response to Recommendations
Contained in GAO-23-105607**

GAO recommended that the Director of U.S. Immigration and Customs Enforcement (ICE):

Recommendation 1: Establish and implement a process to periodically monitor whether HSI [Homeland Security Investigations] staff using facial recognition services to support criminal investigations have completed training requirements.

Response: Concur. On May 14, 2023, ICE HSI conducted a review of all licensed users, and the training that each user received and completed. The results of the review confirmed one hundred percent compliance of users completing training for privacy and the facial recognition technology (FRT) tool prior to receiving a license. Going forward, HSI will continue to ensure completion of required training for any user issued a license by periodically monitoring this activity on an ongoing basis. HSI will also continue to review its user compliance bi-annually to ensure staff using facial recognition services to support criminal investigations have completed training requirements. On July 18, 2023, HSI provided GAO evidence corroborating the completion of licensed users' training.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

GAO recommended that the Commissioner of U.S. Customs and Border Protection (CBP):

Recommendation 4: Determine the extent that staff use facial recognition services to develop and share information in support of other agencies' criminal investigations (such as number of CBP staff that use the services and how often they do so).

Response: Concur. The CBP Office of Field Operations (OFO) will continue to work with current and future service providers to ensure that accurate metrics for CBP usage (e.g., number of queries, type of queries, queries by user, etc.) are available. OFO will also create guidance to capture instances where the use of a facial recognition service contributes to the development and sharing of information for lead purposes with an investigative partner. Estimated Completion Date (ECD): December 29, 2023.

Recommendation 5: Assess whether training would benefit staff using facial recognition services to develop and share information in support of other agencies' criminal investigations, incorporating information on the extent to which staff use such services.

Response: Concur. CBP OFO will develop specific training and guidance on the use of commercial facial recognition services to include how to document the development and sharing of investigative leads. ECD: December 29, 2023.

GAO recommended that the Secretary of Homeland Security ensure the Chief Privacy Officer:

Recommendation 8: Works with DHS components continuing to use facial recognition services to address outstanding privacy requirements, and update privacy documentation as appropriate.

Response: Concur. DHS practices a privacy continuous monitoring strategy in accordance with Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource," dated July 28, 2016.¹ Specifically, DHS practices comport with guidance that—as part of an agency's risk management process, the appropriate privacy official should develop and maintain a privacy continuous monitoring strategy that should catalog the available privacy controls implemented at the agency across the agency risk management tiers. Further, DHS ensures that the controls are effectively monitored on an ongoing basis, at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks. DHS accomplishes these functions through implementation of DHS Directive 047-01, "Privacy Policy and Compliance," dated July 7, 2011,² and DHS Instruction 047-01-001, "Privacy Policy and Compliance," dated July 25, 2011.³ The directive and instruction outline the requirements for DHS Program Managers and System Managers to complete all privacy compliance documentation set forth in applicable requirements (e.g., statutes regulations, Executive Orders, and policies issued by the Chief Privacy Officer), and submit through their respective Component Privacy Office to the DHS Privacy Office for formal approval, as follows:

1. Whenever a DHS information technology (IT) system, technology, rulemaking, program, pilot project, or other activity involves the planned use of personally identifiable information (PII), or otherwise impacts the privacy of individuals as determined by the Chief Privacy Officer, the relevant manager completes a Privacy Threat Assessment (PTA) in accordance with Privacy Office guidance and submits it to the Component Privacy Officer or privacy point of contact (PPOC). The Component Privacy Officer or PPOC then reviews the proposed PTA in consultation with counsel for the Component and submits it, together with a recommendation as to whether a Privacy Impact Assessment (PIA) is necessary, to the Chief Privacy Officer. The Chief Privacy Officer then determines whether a

¹ https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf

² https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf

³ https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf

PIA is required, based on answers provided in the PTA and taking into consideration the Component Privacy Officer's or PPOC's recommendation.

2. If the Chief Privacy Officer concludes that a PIA is necessary for a DHS IT system, technology, rulemaking, program, pilot project, or other activity that impacts the privacy of individuals, the relevant manager works with the Component Privacy Officer or PPOC, counsel for the Component, and the Chief Privacy Officer, as appropriate, to complete the PIA in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all PIAs.
3. The Chief Privacy Officer, in consultation with the relevant Component Privacy Officer or PPOC and counsel for the Component, determines whether a particular collection of PII is a System of Records for Privacy Act purposes and whether to propose a rule that would exempt the system from certain aspects of the Privacy Act. If the system is a Privacy Act System of Records and it is not covered by an existing System of Records Notice (SORN), the Component Privacy Officer or PPOC, in consultation with counsel for the Component, prepares a SORN and, where appropriate, a Notice of Proposed Rulemaking (NPRM) describing proposed Privacy Act exemptions for the System of Records and, after public comment, a final rule, in accordance with guidance issued by the Chief Privacy Officer. The Chief Privacy Officer reviews and provides final approval for all SORNs, NPRMs, and final rules.
4. The Chief Privacy Officer schedules completed PTAs, PIAs, and SORNs for mandatory review at least every three years for PTAs and PIAs, and every two years for SORNs. The Chief Privacy Officer notifies the relevant Component Privacy Officer or PPOC that a PTA, PIA, and/or SORN review is required and begins the collaborative review process, which follows the process described in this Instruction for new PTAs, PIAs, and SORNs.
5. Program Managers and System Managers submit drafts of all Privacy Act Statements to the Chief Privacy Officer, or to the relevant Component Privacy Officer or PPOC, for review and final approval. Privacy Act Statements are included in all documents, whether in paper or electronic form, that the Department uses to collect PII from individuals to be maintained in a Privacy Act System of Records.

Further, the DHS Privacy Office uses the Privacy Compliance Artifacts Tracking System (PRIVCATS) to ensure all outstanding privacy requirements and privacy documentation are completed, as appropriate. The DHS Privacy Office also "tags" programs/systems, etc., in PRIVCATS that implement a specific technology or privacy risk. For example, the DHS Privacy Office can tag all programs/systems, etc., that use facial recognition

services to run specific metrics and reporting and continue to ensure that those programs with unique privacy equities are addressed sufficiently and timely through appropriate privacy compliance documentation. PRIVCATS, through monthly and ad-hoc reporting capabilities, also ensures compliance with the requirements of the directive and instruction. Further, PRIVCATS 2.0 was made fully accessible to all available Components on March 13, 2023, which permitted access to the system to not only the DHS Privacy Office, but also Component Privacy Offices. Any pending or outstanding requirements are communicated by the DHS Privacy Office to Components every month through formal Monthly Component Reports. Additionally, with this new access, Components can view any of their outstanding or expiring privacy compliance documentation requirements at any time.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

Recommendation 9: Collaborates with component program, acquisition, and privacy officials to evaluate components' adherence to the department's privacy compliance process for facial recognition services – taking into account the results of this report – and to remediate any deficiencies identified during their evaluation.

Response: Concur. The DHS Privacy Office is responsible for ensuring that the Department's use of technology sustains, and does not erode, privacy protections relating to the collection, use, maintenance, disclosure, deletion, and/or destruction of personally identifiable information. One of the key functions through which this is accomplished is the privacy compliance process, as outlined in DHS Directive 047-01 and Instruction 047-01-001. The DHS Privacy Office will continue to work with Components using facial recognition technologies on an ongoing basis to ensure that Components adhere to the privacy compliance process for facial recognition services—taking into account the results of this report—and remediate any deficiencies identified during these evaluations, as appropriate. However, it is important to note that DHS practices a privacy continuous monitoring strategy; therefore, compliance is achieved continuously, rather than by a certain date. For example, if a Component were to update its uses of facial recognition services, privacy compliance documentation likewise would require appropriate updates.

DHS requests the GAO consider this recommendation resolved and closed, as implemented.

Appendix IV: GAO Contact and Staff Acknowledgements

GAO Contact

Gretta L. Goodwin, (202) 512-8777 or goodwing@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jeffrey Fiore (Assistant Director), Kathleen Donovan (Analyst-in-Charge), Ricki Gaber, Sheerine Karamzadeh-Rahimi, Grace Kwon, Brooke Linsenbardt and John Vocino made key contributions to this report. Also contributing to this report were Benjamin Crossley, Caitlin Cusati, Richard Hung, Lydie Loth, Lee McCracken, Heidi Nielson, Monica Perez-Nelson, and Kevin Reeves.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.

~~LAW ENFORCEMENT SENSITIVE~~

OFFICE OF INSPECTOR GENERAL

DHS Does Not Have Assurance That All Migrants Can be Located Once Released into the United States (REDACTED)

~~Warning: This document is Law Enforcement Sensitive (LES). Do not distribute or copy this report without the expressed written consent of the Office of Inspector General.~~



Homeland
Security

~~LAW ENFORCEMENT SENSITIVE~~

September 6, 2023
OIG-23-47



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 6, 2023

MEMORANDUM FOR: The Honorable Alejandro Mayorkas
Secretary
Department of Homeland Security

Corey A. Price
Executive Associate Director
Enforcement and Removal Operations

Jason Owens
Chief
United States Border Patrol

FROM: Joseph V. Cuffari, Ph.D. **JOSEPH V CUFFARI**
Inspector General

Digitally signed by
JOSEPH V CUFFARI
Date: 2023.08.29
16:26:26 -04'00'

SUBJECT: *DHS Does Not Have Assurance That All Migrants Can
be Located Once Released into the United States – ~~Law
Enforcement Sensitive~~*

Attached for your action is our final report, *DHS Does Not Have Assurance That All Migrants Can be Located Once Released into the United States – ~~Law Enforcement Sensitive~~*. We incorporated the formal comments provided by your office.

The report contains four recommendations aimed at improving the controls validating migrants' post-release U.S. addresses. Your office did not concur with all four recommendations. Based on information provided in your response to the draft report, we consider all four recommendations open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendations will remain open and unresolved.

Please send your response to OIGAuditsFollowup@oig.dhs.gov.

www.oig.dhs.gov

~~LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

Please contact me with any questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



~~LAW ENFORCEMENT SENSITIVE~~

DHS OIG HIGHLIGHTS

DHS Does Not Have Assurance That All Migrants Can be Located Once Released into the United States

September 6, 2023

Why We Did This Audit

DHS ensures the safety and security of the Nation's borders while managing a safe, orderly, and humane immigration system. DHS released more than 1 million migrants into the United States from March 2021 through August 2022. Prior to releasing each migrant, DHS personnel are required to obtain an address when possible. We conducted this audit to determine the extent to which DHS accurately and effectively tracks migrants' post-release addresses in the United States.

What We Recommend

We made four recommendations to improve the controls validating migrants' post-release U.S. addresses.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Department of Homeland Security has limited ability to track migrants' post-release addresses accurately and effectively. U.S. Border Patrol (USBP) cannot always obtain and does not always record migrant addresses, and U.S. Immigration and Customs Enforcement (ICE) does not always validate migrant addresses prior to migrant release into the United States. Based on our review of 981,671 migrant records documented by USBP from March 2021 through August 2022, addresses for more than 177,000 migrant records were either missing, invalid for delivery, or not legitimate residential locations. In addition to migrants not providing U.S. release addresses, DHS faced several challenges hindering its ability to record and validate migrant addresses as required. USBP did not accurately and effectively capture valid addresses, in part due to the large number of migrants apprehended, as well as its limited coordination with ICE and its limited authority to administer compliance with address requirements. ICE also did not have adequate resources to validate and analyze migrants' post-release addresses.

ICE must be able to locate migrants to enforce immigration laws, including to arrest or remove individuals who are considered potential threats to national security. The notable percentage of missing, invalid for delivery, or duplicate addresses on file means DHS may not be able to locate migrants following their release into the United States. As the Department continues to apprehend and release tens of thousands of migrants each month, valid post-release addresses are essential.

DHS Response

The Department did not concur with all four recommendations.

~~LAW ENFORCEMENT SENSITIVE~~



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background	1
Results of Audit	4
USBP Did Not Receive and Record, and ICE Did Not Validate, All Addresses Prior to USBP Releasing Migrants into the United States	5
Recommendations.....	16

Appendixes

Appendix A: Objective, Scope, and Methodology	20
Appendix B: DHS Comments to the Draft Report	23
Appendix C: [REDACTED]	28
Appendix D: Report Distribution.....	29

Abbreviations

ATD	Alternatives to Detention
CBP	U.S. Customs and Border Protection
C.F.R.	Code of Federal Regulations
e3	e3 system
EARM	ENFORCE Alien Removal Module
ERO	Enforcement and Removal Operations
ICE	U.S. Immigration and Customs Enforcement
NTA	Notice to Appear
NTR	Notice to Report
USBP	U.S. Border Patrol
U.S.C.	United States Code
USPS	United States Postal Service



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Background

The Department of Homeland Security has primary responsibility for securing U.S. borders from illegal activity and regulating travel and legal trade. Within DHS, U.S. Customs and Border Protection's (CBP) mission is to safeguard U.S. borders, and specifically, U.S. Border Patrol (USBP) enforces laws preventing illegal immigration by detecting and apprehending migrants caught crossing the border between legal ports of entry. USBP is also responsible for the short-term detention of migrants. USBP is staffed with more than 16,000 agents who patrol the Southwest border and process migrants each day.

From March 2021 through August 2022, USBP apprehended more than 1.3 million¹ migrants illegally entering the United States across the Southwest border under the provisions of Title 8.² According to the *Immigration and Nationality Act*,³ CBP has the authority to release certain noncitizens into the United States on a case-by-case basis for urgent humanitarian reasons.⁴ USBP may release migrants for removal proceedings using various options, including, but not limited to:

- Notice to Appear (NTA) with Release on Own Recognizance.⁵ USBP may issue a migrant an NTA, which may be filed with the immigration court, to begin removal or admissibility determinations.⁶ During our audit period, from March 2021 through August 2022, USBP released more than 430,000 migrants using NTAs.
- Prosecutorial discretion.⁷ USBP had discretion to release migrants in the United States with a Notice to Report (NTR) to a U.S. Immigration and

¹ This figure represents single adult and family unit USBP apprehensions.

² See 8 United States Code (U.S.C.) § 1182 – *Inadmissible aliens*. An alien present in the United States without being admitted or paroled, or who arrives in the United States at any time or place other than as designated by the Attorney General, is inadmissible.

³ See 8 U.S.C. § 1182(d)(5); 8 Code of Federal Regulations (C.F.R.) § 212.5 – *Parole of aliens into the United States*. The Secretary of Homeland Security has the authority to continue an alien in custody or grant parole under Section 212(d)(5)(A) of the *Immigration and Nationality Act*.

⁴ On occasion, migrants can also be released for significant public benefit such as supporting law enforcement cases.

⁵ See 8 C.F.R. § 1239.1 – *Notice to appear*. Every removal proceeding conducted under section 240 of the Act (8 U.S.C. 1229a) to determine the deportability or inadmissibility of an alien begins with filing a notice to appear with the immigration court. For Orders of Release on Recognizance, DHS has the discretion to release noncitizens from detention.

⁶ If an NTA is not filed with the immigration court, the migrant has no requirement to appear in court and their removability cannot be determined.

⁷ USBP Former Chief, Rodney Scott, issued a memorandum dated March 19, 2021, *Prosecutorial Discretion*, which authorized USBP to exercise discretion to release persons,



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Customs Enforcement (ICE) office near their intended destination within 60 days of release. During our audit period, USBP released nearly 95,000 migrants using this release method.

- Parole Plus Alternatives to Detention (Parole + ATD).⁸ USBP released migrants into the United States using Parole + ATD, which mostly included ATD tracking. ICE manages ATD, which can include electronic devices such as ankle bracelets and smartphones intended to ensure compliance with release conditions, court hearings, and final orders of removal. During our audit period, USBP released more than 318,000 migrants on Parole + ATD. ICE's ATD program had more than 300,000 migrants actively enrolled at the end of FY 2022.⁹

Using these three authorities, DHS released more than 1 million¹⁰ migrant individuals and families into the United States from March 2021 through August 2022. DHS personnel obtain and use migrants' destination addresses to track and locate migrants once released into the United States. For example, ICE relies on migrant-provided information to track migrants, send documentation, and determine which ICE field office migrants will check into while awaiting immigration proceedings. More specifically, ICE Enforcement and Removal Operations (ERO) must be able to contact or locate migrants who are subject to final orders of removal, are fugitive removals,¹¹ or agree to voluntary departure from the United States.

In March 2021, USBP agents were instructed¹² to obtain a U.S. destination address, also referred to as a post-release address, "to the extent the subjects know it." This guidance also instructs USBP to document the address in its

excluding unaccompanied children, who were in the United States illegally, without placing them in removal proceedings. Under prosecutorial discretion, USBP issued a migrant an NTR, also referred to as a "Call-in Letter," and a Form I-385, which required the migrant to report to an ICE office within 60 days of release.

⁸ In November 2021, USBP issued a memorandum, *Parole Plus ATD*, formally ceasing the use of prosecutorial discretion and NTRs at all sectors across the southern border and instructing agents in authorized sectors to use the Parole Plus ATD processing pathway. Similar to NTRs, Parole Plus ATD authorizes USBP to release migrants, on ATD, into the United States without initiating removal proceedings.

⁹ The Department of Homeland Security's Parole + ATD memorandum was vacated by court order in March 2023. See *Florida v. U.S.*, 3:21-cv-01066-TKW-ZCB (N.D. Fla. 2023).

¹⁰ ICE released more than 370,000 migrants during our audit timeframe.

¹¹ Fugitive removals include migrants wanted for a crime in another country regardless of the severity of the crime and generally involve serious crimes, including murder, rape, sexual abuse of a minor, drug offenses, alien smuggling, fraud, or theft.

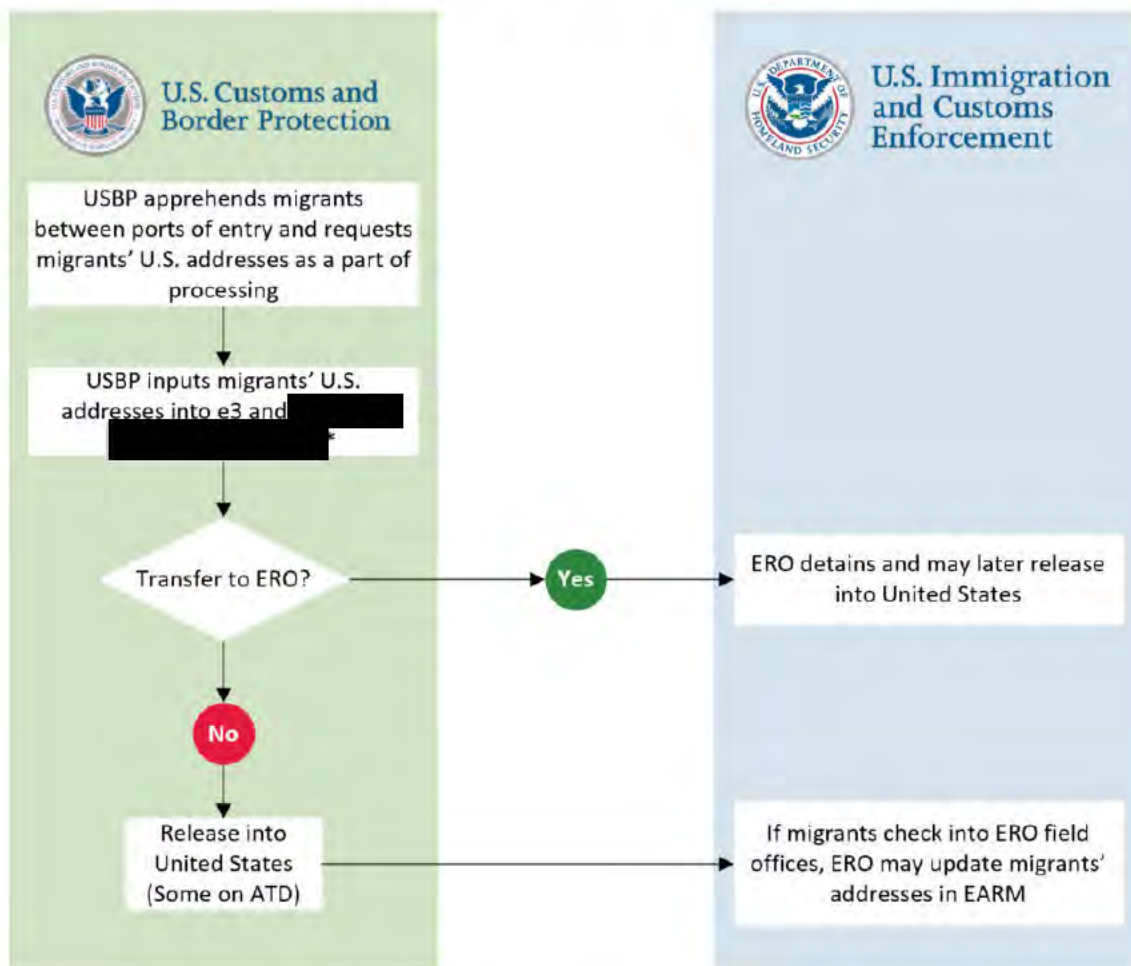
¹² According to an email from the Acting Deputy Chief Law Enforcement Operations Directorate at USBP on March 23, 2021, USBP agents must obtain an address to the extent the subject knows it.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

system of record¹³ and to coordinate and share migrant information with ERO to track migrants throughout the immigration process. ICE has also issued procedures¹⁴ for its officers to validate migrant addresses, captured by ICE, using the United States Postal Service's (USPS) website and, if necessary, update their system of record¹⁵ with the correct address prior to release. Figure 1 outlines the process¹⁶ used by USBP and ERO to obtain and verify post-release addresses when processing migrants.

Figure 1. Overview of Migrant and Address Processes Post Apprehension



Source: DHS Office of Inspector General-created based on CBP and ICE data

* ERO may validate the USBP-captured U.S. addresses prior to USBP release if ERO is notified of the release.

¹³ USBP uses the e3 system (e3) as its system of record for processing apprehended migrants.

¹⁴ ICE's *ENFORCE Alien Removal Module (EARM) Training Manual*, July 2021.

¹⁵ ICE uses EARM to enter migrant case data, such as apprehension details, migrant name, and U.S. point of contact.

¹⁶ This figure does not include all potential processes and pathways for migrants.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

In September 2022, we reported¹⁷ on the importance of DHS personnel documenting U.S. addresses where migrants plan to reside after release from DHS custody. However, we found that USBP did not always document migrant addresses prior to release, which hindered tracking, reporting, and various enforcement activities. We reported USBP only recorded an address about 65 percent of the time from March through June 2021. Additionally, 29 percent (32,092 of 111,990) of migrants released using prosecutorial discretion did not report to ICE within 60 days, as required by their release terms, from March through September 2021. We conducted this audit to follow up on this matter, to determine the extent to which DHS accurately and effectively tracks migrants' post-release addresses in the United States.

Results of Audit

DHS has limited ability to track migrants' post-release addresses accurately and effectively. USBP cannot always obtain and does not always record migrant addresses, and ICE does not always validate migrant addresses prior to migrant release into the United States. Based on our review of 981,671 migrant records documented by USBP from March 2021 through August 2022, addresses for more than 177,000 migrant records were either missing, invalid for delivery,¹⁸ or not legitimate residential locations. In addition to migrants not providing U.S. release addresses, DHS faced several challenges hindering its ability to record and validate migrant addresses as required. USBP did not accurately and effectively capture valid addresses, in part due to the large number of migrants apprehended, as well as its limited coordination with ICE and its limited authority to administer compliance with address requirements. ICE also did not have adequate resources to validate and analyze migrants' post-release addresses.

On average, DHS releases more than 60,000 migrants into the United States each month. ICE must be able to locate migrants to enforce immigration laws, including to arrest or remove individuals who are considered potential threats to national security. The notable percentage of missing, invalid, or duplicate addresses on file means DHS may not be able to locate migrants following their release into the United States. As the Department continues to apprehend and release tens of thousands of migrants each month, valid post-release addresses are essential.

¹⁷ *DHS Technology Systems Do Not Effectively Support Migrant Tracking at the Southwest Border*, OIG 22-66, September 2022.

¹⁸ We refer to addresses invalid for delivery as "invalid" and "undeliverable" throughout this report.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

USBP Did Not Receive and Record, and ICE Did Not Validate, All Addresses Prior to USBP Releasing Migrants into the United States

USBP did not always obtain valid destination addresses for all migrants processed from March 2021 through August 2022. Based on our review of 981,671 migrant records documented by USBP from March 2021 through August 2022,¹⁹ more than 177,000 migrant records were either missing, invalid, or not legitimate residential locations. USBP did not accurately and effectively capture valid addresses because DHS does not have sufficient coordination or authority to administer compliance with address requirements. Further, ICE did not always validate addresses for migrants prior to release into the United States because it did not have the resources necessary to validate and analyze migrants' post-release addresses.

USBP Did Not Always Receive and Record Valid Addresses for Migrants Released into the United States

According to CBP's internal 2021 guidance,²⁰ USBP agents are "required to populate the U.S. address field," [REDACTED] prior to releasing each migrant.²¹ This guidance instructs USBP to type migrants' intended destinations into USBP's system of record, e3, [REDACTED]. A similar guidance document²² instructs USBP agents to type migrants' intended destination into the Find Address Field (within e3), and a validated address will appear. Although not required, we observed some USBP agents call the migrant's point of contact to verify the U.S. address provided by migrants.

USBP's ability to obtain an address is contingent on migrants providing valid addresses, which is not always possible.²³ Numerous USBP and ICE officials we met with stated some migrants do not have an address to provide when

¹⁹ 981,671 is the number of records associated with more than 845,000 migrants USBP released out of its custody from March 19, 2021, through September 8, 2022. The number of records associated with migrants that USBP released from September 1, 2022, through September 8, 2022, is less than 1 percent of the total records.

²⁰ Internal CBP guidance, *Capturing Destination Address for subjects released with NTR*, June 4, 2021.

²¹ See footnote 7, which applies during our audit period but was later superseded by Memorandum, *Policy on the Use of Parole Plus Alternatives to Detention to Decompress Border Locations*, July 20, 2022.

²² August 5, 2021, *Family Unit Parole with ATD initiative*.

²³ Prior encounter information for migrants apprehended by USBP may be used to retrieve previously documented U.S. addresses.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

crossing the border. Others provide handwritten addresses that may be in another language, invalid, or illegible.

More than **54,000**
address records
were blank.

As part of this audit, we reviewed 981,671²⁴ migrant records that USBP obtained from migrants and entered into e3 from March 2021 through August 2022.²⁵ Of these, 6 percent, or 54,663 records contained no address and most records without addresses (more than 54,000) were blank.²⁶ In September 2022, USBP issued guidance via email to instruct agents to enter “FAILED TO PROVIDE ADDRESS” into e3. Almost half of the records with no address obtained occurred in 6 months, from March through August 2021, under prosecutorial discretion releases. Figure 2 details missing addresses by release type.

²⁴ We obtained 981,671 migrant release address records from USBP’s e3 system. Of this total record count, we identified 728,747 records associated with migrants who each had only one address in e3. This total also includes 252,924 address records associated with 116,960 migrants with more than one address in the system of record, further complicating tracking. We tested all records together as we were unable to determine which address the migrant planned to travel to if multiple addresses were listed.

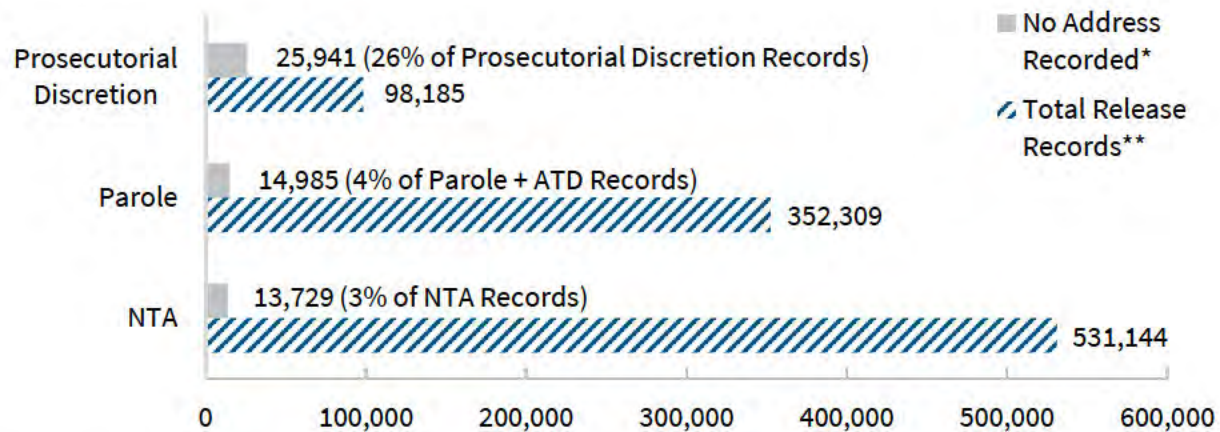
²⁵ All of the 981,671 migrant records tested and included in the report are associated with migrants apprehended and subsequently released by USBP; the report does not include migrants released by ICE.

²⁶ We considered no address as blank entries, “-”, and other obvious invalid addresses such as “111 DID NOT PROVIDE” as invalid addresses that could not receive mail.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Figure 2. Of 981,671 U.S. Release Records, 6% Were Missing Addresses



Source: DHS OIG analysis of USBP address release data from March 2021 – August 2022

* The total addresses not recorded includes eight records associated with other release types, which are not reflected in the figure.

** The total release records do not include 33 records, which are associated with other release types.

In addition, 26,093 of 981,671 addresses were not valid for mail delivery of court documents or for tracking purposes. Specifically, about 3 percent of the addresses received and recorded by USBP agents were undeliverable²⁷ based on Informatica Address Verification.²⁸ Examples of undeliverable addresses in e3 include “Corona Ave, Corona, NY 11368” and “APT 3 Worcester, MA 01604.”

We also identified more than 97,000 apartment addresses with no unit numbers. Based on USPS, these addresses are considered deliverable, but because the addresses did not contain unit numbers, actual delivery is unlikely. A supervisory Deportation and Detention officer stated addresses without specific apartment numbers are “unusable.”

In other instances, we identified non-existent and uninhabitable addresses. The audit team did not test release addresses to identify uninhabitable locations. Of the 28 addresses visited, more than 10 were uninhabitable and we identified more than 20 other uninhabitable locations through data

²⁷ See USPS OIG, *Undeliverable as Addressed Mail*, MS-AR-14-006, July 14, 2014. USPS defines “undeliverable mail” as mail it cannot deliver to the address on the mail piece because of an incorrect or illegible address.

²⁸ We used Informatica Address Verification software to clean, standardize, and match migrant release address data to determine deliverability. We could not match the migrant addresses to a valid address using the address testing service. It is possible the USPS could overcome the address errors we identified and deliver the mail. However, the software was not able to match or resolve the provided migrant release addresses to a valid deliverable address.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

analysis. Figure 3 contains images of uninhabitable migrant release addresses we observed during site visits. We also attempted to locate two addresses in Maryland that did not exist on online maps and confirmed each location was non-existent. USBP agents recorded one of these non-existent addresses 50 different times during a 6-month period.

Figure 3. U.S. Release Addresses Observed



Source: DHS OIG observation photos from Georgia, Illinois, Maryland, and New Jersey

Migrants may share addresses with one another to help ensure they will be released into the country. USBP and ICE personnel at multiple locations affirmed migrants often share commonly used addresses and may reuse addresses based on extended family all going to the same location or based on information from potential smugglers. Based on our analysis, 80 percent (790,090 of 981,671) of addresses were recorded at least twice during an 18-month period, some of which were provided by families upon release. More than 780 of these addresses were used more than 20 times. These families provided addresses that may be unsafe or have overcrowded living conditions based on multiple migrants using the same address. For example, DHS released 7 families, comprising 12 adults and 17 children, to a single-family 3-bedroom New Jersey home in a 70-day period.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

We also identified 7 addresses that were recorded more than 500 times, some of which were other Federal agency locations and charities. USBP agents may input charity addresses. However, charities only serve as temporary residences, not migrants' final destinations. Based on our analysis of USBP release data from March 2021 through August 2022, we identified at least 8,600 migrant release addresses associated with 25 charities. In these situations, migrants must update²⁹ any address changes³⁰ once they reach their final destination in the United States.

According to an ICE official, the U.S. Department of Justice's Executive Office for Immigration Review, which is responsible for conducting migrants' immigration court proceedings, advised against using charity addresses because legal documents should not be sent to locations where migrants temporarily reside. ICE personnel also stated they discourage USBP from using charity addresses because charities do not always share updated migrant addresses with ICE. In addition, the same ICE personnel stated some charities do not always forward migrants' mail. Agents at one USBP location noted they do not use charity addresses as migrants' U.S. point of contact because doing so creates tracking issues for ICE post-release.

ICE Did Not Always Validate Migrant Addresses Prior to USBP's Release into the United States

After USBP and ICE release migrants from custody, ICE is responsible for managing migrant cases. ICE guidance³¹ recommends officers validate ICE captured migrant addresses using USPS' website and, if necessary, update the migrant's address in its official system, EARM, prior to release.

ICE's method to validate U.S. addresses varied by location. For example, we noticed the following variations by location:

- ICE personnel validated some U.S. addresses using open-source websites, such as USPS and online search engines. Based on this level of analysis, some ERO deportation officers identified addresses of parks and commercial retail stores migrants listed as the location at which they would reside.

²⁹ U.S. Department of Justice Executive Office for Immigration Review EOIR-33/IC, *Change of Address/Contact Information Form, Immigration Court*. The information on this form is required by 8 U.S.C. § 1229(a)(1)(F)(ii) and 8 C.F.R. § 1003.15(d)(2) to notify the immigration court and the Office of the Principal Legal Advisor at ICE of any change(s) of address or phone number.

³⁰ For migrants released on Prosecutorial Discretion or Parole + ATD, migrants must notify ICE of their updated U.S. address.

³¹ ICE's *EARM Training Manual*, July 2021.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- ICE personnel did not validate some U.S. addresses provided by migrants. Because of limited time and resources at one location, ERO deportation officers did not perform any additional analysis of addresses and relied solely on USBP's validation [REDACTED]
- ICE personnel conducted more in-depth analysis to validate some addresses, such as searching DHS databases. Using additional analysis, one ICE deportation officer identified more than 100 migrants who used one individual's contact information as their point of contact in the United States.

USBP's and ICE's Inability to Capture and Validate Migrant Addresses Caused by Multiple Factors

In addition to migrants not having U.S. release addresses, DHS faced several challenges hindering its ability to record and validate migrant addresses as required. USBP agents were not able to fully validate addresses, given the large number of migrants apprehended each day and their limited coordination with ICE. DHS personnel were challenged by limited monitoring and authority over migrants who provide invalid addresses, and staff did not have adequate policies or resources to take further action.

Sectors With the Greatest Volume of Migrants had the Greatest Number of Errors

According to guidance, USBP agents should validate addresses provided, [REDACTED] However, during our interviews, agents stated they did not record and validate all addresses because the sectors had to focus more on transferring migrants out of custody within legal time limits,³³ dictated by policy, during upticks in illegal border crossings. As previously stated, from March 2021 through August 2022, USBP apprehended more than 1.3 million migrants illegally entering the United States at the Southwest border. This equates to between 43,000 to 106,000

³² USBP policy directs agents to validate addresses via e3. [REDACTED]

³³ CBP's *National Standards on Transport, Escort, Detention, and Search*, October 2015, states detainees should generally not be held for longer than 72 hours in CBP hold rooms or holding facilities. Every effort must be made to hold detainees for the least amount of time required for their processing, transfer, release, or repatriation as appropriate and as operationally feasible. See also 6 U.S.C. § 211(m)(1)-(3).

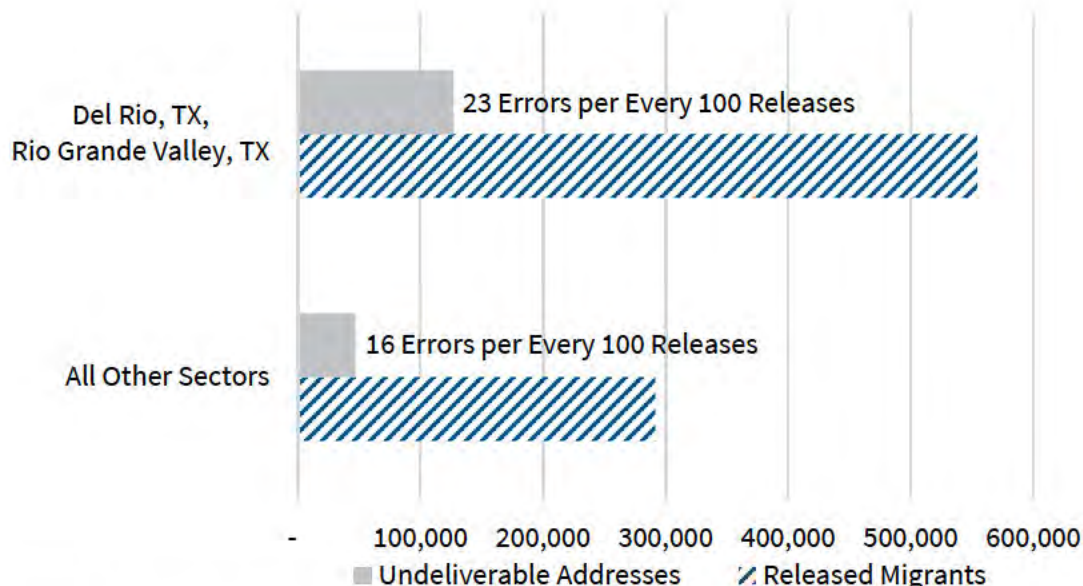


~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

apprehensions per month, or more than 2,000 per day.³⁴ Almost every USBP sector was at capacity during the time of this audit. Therefore, USBP needed to release migrants out of custody as quickly as possible.

The highest rates of undeliverable addresses occurred at the USBP sectors that apprehended some of the largest number of migrants from March 2021 through August 2022. For example, Del Rio and Rio Grande Valley sectors processed and released more than 550,000 migrants and had higher rates of invalid addresses than other sectors. Figure 4 details the USBP sectors with the greatest number of migrant releases and the number of invalid addresses.

Figure 4. Undeliverable Addresses and Total Migrant Releases by USBP Sector, March 2021–August 2022



Source: DHS OIG analysis of USBP address release data from March 2021 – August 2022

We also noted the number of missing addresses increased across all sectors during two separate migrant surges that occurred from March through August 2021, and from February through March 2022:³⁵

³⁴ This daily number is for Title 8 apprehensions only and does not include other USBP migrant encounters, which may further exacerbate issues.

³⁵ Collectively, USBP sectors' cumulative number of missing addresses increased from March through August 2021 and from February through March 2022. However, missing address trends varied by sector.

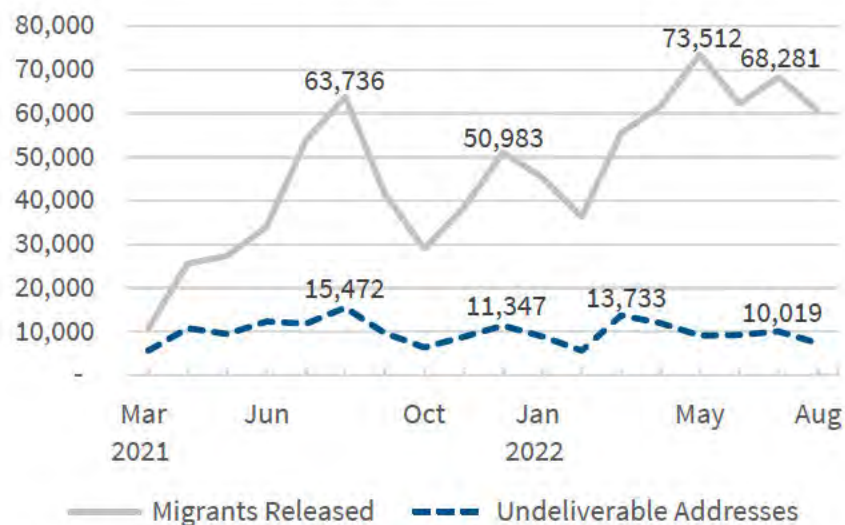


~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

- March through August 2021. The total number of migrants encountered at the entire Southwest border increased between 169 and 428 percent, respectively, compared to February 2021 rates. During the same period more than 30,000 migrants were released without an address.
- February through March 2022. The number of migrant apprehensions began to surge again from 56,000 in February 2022 to 87,000 in March 2022. During this period, the number of migrants released without an address also increased from more than 250 in February 2022 to more than 7,200 in March 2022.

As we noted in a 2022 report,³⁶ one ICE official noted an increase in migrant flow led USBP personnel to focus on speed rather than quality when entering migrant data. Figure 5 demonstrates the total undeliverable addresses, including no address, invalid addresses, and missing apartment numbers, identified compared to the total number of migrants released from March 2021 through August 2022.

Figure 5. Migrants Released by USBP and Undeliverable Addresses Identified March 2021–August 2022



Source: DHS OIG analysis of USBP address release data from March 2021 – August 2022

³⁶ *DHS Technology Systems Do Not Effectively Support Migrant Tracking at the Southwest Border*, OIG 22-66, September 2022.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Limited Coordination Between USBP and ERO

Address problems persisted throughout our fieldwork due to continued coordination challenges between USBP and ICE. Release terms require USBP to coordinate with ICE prior to migrant release into the United States for items such as COVID-19 testing and ATD. There is no requirement for coordination regarding U.S. addresses prior to release, even if the migrant does not have an address upon release. USBP did not always notify and coordinate with ICE³⁷ to validate addresses prior to migrant releases into the United States. Personnel at multiple ICE locations stated USBP released migrants without notifying ICE of the release. Therefore, ICE was unable to validate all migrant addresses captured prior to release.

Migrants may provide USBP the address to a fast-food restaurant prior to release, and ERO would not know where the migrant is located. – ERO Headquarters Official

Although ICE lists validating an address as a best practice, officers are not required by a policy to validate addresses prior to release. ICE is also not required by a policy to identify and report missing migrant addresses, invalid addresses, or potential human smuggling concerns. Additionally, ICE Headquarters does not consistently analyze migrant address data to identify errors or trends related to non-residential and recurring addresses. To mitigate some of these challenges, according to an ICE Headquarters official, ICE is implementing an information technology service³⁸ to validate and standardize migrants' post-release addresses recorded by ICE. However, this system enhancement was slated for release in March 2023 and will not include an analysis of all release records or standardization for USBP entered addresses.

Limited Authority for Verifying Invalid Migrant Addresses

According to CBP's *National Standards on Transport, Escort, Detention, and Search*, October 2015, detainees should generally not be held for longer than 72 hours in CBP hold rooms or holding facilities.³⁹ USBP guidance⁴⁰ recognizes not all migrants have a U.S. release address prior to release. USBP agents also stated they must release migrants even if the migrant has no address, or the U.S. address provided has been used multiple times. Once a

³⁷ According to USBP officials, USBP may not coordinate with ICE before releasing family units or migrants with medical conditions, among other reasons.

³⁸ ICE's Office of the Chief Information Officer expects the service to standardize ICE addresses by identifying errors, non-residential locations, and frequency of use.

³⁹ See 6 U.S.C. § 211(m)(1)-(3).

⁴⁰ According to an email from the Acting Deputy Chief Law Enforcement Operations Directorate at USBP on March 23, 2021, "agents must fill out an outward address... we acknowledge that subjects may not know and/or may not be precise in their responses."



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

migrant is released from USBP custody, ICE assumes responsibility for migrant tracking. USBP is not required based on their authority, and does not follow up post-release, to confirm the migrant is residing at the U.S. address obtained during processing.

Once USBP releases migrants from custody, ICE is unaware of some migrants' locations within the United States until migrants arrive at their final destinations, and only if they check in⁴¹ at a local ICE field office or notify ICE of address changes. If migrants do not check in with ICE within required timeframes, they may become a priority for further enforcement action because they are in the United States without lawful status. ICE makes enforcement decisions on a case-by-case basis, and only if officers can locate the migrant and have the resources to do so. At one field location, officers we interviewed noted they would not know a migrant's location or immigration status unless they looked it up on a case-by-case basis, and only do so if requested. At another field office we visited, an ERO deportation officer noted officers spend their days reviewing migrant cases at their desks and do not feel they are exercising law enforcement authority, for which they were hired. The same officer noted that, without a valid address to locate migrants, ICE may only locate migrants after they have been arrested by state or local police for unrelated offenses post-release. Only after the migrant's arrest would ICE be aware of the migrant's whereabouts. According to an ICE report, since March 2021, USBP released more than 127,000 migrants who were later arrested in the United States, including 5,500 criminal arrests and more than 122,000 non-criminal arrests, which included migrants considered as other immigration violators.⁴²

Limited Resources to Manage Immigration Enforcement

ICE does not have sufficient resources to oversee the volume of apprehended migrants. For example, ICE deportation officers at one field office were responsible for 35,000 migrant cases post-release, averaging about 3 minutes of staff time per case annually. ERO routinely details officers to the border, leaving fewer officers to perform enforcement functions at their assigned field offices. One senior ICE official acknowledged that, due to the high volume of cases, ICE deportation officers cannot always validate migrant addresses or effectively track if migrants check in at field offices, as required.

⁴¹ According to ICE's *Noncitizen CBP PD Release Dashboard*, ICE defines check-ins as making contact with an ICE office, as instructed (for at least one member if in a family unit), or by scheduling an appointment with ICE for a check-in.

⁴² The more than 127,000 arrests were made by ICE ERO and do not include migrants arrested by other Federal agencies or by state and local law enforcement.

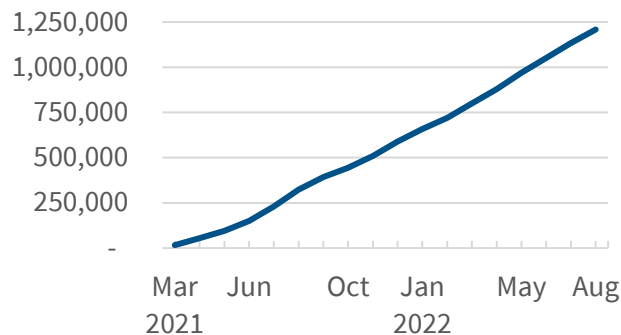


~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Conclusion

Upholding immigration laws and national security is critical, especially at the rate DHS is releasing migrants into the country. From March 2021 through August 2022, CBP and ICE released more than 1 million migrants into the United States, as shown in Figure 6.

Figure 6. Migrants Released by Quarter, March 2021 – August 2022



Source: DHS OIG-created based on USBP and ICE data

Despite this unprecedented number of releases, ICE still must be able to locate migrants to take immigration enforcement actions. If ICE does not have valid addresses for migrants who failed to report, it cannot issue valid NTAs for individuals released on ATD or NTRs. For example, ICE seeks to arrest individuals who pose potential threats to national security. ICE may also seek removal for migrants who are subjects to final orders of removal, are considered fugitive removals, or agree to voluntary departure from the United States. In other cases, ICE may simply need to locate migrants who need to be issued an NTA, which includes upcoming requirements for immigration proceedings and court hearings.

DHS saw an increase in migrants crossing the border. We also noted missing or invalid addresses and lower percentages of migrants checking in with ICE as required. We reviewed more than 25,000 address records for migrants with a dash (-) input as the address. More than 52 percent of those migrants did not check in with ICE as required, based on our analysis of ICE data. According to ICE data, the overall percentage of migrants who did not check in during our audit period was 28 percent. Figure 7 details check-in data by release type.⁴³ When migrants do not check in, ICE cannot ensure the migrant understands

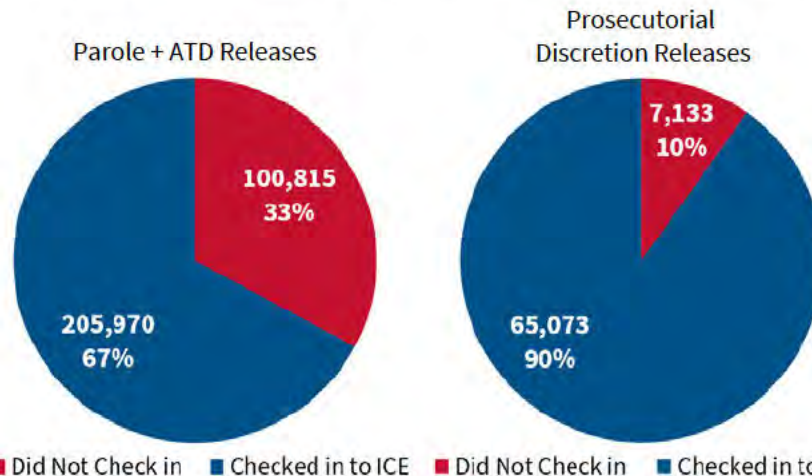
⁴³ This figure does not include migrants released by USBP on a Notice to Appear as migrants under that release type are not required to check in with ICE and must report to court instead.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

the next steps in the immigration process and cannot easily locate migrants who may be threats to public safety or are scheduled for removal.

Figure 7. Migrant Check in Rates by Release Type, March 2021 – August 2022



Source: DHS OIG analysis of migrant release data⁴⁴ extracted from the Unified Immigration Portal from March 2021 – August 2022⁴⁵

Finally, DHS may unknowingly release migrants, including children, to potentially unsafe conditions or smuggling operations. With the number of migrants released into the United States increasing and because USBP must release migrants in cases where the migrant does not have an address or it is uninhabitable, address validation will likely remain a challenge in the future.

Recommendations

Recommendation 1: We recommend the U.S. Customs and Border Protection Acting Commissioner and the Acting Director of U.S. Immigration and Customs Enforcement create and implement a plan of action to coordinate on requirements and processes when migrants do not have a valid U.S. address for release.

Recommendation 2: We recommend the Acting Director of U.S. Immigration and Customs Enforcement establish a policy for ICE field personnel to validate

⁴⁴ Check in rates for migrants released under Prosecutorial Discretion include more than 36,000 migrants who checked in past 60 days. In one example, migrants were apprehended in April 2021 but did not check in with ICE until January 2023.

⁴⁵ We obtained this data directly from the Unified Immigration Portal and, therefore, figures may vary with the background figures and slightly with the ICE rate of 28 percent for migrants who did not check in, as reported above.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

migrant addresses and to elevate address concerns, such as recurring or invalid migrant release addresses, recorded into U.S. Customs and Border Protection and ICE systems.

Recommendation 3: We recommend the Executive Associate Director of U.S. Immigration and Customs Enforcement's Enforcement and Removal Operations analyze migrant U.S. release address data on a recurring basis to identify trends, such as recurring and uninhabitable addresses, and share known address concerns with U.S. Border Patrol.

Recommendation 4: We recommend the Acting Director of U.S. Immigration and Customs Enforcement evaluate resources and address results for officers overseeing addresses for migrants released.

DHS Comments and OIG Analysis

The Department provided written comments in response to a draft of this report. We reviewed the Department's comments, as well as technical comments received under separate cover, and made changes to the report as appropriate. In the comments, the Department acknowledges obtaining valid addresses from migrants has been a longstanding issue. The Department stated that it has significantly improved how it processes noncitizens encountered along the U.S. borders and is currently implementing technology improvements to facilitate information sharing between DHS components and external agencies. DHS also indicated that since the conclusion of our fieldwork, ICE has deployed a new online change of address form, which included built-in address verification. DHS did not concur with our four recommendations. We have included a copy of the comments in their entirety in Appendix B. A summary of DHS' responses and our analysis follows.

DHS Response to Recommendation 1: Non-concur. According to DHS, ICE and CBP already coordinate with Federal counterparts when encountering migrants who are unable or reluctant to provide a valid address. Also, starting in November 2022, DHS and the Department of Justice implemented a process in which USBP schedules a hearing for noncitizens without an address in their intended destination city and issues them a Notice to Appear on a specialized docket. In these cases, the Department of Justice knows not to change the date, time, or location of these hearings to avoid any potential notice issues. If a migrant does not have a valid address, they are referred to ICE ERO for detention, as appropriate.

OIG Analysis: We do not consider DHS' actions responsive to the recommendation, which is unresolved and open. As discussed in our report,



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

once USBP releases the migrant from custody, and before their court appearance, ICE may have difficulty locating the migrant, if needed, for security purposes. Migrants without valid addresses are only referred to ICE “as appropriate.” The intent of the recommendation is for USBP to coordinate with ICE for all migrants without valid addresses to increase visibility of these migrants’ whereabouts. Although detention may not be appropriate or possible in all cases, increased levels of ATD or other tracking methods may improve the Department’s ability to locate migrants released into the United States without a valid address.

DHS Response to Recommendation 2: Non-concur. According to DHS, establishing a new policy for ICE personnel to validate addresses or elevate address concerns would be impractical or resource intensive without adding commensurate value. ICE ERO cannot issue a policy concerning the release of noncitizens who are in the custody of a separate agency. The burden is on the noncitizen to provide a valid address. Further, establishing a policy for ICE field personnel to validate migrant addresses will not resolve the issue because not all migrants are in ICE custody.

OIG Analysis: We do not consider DHS’ actions responsive to the recommendation, which is unresolved and open. Although DHS claims implementing address validation practices would be impractical or resource intensive, ICE personnel at many sites we visited already do so. For example, we learned through our visits to various locations that ICE reviews many USBP-collected migrant addresses prior to their release into the United States. Implementing a policy, as recommended, to standardize this practice across the component would provide ICE personnel formalized guidance to follow, especially when they encounter recurring addresses, which may indicate these locations are used for human trafficking.

DHS Response to Recommendation 3: Non-concur. According to DHS, neither ICE ERO nor CBP have had in the past, or at present, the resources available to regularly perform this analysis, given competing priorities and demands. These demands include ICE ERO’s focus on enforcement actions against individuals who pose a public safety threat and processing noncitizens for release into the United States with instructions to report to an ICE office to complete processing.

OIG Analysis: We do not consider DHS’ actions responsive to the recommendation, which is unresolved and open. As discussed in our report, ICE has already begun efforts in line with our recommendation. Fully implementing this recommendation would ensure ICE continues progress by formalizing comprehensive trend analysis, which ICE personnel can, in turn,



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

share with USBP for their awareness as they encounter migrants. Alerting USBP of known concerning addresses may save ICE both time and resources by reducing the number of migrants ERO personnel must search for who did not provide a valid address prior to release. Identifying these trends may also limit the number of migrants, including children, who may end up in unsafe environments.

DHS Response to Recommendation 4: Non-concur. According to DHS, all Department components, including ICE, regularly evaluate resources to maximize the effectiveness and efficiency of operations. ICE noted the benefits to this recommendation would be unclear as our report tested USBP releases, not ICE releases.

OIG Analysis: We do not consider DHS' actions responsive to the recommendation, which is unresolved and open. Although the Department may regularly review its resources, our report highlights a critical component of the address verification process left incomplete due to resource issues. Specifically, ICE personnel we interviewed in the field did not analyze addresses because of these specific resource limitations.

Although ICE is uncertain it will benefit from implementing this corrective action, ICE already reviews some migrant release addresses captured by USBP prior to release, and even after release. Fully implementing the recommendation will help ICE identify and potentially devote the resources needed to evaluate migrant addresses consistently daily in the field prior to a migrant's release into the United States, and on a recurring basis at Headquarters post-release to identify trends.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine the extent to which DHS accurately and effectively tracks migrants' post-release addresses in the United States. The scope of this audit included U.S. release addresses provided by adult and migrant families apprehended by USBP between ports of entry at the Southwest border from March 2021 through August 2022 and released under Title 8. We focused on the extent to which USBP and ICE used IT systems to obtain, validate, and track migrants' post-release addresses. We determined through audit work whether the Department reviews system data to identify abnormalities of migrant addresses, such as errors and recurring or uninhabitable addresses.

During this audit, we researched and reviewed Federal laws as well as departmental and component policies and procedures related to USBP and ICE information technology systems, training manuals, and processes associated with the post-release address data entry, validation, and tracking of migrants released into the United States. To answer our objective, we conducted more than 20 virtual and in-person interviews. We interviewed the following USBP personnel:

- USBP Headquarters personnel in Washington, DC;
- Del Rio Sector, Boulevard and Chula Vista Stations in the San Diego Sector; and
- Central Processing Centers in El Paso and Rio Grande Valley Sectors.

We interviewed ICE personnel in:

- Office of the Chief Information Officer and the Domestic Operations Division in Washington, DC;
- ERO's Non-Detained Management Division in Phoenix, AZ, and Washington DC;
- ERO field offices in San Diego, CA; El Paso and Harlingen, TX; Philadelphia, PA; Baltimore, MD; and Miami, FL;
- ICE Intelligence Units in San Diego, CA and El Paso, TX, and the ATD Division in Phoenix, AZ; and
- ICE contractor's ATD Program Unit.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

The purpose of our interviews was to obtain an understanding of USBP and ICE processes used to obtain and record, validate, and track migrants' post-release U.S. addresses. We obtained and analyzed more than 100 documents and email correspondences from USBP, ERO, and ICE's ATD contractor to support the work conducted and audit findings. In addition to interviewing USBP and ICE personnel, we received virtual walkthroughs of IT systems and process pathways, and conducted physical site visits to observe ICE migrant check-ins. We also conducted physical site visits to observe 28 judgmentally selected post-release migrant U.S. addresses in Georgia, Illinois, Maryland, and New Jersey.

We assessed data reliability by (1) interviewing USBP and ICE officials knowledgeable about the data, (2) reviewing existing information about the data and the systems that produced it, (3) performing electronic testing of data used for our analysis, (4) reviewing data from CBP's Unified Immigration Portal and ICE's Enforcement Integrated Database, as well as (5) observing data entry in CBP's e3 system and ICE's EARM system during site visits and screen shares.

In addition to having direct access to the Unified Immigration Portal, we leveraged our Office of Innovation to obtain data relevant to our objective and conduct validity testing for address data⁴⁶ from CBP and ICE systems. Our Office of Innovation tested address data for validity and duplication. The Office of Innovation staff cleaned, standardized, and validated USBP address data using third-party address verification and validation software.⁴⁷ They also used the address software to format addresses according to USPS postal standards. The total count of address records obtained and analyzed from USBP was 981,671.

We assessed internal controls and information systems related to CBP and ICE's ability to record valid addresses and track migrants' post-release U.S. addresses. Based on our assessment, CBP and ICE do not have adequate internal controls to record valid addresses and track migrants' post-release U.S. addresses. We identified internal control weaknesses in the body of this report. However, since our internal control assessment was limited to the audit objective, it may not have disclosed other internal control deficiencies that potentially existed.

We conducted this performance audit from July 2022 through March 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and

⁴⁶ Migrant data tested included single adults and family unit members but did not include unaccompanied children, who were outside of the scope of our audit.

⁴⁷ Informatica Address Verification.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

DHS OIG's Access to DHS Information

During this audit, DHS provided timely responses to the information we requested and did not delay or deny DHS OIG's access to DHS information.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B

DHS Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20538



**Homeland
Security**

July 19, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

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

SUBJECT: Management Response to Draft Report: "DHS Does Not Have Assurance That All Migrants Can be Located Once they Are Released into the United States"
(Project No. 22-054-AUD-ICE, CBP)

JIM H. CRUMPACKER
Digitally signed by JIM H. CRUMPACKER
Date: 2023.07.19 15:04:50 -0400

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

DHS leadership is pleased to note the OIG's recognition that the Department ensures the safety and security of the nation's borders while managing a safe, orderly, and humane immigration system. Obtaining valid addresses from migrants has been a longstanding issue across different Administrations since the passing of the Immigration and Nationality Act in 1952.

DHS has made significant improvements to how it processes noncitizens encountered along our borders and has additional technology improvements currently underway to facilitate better information sharing to support accurate and timely processing among various Components and agencies. A key effort is the U.S. Customs and Border Protection's (CBP) Unified Immigration Portal (UIP), which connects datasets from the Department of Health and Human Services, U.S. Citizenship and Immigration Services, U.S. Immigration and Customs Enforcement (ICE), and the Department of Justice (DOJ), to provide integrated digital processing capabilities that support the end-to-end electronic review and approval throughout the immigration lifecycle.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

In addition, in April 2023, ICE deployed a new online change of address form.¹ This new form includes built-in address verification, which officers currently use along with existing public websites, such as the United States Postal Service and Google Maps, to validate addresses provided by migrants. CBP and ICE remain committed to protecting America and safeguarding our borders, preserving national security and public safety, and enhancing the nation's economic prosperity.

The draft report contained four recommendations, with which the Department non-concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Enclosure

¹ <https://onlinechangeofaddress.ice.gov/ocoa>



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

**Enclosure: Management Response to Recommendations
Contained in 22-054-AUD-ICE, CBP**

OIG recommended the Acting Commissioner of CBP and the Acting Director of ICE:

Recommendation 1: Create and implement a plan of action to coordinate on requirements and processes when migrants do not have a valid U.S. address for release.

Response: Non-concur. DHS and its Components already coordinate with federal counterparts when encountering migrants who are unable or are reluctant to provide a valid address. For example, USBP follows an existing process that addresses the intent of this recommendation. Specifically, on November 1, 2022, DHS, in coordination with DOJ's Executive Office for Immigration Review (EOIR), implemented an updated process, whereby CBP USBP and other offices, as appropriate, schedule noncitizens that do not have an address and issue them a Notice to Appear (NTA) on a specialized "E-33 docket" in the noncitizen's intended destination city for an initial master calendar hearing 120 days from the date of NTA issuance. For cases on the E-33 docket, EOIR knows not to change the date, time, and location of these hearings to avoid potential notice issues. Additionally, when the individual comes in for their initial E-33 docket hearing, they are first directed to the court window to provide an EOIR-33 change of address form so that their current address can be recorded for any further communications or notices.

In addition, as a matter of practice USBP refers migrants without a valid address to ICE's Enforcement and Removal Operations (ERO) for detention, as appropriate.

DHS requests that the OIG consider this recommendation resolved and closed.

OIG recommended the Acting Director of ICE:

Recommendation 2: Establish a policy for ICE field personnel to validate migrant addresses and to elevate address concerns, such as recurring or invalid migrant release addresses, recorded into U.S. Customs and Border Protection and ICE systems.

Response: Non-concur. Establishing a new policy would be impractical and resource intensive without adding commensurate value. ICE ERO is not solely responsible for validating migrant addresses; it is a joint effort among several federal agencies, including those outside of DHS (such as DOJ's EOIR), to obtain and use this information. ICE ERO cannot issue a policy concerning the release of noncitizens who are not in ICE custody, but rather in the custody of a separate agency. The burden is on the noncitizen to provide a valid address. Further, establishing a policy for ICE field personnel to validate migrant addresses will not resolve the issue because not all migrants are in ICE custody.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

It is also important to note that in April 2023, ICE deployed a new online change of address form. This new form includes built-in address verification, which officers currently use along with existing public websites, such as the United States Postal Service and Google Maps, to validate addresses. DHS has a process to maximize the collection of valid addresses for migrants which considers the reality that some migrants are unable or reluctant to provide an address to federal agents. Further, although a noncitizen may provide an address at the time of encounter, even with DHS verifying the address [REDACTED] there is no guarantee the noncitizen will reside at that address.

ICE requests that the OIG consider this recommendation resolved and closed.

OIG recommended the Executive Associate Director of ICE ERO:

Recommendation 3: Analyze migrant U.S. release address data on a recurring basis to identify trends, such as recurring and uninhabitable addresses, and share known address concerns with U.S. Border Patrol.

Response: Non-concur. Although DHS regularly analyses available data, neither ICE ERO nor CBP have had in the past, nor have at present, the resources available to perform this analysis on a recurring (or scheduled) basis, given competing priorities and demands. For example, ICE ERO's resources should be focused on enforcement actions against individuals who pose a public safety threat and processing noncitizens who were released into the interior of the United States with instructions to report to an ICE office to complete processing. Moreover, ICE ERO is not solely responsible for validating migrant addresses, so the recommendation would require resource-intensive work across multiple agencies that will not produce actionable data given that many migrants cannot or are reluctant to provide a valid address.

ICE requests that the DHS OIG consider this recommendation resolved and closed.

OIG recommended the Acting Director of ICE:

Recommendation 4: Evaluate resources and address results for officers overseeing addresses for migrants released.

Response: Non-concur. DHS Components, including ICE, regularly evaluate their resources to maximize the effectiveness and efficiency of their operations. For instance, in July 2021, ICE ERO assessed and realigned Southwest Border resources to create a more efficient and effective operational structure to address migrants being released on the Southwest Border. Accordingly, the ERO Harlingen area of responsibility was established on October 1, 2021, to manage the workload and resources more equitably



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

along the Southwest Border.

Additionally, ICE and CBP have implemented more robust technology such as using the UIP and the Case Acceptance Screen (CAS) for CBP officers encountering noncitizens at borders, which also provides alerts to ICE officials when making custody determinations. UIP and the CAS system allow more cohesive case coordination between CBP and ICE with automated processes, including viewing electronic A-Files inclusive of individual case addresses and providing case acceptance/rejection responses back to CBP and data evaluation.

As previously noted, neither ICE ERO nor CBP have the resources available to identify and analyze migrant-provided address information on a recurring (or scheduled) basis as recommended. It is also unclear what benefits would accrue to offset the costs of such analysis, because 100 percent of the migrant releases studied as part of OIG's report were CBP-releases. Thus, any analysis of ICE resources to address the issue of this subset of migrants would not yield any impact on DHS's oversight of these migrants. Instead, ICE ERO's limited resources are needed to address the significant backlog of non-detained migrants who were released into the interior United States without being issued NTAs.

ICE requests that the OIG consider this recommendation resolved and closed as implemented.



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C

[REDACTED]

[REDACTED]

[REDACTED]



~~LAW ENFORCEMENT SENSITIVE~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D **Report Distribution**

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Acting Commissioner, CBP
Acting Director, ICE
ICE Liaison
USBP Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

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

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



OIG HOTLINE

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

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



September 2023

BIOMETRIC IDENTITY SYSTEM

DHS Needs to Address Significant Shortcomings in Program Management and Privacy

Why GAO Did This Study

DHS currently uses an outdated system, implemented over 29 years ago, for providing biometric identity management services (e.g., fingerprint matching). The system stores over 290 million identities. In 2016, DHS initiated a multi-billion dollar program known as HART, which is intended to replace the legacy system. GAO previously reported that due to several challenges, in 2017 the program breached its schedule baseline. In 2019 the program established new cost and schedule commitments with DHS leadership (referred to as a rebaseline). This resulted in delaying the program by 3 years.

GAO was asked to evaluate the HART program. This report's objectives were to (1) determine how the HART program has changed since the 2019 baseline, (2) assess the extent to which the program's cost and schedule estimates followed best practices, and (3) assess the extent to which DHS implemented selected privacy requirements for the program.

GAO reviewed HART planning documentation, evaluated cost and schedule estimates against best practices identified by GAO, and compared privacy documentation to selected Office of Management and Budget privacy requirements. GAO also interviewed appropriate officials.

What GAO Recommends

GAO is making nine recommendations to DHS to follow best practices when preparing HART cost and schedule estimates and implement selected privacy requirements for the system. DHS concurred with the recommendations.

View [GAO-23-105959](#). For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcainm@gao.gov.

BIOMETRIC IDENTITY SYSTEM

DHS Needs to Address Significant Shortcomings in Program Management and Privacy

What GAO Found

Since rebaselining its original cost and schedule commitments in 2019, the Department of Homeland Security's (DHS) Homeland Advanced Recognition Technology (HART) program has further delayed its schedule. Specifically, in 2020 the program declared a second schedule breach and its first cost breach. Accordingly, DHS rebaselined the program again. This extended the schedule for delivering the initial capabilities to replace the legacy system by an additional 33 months beyond the 2019 plan. In addition, the 2022 rebaseline did not include an estimate for completing the program (see table).

Changes in the Homeland Advanced Recognition Technology (HART) Program Schedule from 2019 to 2022

Milestone	Planned completion date ^a (as of May 2019)	Planned completion date ^a (as of May 2022)
Initial operational capability	December 31, 2020	September 30, 2023
Complete full program	June 30, 2024	Not yet planned

Source: GAO analysis of Department of Homeland Security data. | [GAO-23-105959](#)

^aThis represents the schedule threshold dates defined in the HART acquisition program baseline.

Regarding costs, the program's 2022 rebaseline increased its estimated costs by \$354 million. In April 2023, program officials stated that they needed to rebaseline HART's schedule a third time due to, among other things, higher than expected software defects and performance issues.

The program's 2022 cost and schedule estimates did not fully follow GAO's identified cost and schedule best practices and were, therefore, unreliable. Specifically, the program's cost estimate did not substantially or fully meet the four characteristics of a reliable cost estimate. Moreover, the program's schedule estimate did not substantially or fully meet three of the four characteristics of a reliable schedule estimate. Until these weaknesses are addressed, the HART cost and schedule estimates will continue to be unreliable. In turn, this will impair the ability of senior leadership to make informed decisions regarding the program's future.

DHS fully implemented five of 12 selected Office of Management and Budget privacy requirements. For example, the program addressed the requirement to appropriately encrypt information by demonstrating encryption settings for information at rest and in transit. However, DHS had gaps in the remaining seven requirements. For example, the program's privacy impact assessment, which is intended to analyze how personal information is collected, shared, and managed, was missing key information. Specifically, the assessment was missing information on (1) individuals whose data will be stored in the system and (2) the partners with whom the system will share information. In addition, the program did not have assurances that partners that provide information to the system will appropriately retain and dispose of personally identifiable information. Until DHS addresses these privacy weaknesses, the department lacks assurance that the hundreds of millions individuals' personally identifiable information that will be stored and shared by HART will be appropriately protected.

Contents

Letter		1
	Background	5
	The HART Program Experienced Schedule Delays and Cost Increases since the 2019 Rebaseline	13
	HART Cost and Schedule Estimates Were Unreliable	19
	DHS Did Not Fully Implement a Majority of Selected Privacy Requirements for HART	24
	Conclusions	34
	Recommendations for Executive Action	34
	Agency Comments and Our Evaluation	36
Appendix I	Objectives, Scope, and Methodology	40
Appendix II	Results of GAO's Assessment of the HART Program Cost Estimate Compared with Best Practices	46
Appendix III	Results of GAO's Assessment of the HART Program Schedule Compared with Best Practices	48
Appendix IV	Comments from the Department of Homeland Security	49
Appendix V	GAO Contacts and Staff Acknowledgments	59
Tables		
	Table 1: Changes in the Homeland Advanced Recognition Technology's (HART) Program Schedule from 2019 to 2022	15
	Table 2: Assessment of the Homeland Advanced Recognition Technology (HART) Program Cost Estimate Compared to Characteristics for a Reliable Cost Estimate Using GAO's <i>Cost Estimating and Assessment Guide</i> , as of March 2022	20

Table 3: Assessment of the Homeland Advanced Recognition Technology (HART) Program Schedule Compared to Characteristics for a Reliable Schedule Using GAO's <i>Schedule Assessment Guide</i> , as of June 2022	23
Table 4: Summary of Department of Homeland Security's (DHS) Implementation of Selected Office of Management and Budget Privacy Requirements for the Homeland Advanced Recognition Technology (HART) Program	25
Table 5: Assessment of the Homeland Advanced Recognition Technology Program's Cost Estimate Compared to Best Practices, as of March 2022	46
Table 6: Assessment of the Homeland Advanced Recognition Technology (HART) Program's Schedule Estimate Compared to Best Practices, as of June 2022	48

Figures

Figure 1: Homeland Advanced Recognition Technology (HART) Key Partners	7
Figure 2: Simplified Planned Process Flow between U.S. Customs and Border Protection and the Homeland Advanced Recognition Technology (HART) System for Biometric Identification and Verification for Air, Land, or Sea Entry	9
Figure 3: Timeline of Homeland Advanced Recognition Technology (HART) Acquisition Program Baselines and Breaches	14
Figure 4: Changes in the Homeland Advanced Recognition Technology (HART) Life Cycle Cost Estimate from May 2019 to May 2022	18

Abbreviations

DHS	Department of Homeland Security
HART	Homeland Advanced Recognition Technology
IDENT	Automated Biometric Identification System
OBIM	Office of Biometric Identity Management
OMB	Office of Management and Budget
PIA	privacy impact assessment
PII	personally identifiable information
SAOP	Senior Agency Official for Privacy

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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.



September 12, 2023

The Honorable Gary C. Peters
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Ron Johnson
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

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

Biometric identity management services, such as fingerprint matching and facial recognition technology, are commonly used across business and government sectors as tools for identifying an individual or verifying an individual's identity. Within the Department of Homeland Security (DHS), the Management Directorate's Office of Biometric Identity Management (OBIM) is the lead entity responsible for providing biometric identity management services.

OBIM's mission is to provide biometric identity services that support national security and public safety decision making for DHS and its partners. OBIM provides services to several DHS components (e.g., U.S. Customs and Border Protection and Federal Emergency Management Agency); as well as the Departments of State, Justice, and Defense; tribal, state, local, and territorial law enforcement; the intelligence community; and international partners.

DHS currently provides biometric identity management services through the Automated Biometric Identification System (IDENT), which became operational over 29 years ago.¹ Among other things, the department uses IDENT to store biographic (e.g., full name, date of birth, and country of origin) and biometric information (e.g., fingerprints, facial features, and iris

¹IDENT became operational in 1994.

patterns) on U.S. citizens and foreign nationals. It then shares that information with partners to facilitate legitimate travel, trade, and immigration.²

However, in 2011 DHS reported that IDENT had significant shortcomings such as system capacity constraints, a lack of ability to handle multiple types of biometric information, and limitations on accuracy and assurance. To mitigate these challenges, DHS initiated the Homeland Advanced Recognition Technology (HART) program in 2016 to replace IDENT and to provide additional capabilities.³

The HART system is intended to be a centralized DHS-wide biometric database, which stores and manages over 290 million individuals' personally identifiable information (PII), including biographic and biometric information.⁴ HART was originally estimated to cost about \$4.2 billion and to be fully implemented by 2021.⁵

In June 2017, the HART program determined it would not be able to meet its initial acquisition program baseline milestones and declared a schedule breach. DHS rebaselined the HART program 2 years later (in May 2019) in response to the breach. However, in June 2021, we reported that the program was significantly behind schedule and had exceeded its most recent cost estimate.⁶

²We generally use the term "foreign national" to refer to an "alien," which is defined under U.S. immigration law as any person who is not a U.S. citizen or national. See 8 U.S.C. § 1101(a)(3). In addition, temporary visitors are foreign nationals present in the United States on a temporary basis pursuant to a specific nonimmigrant category (see 8 U.S.C. § 1101(a)(15); 8 C.F.R. § 214.1(a)(1)-(2)), including those who are allowed to seek admission without a visa.

³Examples of enhanced functionality include tools to improve human examination of multiple types of biometric information when verifying individuals, a web portal to improve accessibility and provide users with a single web-based point of access to the HART system, and the use of additional types of biometric information such as DNA.

⁴In general, PII is any information that can be used to distinguish or trace an individual's identity, such as name, date or place of birth, and biometric records; or that otherwise can be linked to an individual.

⁵This figure represents the program's life cycle cost estimate established by DHS and OBIM in April 2016. It is presented in base-year 2016 dollars at a 50 percent confidence level and does not include the effects of inflation.

⁶GAO, *Homeland Security: DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System*, [GAO-21-386](#) (Washington, D.C.: June 8, 2021).

In addition, in 2022, we highlighted that the potential for breaches of biometric information, such as facial images and iris scans, at federal agencies could result in this sensitive information being revealed to unauthorized entities.⁷ A breach involving this information may have more serious consequences than the breach of other PII because, unlike conventional identification methods, biometric technologies measure things that are generally distinct to each person and cannot easily be changed.

You asked us to review the HART program. Our specific objectives were to (1) determine how the HART program has changed since the 2019 baseline, (2) assess the extent to which the HART program's cost and schedule estimates followed best practices, and (3) assess the extent to which DHS implemented selected privacy requirements for the HART program.

To address the first objective, we reviewed HART planning documentation to describe the schedule and cost changes that HART has experienced since the 2019 DHS approved baseline. Specifically, we compared the HART schedule and life cycle cost estimates from 2019 to 2022. We also reviewed relevant documentation to describe the status of the program. In addition, we interviewed HART program office officials regarding changes in the program schedule and cost.

To address the second objective, we reviewed and assessed the HART program's cost and schedule estimates from March 2022 and June 2022, respectively. To assess HART's cost estimate, we evaluated documentation against best practices associated with the characteristics of a reliable cost estimate identified in *GAO's Cost Estimating and Assessment Guide*.⁸ To assess HART's schedule, we evaluated supporting documentation against best practices associated with the characteristics of a reliable schedule identified in *GAO's Schedule Assessment Guide*.⁹

For both assessments, we also interviewed program officials responsible for developing and managing the program estimates. We provided OBIM and HART program officials with draft versions of our detailed analyses of

⁷GAO, *Facial Recognition Technology: Federal Agencies' Use and Related Privacy Protections*, [GAO-22-106100](#) (Washington, D.C.: June 29, 2022).

⁸GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar. 12, 2020).

⁹GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, [GAO-16-89G](#) (Washington, D.C.: Dec. 22, 2015).

the program's cost and schedule estimates to verify that the information on which we based our findings was complete, accurate, and up-to-date.

We determined that the cost and schedule data provided by OBIM was not complete and reliable. We discuss the limitations of these data in the report and we have made appropriate attribution indicating the sources of these data.

To address the third objective, we assessed HART program documents and privacy-related artifacts against selected privacy requirements. Specifically, we selected 12 privacy requirements from Office of Management and Budget (OMB) guidance, including *Managing Information as a Strategic Resource* and *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.¹⁰

Next, we assessed HART program documentation, including the privacy impact assessment (PIA), system security and privacy plan, records retention schedules, contracts, and information sharing and access agreements inventory and documentation, against the selected requirements. We also interviewed officials from OBIM and other offices within DHS regarding their efforts to implement privacy requirements for HART.

We assessed the reliability of data contained in the system security and privacy plan as well as the information sharing and access agreement inventory by reviewing related documentation and examining these data to identify missing or incorrect information. We followed up with the appropriate officials, as needed. We determined that these data contained in the system security and privacy plan were sufficiently reliable for our reporting objective. We determined that the inventory was not reliable because it was incomplete. We discuss the limitations of these data in the report. A detailed discussion on our objectives, scope, and methodology is provided in appendix I.

We conducted this performance audit from April 2022 to July 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our

¹⁰OMB, Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016); Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, (Washington, D.C.: Sept. 26, 2003); and Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a); E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (2002).

findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

OBIM uses a 29-year-old system known as IDENT to provide DHS and its partners with biometric identity services.¹¹ The partners use the results from IDENT to perform critical functions, including:

- determining visa issuance and admissibility into the United States;
- establishing eligibility for immigration benefits, including asylum and refugee status;
- determining whether an individual should be granted access to a sensitive facility or sensitive system;
- taking law enforcement actions with potential homeland security implications; and
- verifying the identity of persons associated with matters of national security.

However, in 2011, DHS reported that IDENT had significant shortcomings. Specifically, the department reported that IDENT had:

- significant system capacity constraints,
- a lack of ability to handle multiple types of biometric information,
- the need for improved performance and availability,
- limitations on accuracy and assurance,
- the need for increased interoperability and achievement of cost efficiencies,
- the need for IT security compliance, and
- an inability to meet other current and future mission requirements.

To mitigate these shortcomings, the department initiated the HART program in 2016 to replace IDENT and to provide additional capabilities. At that time, OBIM planned to implement HART in four increments.

¹¹IDENT matches, stores, and shares biometric and biographic information that are collected from individuals by partners. OBIM's partners include several DHS components (e.g., U.S. Customs and Border Protection and Federal Emergency Management Agency); as well as the Departments of State, Justice, and Defense; tribal, state, local, and territorial law enforcement; the intelligence community; and international partners.

Increment 1 included the core foundational infrastructure necessary to replace IDENT, operate HART, and to achieve initial operational capability. Once the office completed increment 1, all partners were expected to have migrated from IDENT to HART, thus making HART the system of record. Following this transition, OBIM officials intended to decommission IDENT.

Increments 2 through 4 were intended to deliver additional capabilities, such as using two forms of biometric information to identify and verify an individual (referred to as multimodal fusion);¹² using additional types of biometric information such as DNA, palm, and voice; and performing additional analysis and reporting functions.¹³

HART Is to Store and Share Biometric Information to Identify and Verify Individuals' Identities

Similar to IDENT, HART is intended to match, store, and share biometric and associated biographic information. The partners collect and provide this information in the course of carrying out their missions and submit it to HART. Using HART's biometric identity services, the partners may also submit queries to the system to identify or verify an individual's identity.¹⁴

OBIM has documented approximately 140 partners that will provide information to HART and/or use the system's biometric identity services.¹⁵ Figure 1 depicts key partners that submit data to HART and/or use the system's biometric identity services.

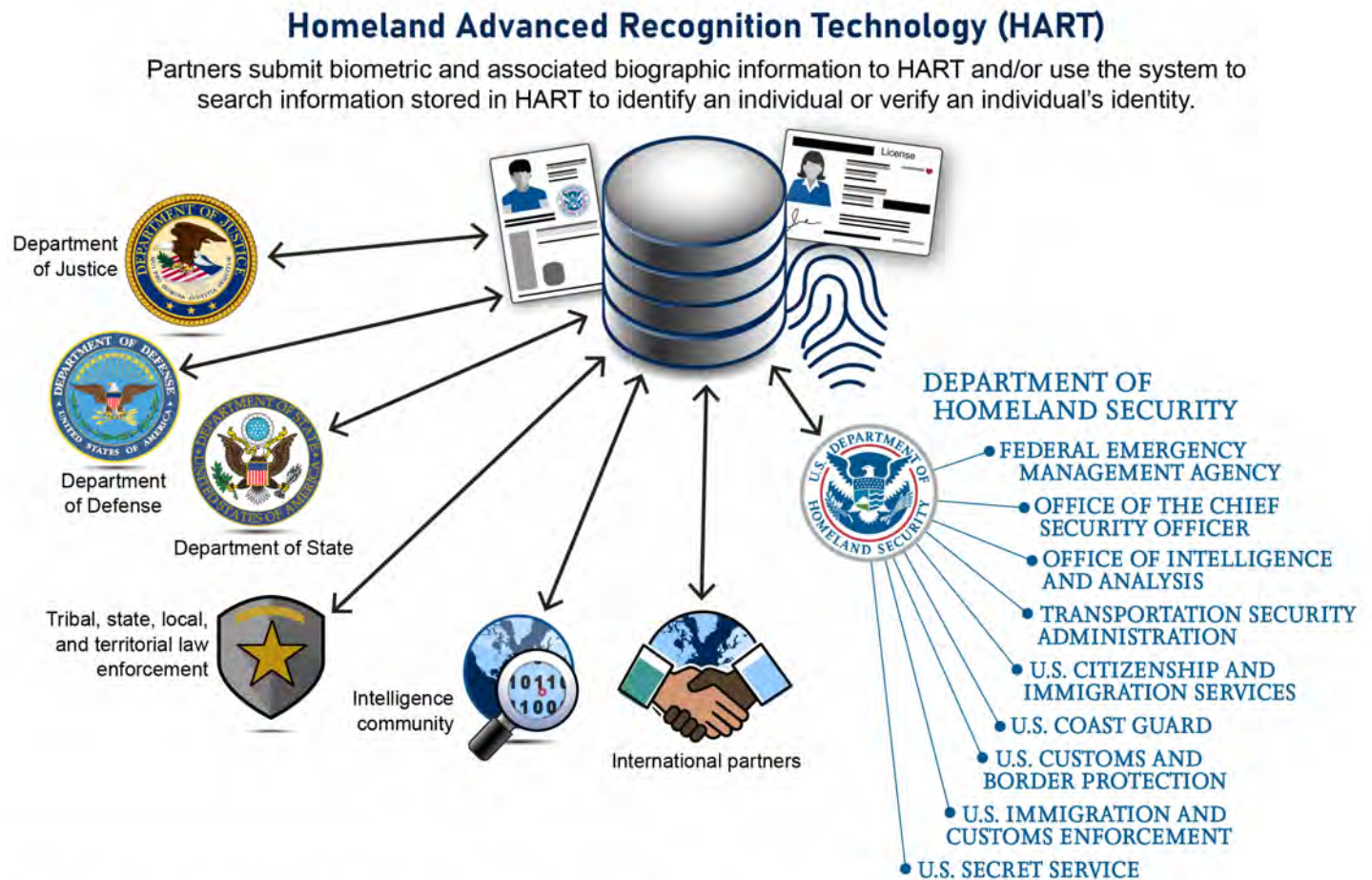
¹²Multimodal fusion is intended to allow for the combining of information from multiple types of biometrics (such as fingerprint and iris pattern) to provide more efficient and accurate identification services and reduce the burden on examiners.

¹³The planned analytic and reporting capabilities are intended to identify trends and patterns, and increase the ability to detect activities requiring immigration or law enforcement action, among other things.

¹⁴Most partners are considered data providers as well as data users. This means that these partners will submit biometric and biographic information to HART, as well as use the system to search information stored in HART to identify an individual or verify an individual's identity. A small subset of the partners will provide information to HART, but will not query the system. This includes partners that will provide historical information, such as gang affiliations. There are also rare instances where partners will only query the system, but will not provide information to the system. For example, according to OBIM officials, DHS personnel that assist with the Freedom of Information Act requests may search for and extract information to fulfill those requests, but will not provide individuals' information to HART to be stored by the system.

¹⁵OBIM's documentation identifies partners at the organization, unit, and subunit level. For example, there are seven subunits associated with the Department of State, including one for the Consular Affairs Office's Immigrant Visa Applications and another for Non-Immigrant Visa Applications.

Figure 1: Homeland Advanced Recognition Technology (HART) Key Partners



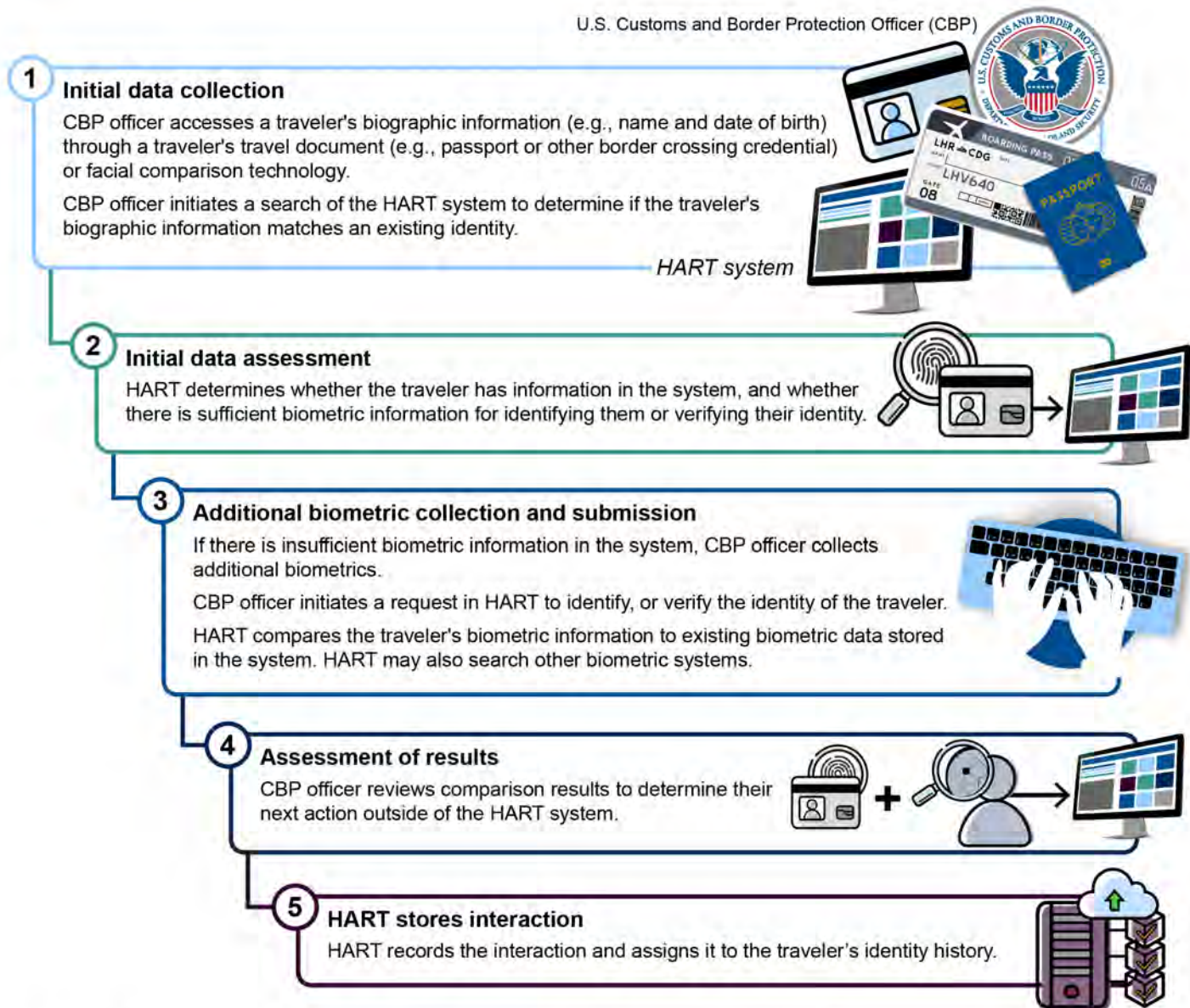
Sources: GAO (analysis of Department of Homeland Security data; icons); agencies (logos). | GAO-23-105959

Similar to their use of IDENT, partners will be expected to use HART for different purposes. For example, among other things, the Department of State is expected to use HART to support biometric identification and verification of international travelers seeking U.S. visas to help determine if visas should be issued. The Transportation Security Administration is expected to rely on the system to retrieve identity information for trusted travelers scheduled to fly within the next 24 hours for use in identity verification at airport security checkpoints. In addition, U.S. Customs and Border Protection is expected to use HART to support biometric identification and verification of in-scope travelers entering and exiting the

U.S. through air, sea, and land ports of entry.¹⁶ Figure 2 describes the planned process flow by which a U.S. Customs and Border Protection officer may use the system.

¹⁶In-scope international travelers do not include: U.S. citizens; Canadian citizens visiting the United States temporarily for business or pleasure; visitors admitted on a specified visa; children under the age of 14 (unless participating in a trusted traveler program); persons over the age of 79; classes of visitors the Secretary of State and the Secretary of Homeland Security jointly determine shall be exempt; an individual visitor the Secretary of State, the Secretary of Homeland Security, or the Director of the Central Intelligence Agency determines shall be exempt; and Taiwanese officials who hold the specified visas and members of their immediate families who hold these same visas.

Figure 2: Simplified Planned Process Flow between U.S. Customs and Border Protection and the Homeland Advanced Recognition Technology (HART) System for Biometric Identification and Verification for Air, Land, or Sea Entry



Sources: GAO (analysis of agency data; icons); CBP (logo); James Thew/stock.adobe.com; Buffaloboy/stock.adobe.com. | GAO-23-105959

Storing Vast Quantities of PII Poses Privacy Risks

The HART system is expected to store vast quantities of biometric and biographic PII. As of April 2023, OBIM officials stated that IDENT stored more than 290 million separate and distinct identities. In addition, prior to

the Coronavirus Disease pandemic, the IDENT fingerprint gallery was growing at a rate of approximately 2 million fingerprint records each month. OBIM also reported that, on average, the system processed nearly 350,000 transactions daily. The office officials projected that the transaction volumes would return to the pre-pandemic levels and that the number of stored biometrics would continue to increase.

The protection of personal privacy has become a more significant issue in recent years with the increasing amount of data that agencies and other organizations collect, as well as new techniques available for analyzing them. For example, advances in technology, such as new search technology and data analysis software, have made it easier for individuals and organizations to correlate information and track it across large and numerous databases. Recognizing these challenges, we expanded our information security high-risk area in 2015 to include protecting the privacy of PII.¹⁷

In 2022, we highlighted privacy risks specifically related to facial recognition technology, such as the facial matching capabilities that HART is expected to employ.¹⁸ The potential for data breaches of biometric information such as facial image data sets and iris patterns could result in sensitive information being revealed to unauthorized entities. This is especially concerning because, unlike conventional identification methods, biometric technologies measure things that are generally distinct to each person and cannot easily be changed.

Federal agency collection and use of personal information, including facial images, is governed primarily by the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002.¹⁹ The Privacy Act places limitations on agencies' collection, disclosure, and use of personal

¹⁷See, most recently GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 2, 2021) and *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021).

¹⁸[GAO-22-106100](#).

¹⁹5 U.S.C. § 552a; Pub. L. No. 107-347, § 208, 116 Stat. at 2921.

information maintained in systems of records.²⁰ The E-Government Act requires agencies to conduct, where applicable, a PIA that analyzes how personal information is collected, stored, shared, and managed in a federal system.

In addition, OMB Memorandum M-03-22 provided guidance on implementing the privacy provisions of the E-Government Act.²¹ The guidance discusses when agencies should conduct or update a PIA, and what elements are to be included, such as what information is being collected and how it will be used and shared. Further, OMB Circular A-130 outlines some of the general responsibilities for federal agencies managing information resources that involve PII and summarizes the key privacy requirements for managing those resources.²²

The HART Program Breached Its Initial Baseline and Rebaselined

In April 2016, DHS approved the initial acquisition program baseline for HART. The baseline estimated the total life cycle cost of the new system to be about \$4.2 billion.²³ Further, the baseline estimated that initial operational capability would occur in 2018, which would result in the decommissioning of IDENT. The baseline also estimated that full implementation would occur in 2021.

In June 2017, the HART program determined it would not be able to meet its initial acquisition program baseline milestones and declared a schedule breach. According to DHS officials, the breach was due to delays early in the contract award process for increments 1 and 2. In September 2017, 3 months after declaring the schedule breach, DHS awarded a \$95 million contract to develop increments 1 and 2.

DHS rebaselined the HART program's cost and schedule estimates 2 years later (in May 2019) in response to the breach. As part of the rebaseline, the department delayed the deployment date for increment 1 by 2 years (from December 2018 to December 2020) and pushed out the

²⁰A system of record is defined by the Privacy Act of 1974 as a group of records containing personal information under the control of any agency from which information is retrieved by the name of an individual or by an individual identifier. See 5 U.S.C. § 552a(a)(4), (5).

²¹OMB, Memorandum M-03-22.

²²OMB, Circular A-130.

²³This figure represents the program's life cycle cost estimate established by DHS and OBIM in April 2016. It is presented in base-year 2016 dollars at a 50 percent confidence level and does not include the effects of inflation.

program's full deployment date by nearly 3 years (from September 2021 to June 2024).

The rebaselined life cycle cost estimate resulted in a decrease of about \$1.4 billion (from \$4.2 billion to approximately \$2.8 billion).²⁴ Program officials primarily attributed the cost decrease to a decision to provide storage for HART data using a less expensive cloud-based solution, rather than DHS's data centers.²⁵ The officials indicated that another reason for the decrease was the removal of technology and refresh upgrades, which were no longer necessary under the cloud approach.

GAO Previously Reported on HART Program Management and DHS Privacy Challenges

GAO previously reported on HART program management and DHS privacy challenges. Specifically, in June 2021, we assessed the extent to which the HART program was adhering to IT acquisition best practices related to risk, contractor, and requirements management, as well as project monitoring and control.²⁶ We reported that the program had mixed results in implementing the selected IT acquisitions best practices. For example, we reported that a lack of traceability within requirements made it difficult for the program to understand what features had been completed, what work remained, and how to test to ensure features would ultimately meet customers' needs upon integration. We also reported that although the multibillion dollar HART program had suffered continuing delays, the DHS CIO had reported the program as low risk.

We made seven recommendations to improve the success of the program. DHS concurred with all of the recommendations and provided estimated dates for implementing them. As of March 2023, DHS had fully implemented four of our recommendations. However, it has not yet fully implemented the remaining three recommendations related to reviewing contractor deliverables, tracking government labor costs, and monitoring stakeholder involvement.

²⁴These figures represent the program's life cycle cost estimate established by DHS and OBIM in April 2016 and May 2019. They are presented in base-year 2016 dollars at a 50 percent confidence level and do not include the effects of inflation.

²⁵Cloud computing is a means for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

²⁶[GAO-21-386](#).

The HART Program Experienced Schedule Delays and Cost Increases since the 2019 Rebaseline

In addition, in December 2021, we reported on DHS's policies and procedures for protecting PII collected by or shared with its contractors.²⁷ We made seven recommendations to DHS and its components aimed at improving the oversight of contractors handling PII. For example, we recommended that the DHS Privacy Office provide targeted role-based privacy training to contractors responsible for protecting PII. DHS agreed with the recommendations; however, as of May 2023, the department had not implemented these recommendations.

In September 2022, we reported on privacy program implementation at DHS and other federal agencies.²⁸ We recommended that DHS fully define and document the role of privacy officials in reviewing and approving system categorizations, overseeing privacy control assessments, and reviewing authorization packages for information systems that involve PII to ensure compliance. We also recommended that the department document a privacy continuous monitoring strategy to ensure that they are effectively monitoring privacy controls on an ongoing basis. DHS agreed with the recommendations; however, as of May 2023, the department had not implemented these recommendations.

Since the first rebaselining in 2019, the program has experienced additional delays in its schedule and increased estimated costs. Specifically, in January 2020, the program declared a second schedule breach—8 months after the initial rebaseline. Moreover, in May 2020, the program also declared its first cost breach.²⁹

In May 2022, the program rebaselined its schedule and costs for a second time (2.5 years after declaring the schedule breach).³⁰ This rebaseline extended the schedule for delivering initial operational capability and prolonged DHS's dependency on IDENT by at least 2

²⁷GAO, *DHS Privacy: Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps*, [GAO-22-104144](#) (Washington, D.C.: Dec. 16, 2021).

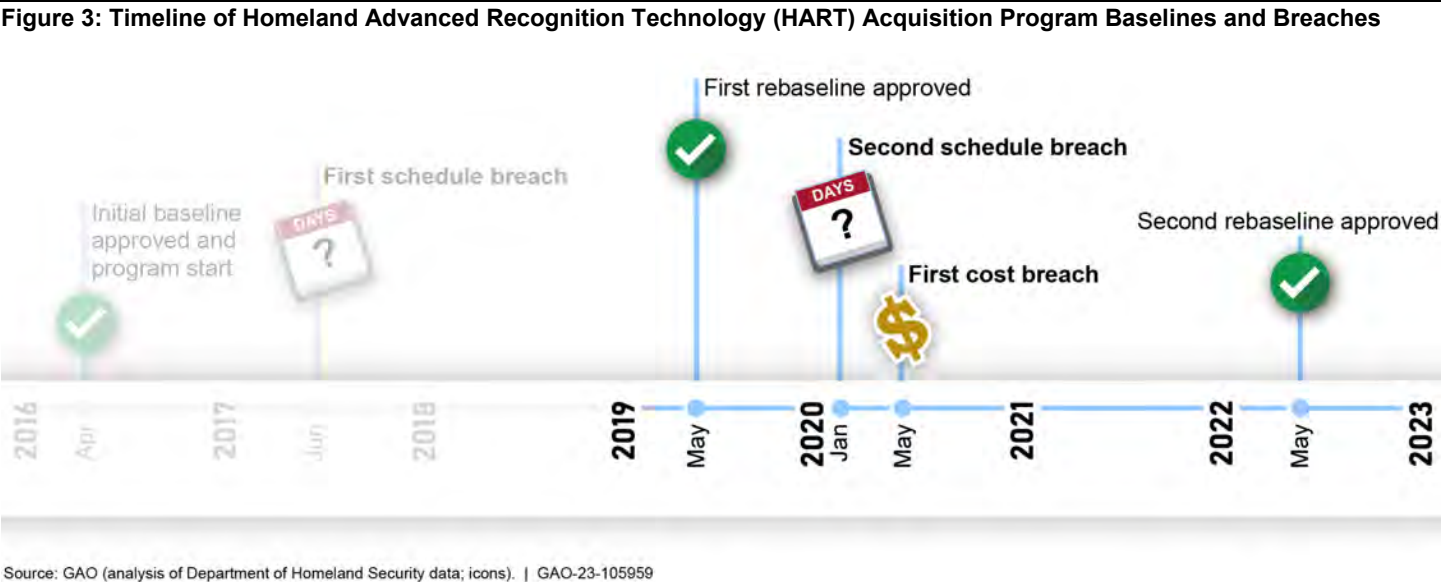
²⁸GAO, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges*, [GAO-22-105065](#) (Washington, D.C.: Sept. 22, 2022).

²⁹According to the breach remediation plan, the 2020 schedule and cost breaches were due to a variety of factors, including technical challenges related to developing key HART subsystems, disagreements between OBIM and the contractor about the interpretation of certain functional requirements, and the technical approach for customer migration and biometric matching.

³⁰According to HART program officials, the DHS Acquisition Review Board met and approved the rebaseline in April 2022. This approval was formally documented in a May 2022 acquisition decision memorandum.

years from the 2019 rebaseline, and at least 4 years from the original 2016 baseline. The HART program also significantly increased its development and operations and maintenance costs in the 2022 rebaselined estimate. Specifically, development costs are estimated to increase by \$92 million, and the operations and maintenance costs are estimated to increase by \$262 million, for a total increase of \$354 million.

Figure 3 shows a timeline of HART’s acquisition program baselines and breaches.



The HART Program Further Delayed the Schedule

The HART program’s 2022 rebaseline extended the plan for delivering initial operational capability by at least 2 years from the 2019 rebaselined schedule. In addition, the 2022 rebaseline did not include an estimated time frame for completing the program. Program officials stated that they intend to develop the remainder of the program’s schedule when the system is closer to initial operational capability. Table 1 shows the

changes that DHS made to the HART program schedule from 2019 to 2022.³¹

Table 1: Changes in the Homeland Advanced Recognition Technology's (HART) Program Schedule from 2019 to 2022

Milestone	Planned completion date ^a (as of May 2019)	Planned completion date ^a (as of May 2022)	Years/months delayed
Program start	April 25, 2016	April 25, 2016	0
Initial operational capability	December 31, 2020	September 30, 2023	2 years, 9 months
Complete increment 1	December 31, 2020	September 30, 2024	3 years, 9 months
Complete full program	June 30, 2024	Not yet planned	Unknown ^b

Source: GAO analysis of HART 2022 and 2019 acquisition program baselines. | GAO-23-105959

^aThis represents the schedule threshold dates defined in the HART acquisition program baseline.

^bThe 2022 rebaseline did not include an estimate for completing the program. As such, the number of years that this milestone has been delayed is unknown.

The schedule delays reflected in the 2022 rebaseline were due to several factors, such as expanding increment 1 to include, among other things, full performance testing, which was originally planned for completion in increment 2. Other factors for the delay were addressing technical challenges related to some of the key subsystems, such as an overly complex database structure, and changing the technical approach to run HART and legacy system operations in parallel for a longer period of time.

In response to the delays, in September 2021, program officials made a major modification to the primary HART development contract. This modification reallocated all resources to work on increment 1 in order to achieve initial operational capability and suspended all work associated with increment 2. OBIM officials decided to shift the remainder of the

³¹The HART program baseline includes schedule parameters from the master schedule. The schedule parameters establish both objective and threshold dates. Objective dates are the earliest feasible dates, based on acceptable risk that the milestones can occur. Threshold dates represent the latest feasible and acceptable dates the milestones can occur. Exceeding the threshold dates represents a schedule breach and requires a program to develop a breach remediation plan to identify corrective actions and a path forward.

originally planned increment 2 functionality into a later increment, referred to as the future capabilities increment.³²

As a result, functionality such as the multimodal fusion has been deferred.³³ Specifically, this functionality was intended to be delivered in increment 2 by September 2021. However, since the schedule for future capabilities was not established in the 2022 rebaseline, multimodal fusion has been delayed for an indefinite amount of time.

More recently, since rebaselining in May 2022, the program has encountered additional challenges affecting the schedule. Specifically, in December 2022 program officials reported experiencing higher than expected software defects, security vulnerabilities, and performance issues. For example, in August 2022, program officials began operating HART in parallel with IDENT to test increment 1 in a live environment, which unveiled issues, such as system response times not being met.³⁴

Moreover, in April 2023, program officials stated that they plan to again revise their approach for achieving initial operational capability. Officials attributed this decision to the ongoing challenges along with a decrease in fiscal year 2023 appropriations made available for HART.³⁵ Program officials stated that they are working with DHS leadership to define the path forward and update the schedule. They further stated that it is unlikely that they will achieve initial operational capability by September

³²In August 2020, the program made a contract modification to address the technical challenges related to the development of increment 1 and decided to combine increments 3 and 4 into a single increment, referred to as future capabilities. In September 2021, the program made another modification to the contract to move increment 2 into the future capabilities increment.

³³Multimodal fusion is intended to allow for the combining of information from multiple types of biometrics (such as fingerprint and iris pattern) to provide more efficient and accurate identification services and reduce the burden on examiners.

³⁴During parallel operations, IDENT remains the official system of record and users continue to receive responses to their queries from IDENT. The queries are passed along to HART where program officials review the responses for consistency with IDENT and against required response times (e.g., retrieving an individual's identity in under 30 seconds).

³⁵Joint explanatory statement of conference, 168 Cong. Rec. S7819, S8555 (daily ed. Dec. 20, 2022) (statement of Chair Leahy), specifically referenced in section 4 of the Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, § 4, 136 Stat. 4459 (2022).

2023. As a result, program officials stated that they needed to rebaseline HART's schedule for a third time.

Consequently, each time that the program has deferred initial operational capability, OBIM has needed to extend its support of the legacy system. However, IDENT has significant shortcomings that require DHS to make additional investments in the system to keep it operational much longer than planned. For example, the department plans to spend \$155 million in fiscal year 2023 to continue IDENT system operations. As we reported in April 2023, the program has had to seek additional funding and reprioritized activities to address funding gaps.³⁶

The HART Program Cost Estimate Increased Development and Operations Costs

HART significantly increased its development and operations and maintenance costs in the 2022 life cycle cost estimate. Specifically, when comparing these costs from the 2019 to 2022 estimates, development costs are estimated to increase by \$92 million, and the operations and maintenance costs are estimated to increase by \$262 million, for a total increase of \$354 million.³⁷

Key reasons for these cost increases include additional testing activities, supplementing the prime development contractor with additional engineers, additional software purchases, and updated maintenance projections. The program also incorporated additional costs to account for the ongoing need to satisfy known and unknown requirements when developing future capabilities.

It is important to note that, although the estimated development and operations and maintenance costs increased in the 2022 estimate, the total life cycle cost estimate of \$2.63 billion is a decrease of \$180 million from the 2019 estimate of \$2.81 billion. This decrease was largely due to removing costs that were not specific to the HART program. For example,

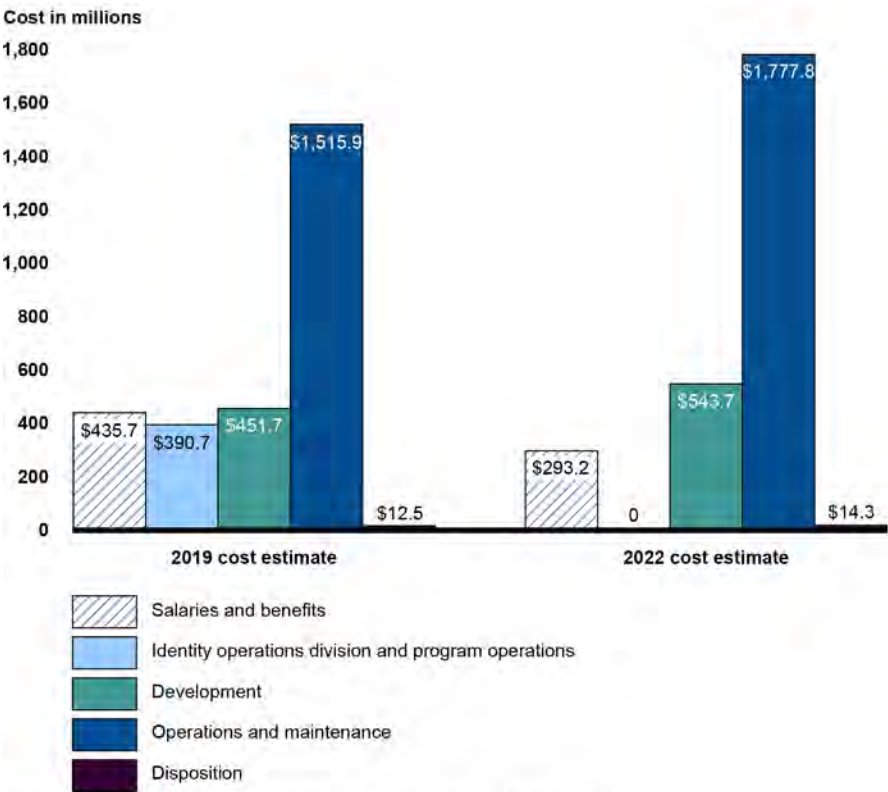
³⁶GAO, *DHS Annual Assessment: Major Acquisition Programs Are Generally Meeting Goals, but Cybersecurity Policy Needs Clarification*, [GAO-23-106701](#) (Washington, D.C.: Apr. 20, 2023). We reported that due to schedule delays and having to operate IDENT longer than planned, the program was not fully funded. Program officials said that in fiscal year 2022, the HART shortfall was addressed through reprogramming and the IDENT shortfall was addressed through a technical assistance package. To mitigate shortfalls in fiscal year 2023, program officials were seeking additional funding and reprioritizing activities as needed to align with existing funding, among other things.

³⁷These figures are presented in base-year 2016 dollars at a 50 percent confidence level. The base-year is used as a constant dollar reference point to track program cost growth. Expressing an estimate in base-year dollars removes the effects of economic inflation and enables comparing separate estimates, such as the 2019 and 2022 HART cost estimates. All of the cost figures in this report section are represented in base-year dollars.

all costs associated with OBIM's Identity Operations Division and Program Operations, totaling \$391 million, were removed from HART's 2022 program estimate. According to program officials, these costs are now captured in a separate OBIM office estimate.

Figure 4 identifies the changes to the HART program's life cycle cost estimate, as of May 2022.

Figure 4: Changes in the Homeland Advanced Recognition Technology (HART) Life Cycle Cost Estimate from May 2019 to May 2022



Source: GAO analysis of Department of Homeland Security data. | GAO-23-105959

Since updating the baseline life cycle cost estimate in May 2022, the program has incurred additional cost increases. Specifically, in August 2022 HART program officials stated that the program expected to reimburse the contractor for additional engineers needed to add capacity to complete development and test work. In addition, the program planned to utilize development teams supplied from another OBIM contract. Although each of these actions will result in added cost to the program

beyond the amount that had been approved in the 2022 life cycle cost estimate, as of February 2023, officials were unable to quantify the additional cost growth. Program officials stated that they will be unable to quantify the cost growth until after agreeing on a new approach for achieving initial operational capability.

HART Cost and Schedule Estimates Were Unreliable

OBIM developed unreliable cost and schedule estimates for the HART program that did not adhere to accepted practices. Specifically, the program's cost estimate did not substantially or fully meet any of the four characteristics of a reliable cost estimate. Moreover, the program's schedule estimate did not substantially or fully meet three of the four characteristics of a reliable schedule estimate.

OBIM's Cost Estimate for the HART Program Was Unreliable

Employing reliable cost estimates is crucial for realistic program planning, budgeting, and management. Cost estimates are necessary for government acquisition programs for many reasons, including to support decisions about funding one program over another, to develop annual budget requests, and to evaluate resource requirements at key decision points. Moreover, having a realistic estimate of projected costs makes for effective resource allocation, and it increases the probability of a program's success. According to the *GAO Cost Estimating and Assessment Guide*, the four characteristics of a high-quality, reliable cost estimate are that it is comprehensive, well-documented, accurate, and credible.

We determined that OBIM's cost estimate for the HART program was unreliable because it did not fully or substantially meet any of the four characteristics of a high-quality, reliable cost estimate. Specifically, the cost estimate partially met all four characteristics of a reliable cost estimate—comprehensive, well-documented, accurate, and credible. Table 2 summarizes our assessment of OBIM'S HART cost estimate compared to these characteristics, as of March 2022. Appendix II provides additional information on our cost assessment.

Table 2: Assessment of the Homeland Advanced Recognition Technology (HART) Program Cost Estimate Compared to Characteristics for a Reliable Cost Estimate Using GAO’s *Cost Estimating and Assessment Guide*, as of March 2022

Cost estimating characteristic	GAO assessment
Comprehensive—The estimate should be comprehensive, including identifying all life cycle costs and basing the cost estimate on a technical baseline description that completely defines the program and reflects the current schedule.	Partially met. The HART life cycle cost estimate covered government and contractor costs from the beginning of the program’s planning activities and was based on a work breakdown structure that included four cost categories. However, the estimate excluded some costs due to a lack of data and uncertain requirements that officials planned to further define as the program approached initial operational capability. For example, while the estimate included costs associated with future capabilities, the program had not defined the actual scope of the future capabilities to inform the associated cost estimates. In addition, the HART Cost Estimating Baseline Document, which served as the technical baseline description for the cost estimate, was outdated and did not reflect programmatic changes since April 2021. For example, the document, which was finalized in April 2021, did not incorporate new work associated with a major contract modification that was awarded in September 2021. Moreover, the assumptions defined in the cost estimate were not used to develop the sensitivity analysis.^a Without fully accounting for life cycle costs, management will have difficulty successfully planning program resource requirements and making informed decisions. In addition, without analyzing the effects of an invalid assumption on the cost and schedule of a program, cost estimators and management will not have a full understanding of the effects of changing ground rules and assumptions.
Well-documented—The estimate should be well-documented, including showing the source data and the estimating methodology used to derive each element’s cost. The estimate should also ensure data in the technical baseline documentation are consistent with data and assumptions in the cost estimate.	Partially met. The Office of Biometric Identity Management (OBIM) documented some of the estimating methodologies used to develop the cost estimate. For example, the HART cost estimate documentation stated that officials used methodologies such as parametric modeling (i.e., relying on statistical relationships between historical costs from other comparable programs) and engineering build-ups (i.e., estimating costs at the lowest level). However, there was insufficient detail provided about data sources used to make a judgment on data reliability. For example, while the supporting documentation provided an overall description of data sources used to generate the HART estimate, it did not include a discussion of data reliability. In addition, some of the technical data and assumptions in the cost estimate were inconsistent with the technical baseline documentation. Without fully documenting data sources used to inform the cost estimate, it will be difficult to update the cost estimate and provide a verifiable trace to a new cost baseline as key assumptions change during the course of the program’s life. In addition, without ensuring technical data and assumptions are consistent with the technical baseline, the credibility of the cost estimate will suffer.

Cost estimating characteristic	GAO assessment
Accurate—The estimate should be accurate, including estimating each work breakdown structure element using the best methodology, and adjusting for inflation. The estimate should be updated regularly to reflect program changes, document the variances between planned and actual costs, and document lessons learned.	Partially met. The cost estimate built up program cost from low-level work breakdown structure elements. In addition, the HART program minimized mistakes by using a software tool to build out the cost estimate. However, large portions of the cost model were based on methodologies that were not fully documented. For example, the estimate relied heavily on subject matter expert opinion, which is a practice that should be limited. The expert opinion method should account for the possibility that bias influenced the result. However, the program did not document taking such steps in its methodology. In addition, the cost estimate did not properly adjust for inflation. For example, the program did not apply inflation to elements representing about 25 percent of the total estimated costs. Moreover, the cost estimate and supporting documentation did not include a discussion of variances between planned and actual costs or lessons learned from elements whose actual costs differed from the estimate. Without fully documenting all elements in the cost model, program management officials and oversight bodies cannot be certain that all cost estimate calculations are accurate and account for all costs. In addition, without properly adjusting for inflation, the HART estimate is at risk of overstating or understating the cost of the program. Lastly, without a documented comparison between the current estimate that is updated with actual costs and the old estimate, cost estimators cannot determine how well they are estimating and how the program is changing over time.
Credible—The estimate should be credible, including developing a sensitivity analysis, a risk and uncertainty analysis, ^b and cross-checks on major cost elements to validate results. The estimate should also be reconciled with an independent cost estimate. ^c	Partially met. HART program officials documented the results of a sensitivity analysis, as well as a risk and uncertainty analysis in the cost estimate. However, the risk and uncertainty analysis was applied inconsistently, resulting in an unreliable risk analysis. For example, for the HART capability support cost element, the program applied risk at both the input level (e.g., labor rate) and to the total cost which likely double counted risk. The program also did not demonstrate performing cross-checks of major cost elements to see if results were similar. In addition, the Cost Analysis Division did not generate an independent cost estimate for comparison with the HART program office's cost estimate because the Department of Homeland Security leadership did not require the division to prepare such an estimate. Instead, the division prepared an independent cost assessment, which identified recommendations for the program office to improve its estimate. However, some of the recommendations were not fully addressed. A poorly executed risk and uncertainty analysis gives HART program officials a false sense of security that all risks have been accounted for, which leads to decisions based on bad information. In addition, without employing cross-checks, the estimate will have less credibility because stakeholders will have no assurance that alternative estimating methodologies produce similar results. Moreover, a program estimate that has not been fully reconciled with an independent cost estimate or assessment has an increased risk of proceeding underfunded because it lacks unbiased assessment of whether the estimate can be achieved.

Legend: Met—OBIM provided complete evidence that satisfies the entire criterion; Substantially met—OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion; Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program cost estimate and supporting documentation. | GAO-23-105959

^aA sensitivity analysis identifies a range of possible costs based on varying major assumptions, parameters, and data inputs. The analysis examines the effect of changing one assumption or cost driver at a time while holding all other variables constant.

^bA risk and uncertainty analysis quantifies the risks and identifies the effects of changing key cost driver assumptions and factors. It uses statistical techniques to predict the probability of successfully executing a program within its budget by capturing the cumulative effect of program risks and uncertainty.

^cAn independent cost assessment is a non-advocate's evaluation of a cost estimate's quality and accuracy, looking at aspects such as the program's technical approach and risk, to ensure that the estimate captures all requirements. It may be used to determine whether the cost estimate reflects the program of record. It is not as formal as an independent cost estimate and does not have to be performed by an organization independent of the acquisition chain of command, although it usually is.

OBIM officials acknowledged that they were not fully or substantially addressing all of the characteristics of a reliable cost estimate. The officials explained that in some cases they were taking the appropriate estimating steps; however, they had not fully documented those steps in order to support the estimate. Officials stated they plan to update documentation supporting the HART life cycle cost estimate. However, they were unable to provide a time frame for completion, as they were in the initial phase of rebaselining the program, which will require the program to revise the cost estimate and associated documentation.

Until OBIM develops an updated cost estimate that fully meets the four characteristics of a reliable cost estimate, the office risks being unable to effectively estimate HART's future funding needs. It also risks using unreliable data to make budgetary decisions to hold the program accountable. As such, it faces an increased likelihood of cost overruns and unmet performance targets for the work associated with the remaining HART capabilities.

OBIM's Schedule Estimate for the HART Program Was Unreliable

The success of a program depends, in part, on having an integrated and reliable master schedule. The schedule provides not only a roadmap for project execution, but also the means by which to gauge progress, identify and resolve potential problems, and promote accountability at all levels of the program. Among other things, scheduling allows program management to decide between possible sequences of activities, determine the flexibility of the schedule according to available resources, predict the consequences of managerial action or inaction on events, and allocate contingency plans to mitigate risks. According to the GAO *Schedule Assessment Guide*, the four characteristics of a high-quality, reliable schedule are that it is comprehensive, well-constructed, credible, and controlled.

We determined that OBIM's schedule for the HART program was unreliable because it substantially met only one of the four characteristics of a reliable schedule estimate—being credible. The schedule partially met the remaining characteristics—being comprehensive, well-constructed, and controlled. Table 3 summarizes our assessment of the HART program's schedule compared to these characteristics, as of June 2022. Appendix III provides additional information on our schedule assessment.

Table 3: Assessment of the Homeland Advanced Recognition Technology (HART) Program Schedule Compared to Characteristics for a Reliable Schedule Using GAO’s *Schedule Assessment Guide*, as of June 2022

Schedule estimating characteristic	GAO assessment
Comprehensive—The estimate should be comprehensive, including capturing all activities for managing the entire program and durations of all activities based on a realistic reflection of how long each activity will take. The schedule should also assign resources for the activities and allocate them to determine whether they will be available when needed.	Partially met. The HART integrated master schedule included government, contractor, and subcontractor activities through increment 1. Officials also established project activity durations. However, the HART schedule did not include activities beyond increment 1, such as all the development and implementation of work associated with future capabilities. In addition, most activities in the schedule (approximately 98 percent) did not include resource assignments. If the schedule does not fully and accurately reflect the program, it will not be an appropriate basis for analyzing or measuring technical work accomplished and may result in unreliable completion dates, time extension requests, and delays. Moreover, without accurate and complete resource assignments, management’s ability to monitor productivity, allocate unused resources, and monitor resource-constrained activities is limited.
Well-constructed—The estimate should be well-constructed, including accommodating a reasonable amount of float, confirming that the critical path is valid and includes all the activities that drive the program’s earliest completion date, and sequencing all activities to ensure that each activity includes predecessor and successor logic.	Partially met. The schedule accommodated a reasonable amount of time an activity can slip before the program’s end date is affected (i.e., float). For example, of the 554 remaining HART tasks set to occur as soon as possible, the majority had a reasonable amount of float of 50 or fewer days. In addition, the critical path for the HART program included activities that drive the program’s earliest completion date. However, the critical path we independently calculated within the schedule included three activities that did not appear on the path submitted by program officials. Moreover, the schedule was not properly sequenced. For example, 10 percent of activities were not able to start before a set date, even if their predecessors were complete (i.e., unjustified date constraints). Without a fully defined critical path based upon sound schedule logic, the program may be relying on an unrealistic or overly aggressive plan that cannot predict the impact changes in the program such as delayed activities, scope changes, and the effect of risk events. In addition, date constraints prevent activities from responding dynamically to changes in the program, including actual progress and availability of resources.
Credible—The estimate should be credible, including horizontal and vertical traceability. ^a	Substantially met. Program officials reported that they performed a 15-point check on the schedule logic to ensure that the schedule could be horizontally and vertically traced. We tested the horizontal and vertical traceability of the schedule and found the schedule generally responded to our manipulation as expected.
Controlled—The estimate should be controlled, including regularly updating the schedule and using actual progress and logic to realistically forecast dates for program activities. The scheduler should also maintain a baseline schedule to measure and report performance and variances from the plan.	Partially met. Program officials stated that the contractor’s scheduler meets with government staff responsible for schedule activities to review and update the schedule based on progress. The HART program also compared performance and identified variances from the current schedule. However, updates to the activities in the schedule were not always logical. For example, we found 50 activities completed out of sequence, including two activities starting before their predecessors. Moreover, although program officials stated that they measure performance against the baseline, they did not report trends in performance over time. If changes are not controlled and fully documented, performance cannot be accurately measured against the original plan. Undocumented or unapproved changes will hamper performance measurement and may result in inaccurate variance reporting, inconsistent stakeholder versions of the same plan, and unreliable schedule data.

Legend: Met—The Office of Biometric Identity Management (OBIM) provided complete evidence that satisfies the entire criterion; Substantially met—OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion;

Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program schedule and supporting documentation. | GAO-23-105959

^aHorizontal traceability demonstrates that the overall schedule is rational, has been planned in a logical sequence, accounts for the interdependence of detailed activities and planning packages, and provides a way to evaluate current status. Vertical traceability demonstrates the consistency of dates, status, and scope requirements between different levels of a schedule—summary, intermediate, and detailed.

OBIM officials acknowledged that the HART integrated master schedule did not fully or substantially address all of the characteristics of a reliable schedule. They explained that DHS and OBIM do not require the program to perform some of the best practices that comprise the four characteristics.

Until OBIM revises the HART program's schedule to follow the four characteristics of a reliable schedule, it runs the risk of additional delays as it works to implement the remainder of the program. Further, until OBIM updates the schedule estimate to account for the total time needed to fully implement the remaining effort, department leadership will be limited in its ability to make informed decisions regarding the program's future. Such uncertainty can cause schedule slippages and increased program costs.

DHS Did Not Fully Implement a Majority of Selected Privacy Requirements for HART

OMB established privacy protection requirements for federal agencies to manage federal information resources that involve PII.³⁸ These requirements include, but are not limited to, following approved records retention schedules, imposing conditions on shared PII, and implementing a risk management framework to manage privacy risks. In addition, OMB established guidance on implementing the privacy provisions of the E-Government Act, including conducting a PIA to analyze how personal information is collected, stored, shared, and managed in a federal system.³⁹

Lastly, OMB also issued guidance that outlines the role and designation of agencies' Senior Agency Official for Privacy (SAOP). In particular, it

³⁸OMB, Circular A-130.

³⁹OMB, Memorandum M-03-22 and Pub. L. No. 107-347, § 208, 116 Stat. at 2921.

describes the position, expertise, and authority the SAOP should have, and it provides details on the official's responsibilities.⁴⁰

DHS did not fully implement a majority of the selected federal privacy requirements to ensure the protection of PII in the HART program. Specifically, of the 12 selected OMB privacy requirements, the department fully implemented five and partially implemented seven. Table 4 describes the selected requirements and provides our assessment of the HART program's implementation of these requirements.

Table 4: Summary of Department of Homeland Security's (DHS) Implementation of Selected Office of Management and Budget Privacy Requirements for the Homeland Advanced Recognition Technology (HART) Program

Privacy requirement	GAO assessment
Review and approve the system security categorization. The Senior Agency Official for Privacy (SAOP), or other delegated officials, shall review and approve the categorization (e.g., low, moderate, or high-impact) of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII). ^a	●
Establish a required security categorization level for shared PII. Agencies that share PII shall require, as appropriate, other agencies and entities with which they share this information, to maintain the PII in a system with a particular categorization level.	●
Incorporate privacy requirements in contracts. Agencies shall ensure contracts incorporate privacy requirements.	●
Encrypt moderate-impact and high-impact information. Agencies shall encrypt all moderate-impact and high-impact information at rest and in transit. ^a	●
Implement a privacy control selection process. Agencies shall employ a process to select and implement from 26 privacy controls that the National Institute of Standards and Technology specified for information systems and programs. ^b Among other things, these privacy controls relate to minimization of PII, responding to a privacy incident, and sharing information with third parties.	●
Conduct a privacy impact assessment (PIA). Agencies shall conduct a PIA to ensure that the handling of PII conforms to applicable privacy requirements. A PIA is intended to identify and evaluate ways to mitigate privacy risks. Among other things, the PIA should describe the intended use of the information being collected, what information will be collected, with whom the information will be shared, and how the information will be secured. In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. The PIA also serves as notice to the public regarding agencies' practices with respect to privacy.	◐

⁴⁰OMB guidance states that at the discretion of the SAOP and consistent with applicable law, other qualified agency personnel may perform privacy functions that are assigned to the SAOP. In all cases, this senior official will retain responsibility and accountability for the agency's privacy program. OMB, Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Washington, D.C.: Sept. 15, 2016). DHS has designated its Chief Privacy Officer as the SAOP.

Develop a privacy plan and control assessment methodologies. Agencies shall develop and maintain a privacy plan that describes the privacy controls selected for an information system and how the controls have been implemented. In addition, the agency should describe the planned methodologies that will be used to assess whether the privacy controls are implemented correctly and operating as intended.	●
Assess privacy controls. The SAOP (or other delegated officials) shall conduct and document the results of privacy control assessments prior to the operation of an information system and periodically thereafter to verify their continued effectiveness and to ensure compliance with applicable privacy requirements and manage privacy risks.	●
Correct privacy-related deficiencies. Agencies shall correct deficiencies that are identified through privacy assessments and use corrective action plans to manage their remediation.	●
Review the system authorization package. The SAOP (or other delegated officials) shall review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks. The packages should be reviewed prior to authorizing officials making risk determination and acceptance decisions. At a minimum, the authorization package should include the system security and privacy plan, security and privacy control assessment, and any relevant corrective action plans.	●
Impose conditions on shared PII through agreements. Agencies shall impose conditions that govern, among other things, use, disclosure, and disposal of shared PII, through written agreements.	●
Follow records retention schedules. Agencies shall ensure that all records with PII are maintained and disposed of in accordance with applicable schedules that document the period of time that agencies should retain records (called records retention schedules).	●

Legend: ● = Fully implemented: evidence demonstrated implementation of all aspects of the requirement; ● = Partially implemented: evidence demonstrated implementation of some, but not all of the requirement; ○ = Not implemented: evidence did not demonstrate implementation of any aspect of the requirement

Source: GAO analysis of HART privacy documents. | GAO-23-105959

^aThe National Institute of Standards and Technology Federal Information Processing Standards Publication 199 dictates that a system's security categorization is expressed as either low, moderate, or high-impact. The categorization is based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals. National Institute of Standards and Technology, *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004).

^bOMB Circular A-130 describes privacy controls as the administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. In April 2013, the National Institute of Standards and Technology developed its fourth revision of the Special Publication on Security and Privacy Controls for Federal Information Systems and Organizations, which includes 26 privacy controls for agencies to implement. Although a fifth revision was issued in September 2020, the fourth revision was used as criteria because DHS had not yet implemented the fifth revision. National Institute of Standards and Technology SP 800-53, Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations* (Gaithersburg, Md.: April 2013, withdrawn Sept. 23, 2021).

The five privacy requirements that the department fully implemented represent important steps toward protecting PII that will be matched, stored, and shared by HART. For example, the Senior Director for Privacy Compliance reviewed and approved the system security categorization of the HART system. In addition, OBIM documented the required security categorization level for entities that HART shares data with in interconnection security agreements. The office also included

privacy requirements in applicable contracts and demonstrated that HART data are encrypted at rest and in transit. Further, the DHS Privacy Office selected and documented the implementation for all 26 privacy controls established by the National Institute of Standards and Technology.

The following summarizes the seven privacy requirements that were partially implemented.

- **Conduct a privacy impact assessment – partially implemented.** DHS Privacy Office officials conducted a PIA of HART and published it in February 2020. Among other things, the PIA described the intended use of the information being collected. For example, the assessment stated that OBIM uses these data to match, store, and share results as permitted to support national security, employment credentialing, law enforcement, immigration, and intelligence. The assessment also analyzed and described how the information will be secured in HART through the use of a robust set of access controls. In addition, Privacy Office officials reviewed the published PIA in December 2021 and determined that no updates were necessary at that time.⁴¹

However, although the assessment analyzed and described most types of information that will be stored in the system, it did not describe the categories of individuals' information whose data will be stored in HART. Specifically, the assessment did not disclose whether the system will be collecting and storing foreign nationals' data, U.S. citizens' data, or both. OBIM officials stated that, because the assessment names particular programs which use U.S. citizen data, readers of the PIA should be able to infer that U.S. citizen data will be stored in HART.⁴²

However, this approach puts the onus on the public to know the purpose of the relevant programs and associated systems to understand if U.S. citizen data will be stored in the system. This is important because the statutory privacy rights and protections specified in the Privacy Act of 1974 apply to U.S. citizens and lawful

⁴¹The DHS Senior Director for Privacy Compliance conducted this review when the department consolidated the HART production and test environments.

⁴²Examples of such programs referenced by the PIA include TSA PreCheck, Domestically Filed Intercountry Adoption Applications and Petitions, and Transportation Worker Identification Credential.

permanent residents,⁴³ whereas they do not always apply to foreign nationals. Officials stated that they will include this information in the next HART PIA. As of May 2023, OBIM officials stated that they were coordinating with the Privacy Office to determine the best time frame for updating the HART PIA, but did not provide an estimated completion date.

In addition, although the HART PIA identified 18 entities that these data will be shared with, the list was incomplete.⁴⁴ This is contrary to DHS's PIA guidance, which requires that the assessments identify the names of the federal agencies and foreign governments with which a system shares information. Specifically, the PIA omitted several partners, such as the Office of Personnel Management, Germany, and Croatia.

DHS officials acknowledged that certain partners may not be reflected in the PIA because they were added after the document was published in 2020. Officials stated that they will incorporate new partners into the PIA when it is next updated. However, as previously mentioned, OBIM did not provide an estimated completion date for incorporating the updates.

As such, until the Privacy Office establishes and implements a timeline for incorporating these important updates in the PIA, the public will not be fully aware of whether their information is stored in HART and with whom their information is shared.

- **Develop a privacy plan and control assessment methodologies – partially implemented.** The HART system security plan includes a privacy plan. This privacy plan describes the 26 privacy controls and 63 associated sub-elements. The plan also discusses how the controls will be implemented. For example, to implement a control related to privacy awareness and training, the HART plan states that employees handling sensitive PII should receive role-based training.

Regarding assessment methodologies, the DHS Privacy Office documented methods for a limited portion of the controls. Specifically, for eight of the 63 privacy control sub-elements, the office documented the steps the office planned to take to determine whether the control

⁴³5 U.S.C. § 552a.

⁴⁴These 18 entities include DHS component users, such as the U.S. Customs and Border Protection and the Transportation Security Administration, as well as agencies such as the Department of Justice and Department of State.

was implemented correctly or operating as intended. For example, to assess implementation of a control related to privacy requirements for contractors and service providers, the office documented that it plans to review and approve sections of the contracts to ensure all privacy language is included.

However, contrary to OMB's guidance, the Privacy Office did not clearly describe planned methodologies for assessing the implementation for each of the remaining 55 privacy control sub-elements. Privacy Office officials stated that they did not believe describing planned assessment methods was necessary.

Without documented assessment methods for each control, there is a lack of transparency regarding what steps the office took (or plans to take) to determine whether a control was (or will be) implemented correctly. Further, without documented methods, the process will not be repeatable for new staff who may be responsible for future assessments of the privacy controls. Until the Privacy Office ensures that detailed methodologies are defined for the HART program, the department risks assessing privacy controls incorrectly or having controls that do not work as intended.

- **Assess privacy controls – partially implemented.** Delegated privacy office officials conducted an initial assessment of the privacy controls for the HART system. Privacy Office officials stated that they assessed the controls through their review and approval of privacy compliance documentation, including the PIA, privacy threshold analysis, and system of records notices. Following the approval of the PIA in February 2020, the office documented the results of its assessment of the controls as implemented. In addition, Privacy Office officials stated that they reassessed the implementation of the privacy controls when the office reviewed and updated the privacy threshold analysis in December 2021.

In addition to taking these actions, DHS also planned to assess the continued effectiveness of the privacy controls by initiating a privacy compliance review within 1 year of completing the PIA (by February 2021). However, as of May 2023, the privacy office had not completed this privacy compliance review and it was 2 years overdue. Privacy Office officials stated that they had initiated the compliance review, but paused it due to difficulty filling a vacancy gap in the Director of Oversight position whose responsibility was to conduct the review. As of May 2023, the position remained vacant, but DHS was actively conducting an applicant screening process.

Nevertheless, until the office prioritizes developing and implementing a timeline for completing the planned privacy compliance review, DHS will not have taken the steps necessary to help ensure that the program's privacy controls are effective.

- **Correct privacy-related deficiencies – partially implemented.** The DHS Privacy Office identified 13 deficiencies and made recommendations to OBIM to remediate them in a February 2020 PIA. OBIM officials reported completed or planned actions for addressing six of the 13 deficiencies. For example, the Privacy Office identified that OBIM did not regularly confirm that the information that HART shares is consistent with the data provider's requirements. In response, OBIM reported that the office plans to conduct periodic reviews to ensure that any new or existing information sharing rules are consistent with the data provider's requirements.

However, as of May 2023, OBIM has not demonstrated that it had addressed or established corrective action plans to address the remaining seven deficiencies. Privacy Office officials stated that they are not actively monitoring the status of these deficiencies due to staff vacancies. Nevertheless, without ensuring that OBIM has fully addressed the remaining seven privacy deficiencies or has corrective action plans in place to do so, OBIM is in jeopardy of leaving some privacy risks unaddressed.

- **Review the system authorization package – partially implemented.** The DHS Privacy Office reviewed some of the documents comprising the HART authorization package, including the December 2021 privacy threshold analysis and the February 2020 PIA. However, the office did not review other parts of the package, such as the security control assessment.

Privacy Office officials stated that they reviewed only those artifacts that are applicable to privacy and that they are not required to review the other artifacts, such as the security control assessment. However, this is contrary to OMB's guidance, which states that the SAOP (or other delegated official) has a responsibility for reviewing the authorization package for information systems to ensure that privacy risks are managed prior to system authorization.⁴⁵ In addition, these other documents within the package that privacy officials did not

⁴⁵OMB Circular A-130 defines the authorization package as including the system security and privacy plan, security and privacy control assessment, and any relevant corrective action plans.

review address security controls that are of particular importance to protecting PII (e.g., remote access, authentication, and encryption).⁴⁶

Finally, in September 2022, we recommended that DHS fully define and document the role of the SAOP or other designated privacy official in reviewing authorization packages.⁴⁷ However, as previously mentioned, as of May 2023, the department had not taken steps to implement this recommendation. Until the appropriate privacy official reviews all documentation associated with the HART authorization package, the system will lack sufficient oversight for all controls related to privacy. Privacy officials may also fail to identify potential privacy risks or deficiencies.

- **Impose conditions on shared PII through agreements – partially implemented.** OBIM and its predecessor established information sharing and access agreements with entities which the IDENT system (and HART once deployed) shares PII.⁴⁸ OBIM officials stated that these agreements contain conditions for shared PII. However, the information sharing and access agreements we reviewed did not consistently address seven key conditions for protecting PII (i.e., use, disclosure, retention and disposal, correction and redress, data sensitivity, authority for sharing, and privacy).

Specifically, OBIM provided two lists that collectively identified 111 agreements. Of the 18 selected agreements we reviewed, only six contained all seven conditions. The remaining 12 agreements did not consistently address each of the conditions. For example, three

⁴⁶DHS established guidance that identifies specific National Institute of Standards and Technology security controls that should be implemented for privacy sensitive systems that permit remote access to PII, such as HART. For example, the guidance requires all privacy sensitive systems to implement security controls related to remote access and authenticator management to ensure that remote access to PII is appropriately protected. The guidance also requires that the SAOP approves cases where these required security controls cannot be implemented. DHS, *4300A Sensitive Systems Handbook, Attachment S, Compliance Framework for Remote Access to and Extracts from Privacy Sensitive Systems, Version 11.0* (Washington, D.C.: Aug. 5, 2014).

⁴⁷GAO, *Privacy: Dedicated Leadership Can Improve Programs and Address Challenges*, [GAO-22-105065](#) (Washington, D.C.: Sept. 22, 2022).

⁴⁸OBIM was formerly known as the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program. US-VISIT was established in 2003 to provide U.S. visa-issuing posts and ports of entry with the biometric technology that enabled the U.S. government to establish and verify identities. In 2013, pursuant to the Consolidated and Further Continuing Appropriations Act, 2013, Pub. L. No. 113-6, 127 Stat. 198, 356 (2013) Congress replaced funding for US-VISIT's biometric identity management functions with funding for the newly created OBIM.

agreements did not address the condition related to the use of PII, and three agreements did not address the condition related to the disposal of PII.

The missing conditions were due, in part, to the age of certain agreements. Specifically, over half of the agreements were established before 2010 when DHS issued guidance on the required contents and conditions that should be included in the information sharing and access agreements. Officials from OBIM and the DHS Office of Strategy, Policy, and Plans recognized that these agreements may not always include all of the required conditions in the guidance.⁴⁹ In February 2023, the policy officials stated that the Office of the Chief Information Officer is working on updating the information sharing and access agreement guidance, and once updated the policy officials will begin work on updating the agreements to be consistent with the new guidance.

As of May 2023, the department expected to complete a draft of the revised information sharing and access agreement guidance by September 2023 and publish a final version by January 2024. If DHS updates each of the information sharing and access agreements that were missing the required conditions, as planned, it will provide the department with greater assurance that HART partners are consistently applying appropriate privacy conditions for shared PII.

In addition to missing conditions for protecting PII in the agreements, OBIM does not maintain a reliable inventory of these agreements. Specifically, while a key characteristic of data reliability includes completeness, OBIM's lists identifying 111 information sharing and access agreements were incomplete. The lists did not clearly identify agreements for each of OBIM's approximately 140 partners. For example, according to the lists, the Office of Personnel Management and the Department of Justice's Bureau of Prisons do not appear to have agreements with OBIM.

OBIM officials stated that the reason that some partners do not appear to be covered by a sharing agreement is because some agreements cover multiple partners. For example, officials stated that the Office of Personnel Management's and the Bureau of Prisons' information sharing with HART is covered by an agreement between

⁴⁹With regard to information sharing and access agreements, DHS Office of Strategy, Policy, and Plans officials have stated that their office supports DHS components with their data sharing requirements and leads the coordination, drafting, and updating of department-level sharing arrangements where multiple components are responsible parties.

DHS, the Departments of State and Justice, and OBIM. However, there is no traceability that shows that this agreement covers the bureau and the office. In addition, OBIM's lists did not specify this arrangement for either of these partners. As such, the lists lack critical information to ensure that OBIM has a complete inventory of agreements that cover all partners.

In February 2023, officials from the Office of the Chief Information Officer stated that they developed an inventory system for sharing agreements, which is available for DHS components to access. In May 2023, DHS officials stated that OBIM was reviewing the technical capabilities of the system to determine if it would meet the office's needs for maintaining HART's agreements. However, they did not provide a timeline for determining next steps. Until OBIM establishes and implements a timeline for maintaining a reliable inventory of information sharing and access agreements for HART, the office will be limited in its ability to ensure that appropriate conditions are imposed on partners to protect PII.

- **Follow records retention schedules – partially implemented.** OBIM issued guidance that all partners that provide data are responsible for the retention and disposal of the records that they provide to HART in accordance with their retention schedules. Specifically, these data providers must use HART services to delete records in the system.⁵⁰

HART records containing PII are subject to varying retention periods depending on the data providers' retention schedules. For example, U.S. Citizenship and Immigration Services data entered into HART regarding adoption application processing should be disposed of after 50 years.

However, OBIM does not take steps to verify that data providers appropriately dispose of records containing PII in HART. While OBIM officials stated that the office has the ability to create reports to assist partners in determining adherence to the records retention schedule, it does not require its partners to request such reports from OBIM on a recurring basis to ensure that PII is appropriately disposed of from the system. OBIM officials also stated partners have not requested such reports for this use.

⁵⁰Using the HART service known as "delete encounter," data providers can submit a request for the system to delete their records in accordance with the applicable retention schedule. The data providers may also send OBIM a list of records for the office to delete.

Given the large number of partners that provide data to HART (approximately 140), and varying retention periods for the vast quantity of PII stored in the system, there is a risk that the partners will not appropriately dispose of PII. As such, until OBIM establishes and maintains a process for ensuring that these partners have used HART services to appropriately delete PII from the system, the office risks retaining PII in the system longer than the scheduled retention period, which could potentially compromise individuals' privacy.

Conclusions

DHS's reliance on the 29-year-old biometric identity management system to support national security, law enforcement, and immigration decisions, emphasizes the critical need for OBIM to avoid further delays, cost overruns, and performance issues. However, the program's repeated cost and schedule baseline breaches since 2017 have prolonged DHS's and its partners' dependency on IDENT for at least 4 years beyond the original plan. In addition, HART's development and operations costs have grown by at least \$354 million.

OBIM's schedule and cost shortcomings for HART reflect its lack of alignment with important cost and schedule estimation best practices. Specifically, OBIM's lack of reliable cost and schedule estimates increases the risk that management will not have the information necessary for effective decision-making. Further, until the significant weaknesses in the cost and schedule estimates are addressed the office risks further cost overruns and schedule delays. These risks are especially concerning as the program is in its seventh year and has yet to achieve initial operational capability.

While HART promises to deliver benefits, deploying the modernized system will increase privacy risks as OBIM plans to store additional kinds of biometrics (e.g., DNA) and anticipates continued growth in users and identities stored in HART. DHS has taken important steps to fully implement five of the 12 selected privacy requirements; however, the gaps in the remaining seven requirements reduce HART's ability to appropriately protect individuals' PII. As such, until OBIM addresses weaknesses in HART privacy protections, such as the missing information in the PIA and the lack of assurances in partners' adherence to records retention schedules, the office may develop a system that puts individuals' PII at increased risk for compromise.

Recommendations for Executive Action

We are making nine recommendations to DHS:

The Secretary of DHS should direct the OBIM Director to update the cost estimate for the HART program to account for all costs and incorporate

the best practices called for in the *GAO Cost Estimating and Assessment Guide*. (Recommendation 1)

The Secretary of DHS should direct the OBIM Director to revise the schedule estimate for the HART program that incorporates the best practices called for in the *GAO Schedule Assessment Guide*. (Recommendation 2)

The Secretary of DHS should direct the OBIM Director to coordinate with the Privacy Office to establish and implement a timeline for updating the HART PIA to fully describe the categories of individuals whose data will be stored in HART and the partners with whom the system shares information. (Recommendation 3)

The Secretary of DHS should direct the Privacy Office to describe planned methodologies for determining that all privacy controls are implemented correctly and operating as intended for future control assessments of the HART program. (Recommendation 4)

The Secretary of DHS should direct the Privacy Office to develop a timeline for completing the planned HART privacy compliance review. (Recommendation 5)

The Secretary of DHS should direct the OBIM Director to coordinate with the Privacy Office to establish and implement plans for correcting seven remaining privacy deficiencies identified in the HART PIA. (Recommendation 6)

The Secretary of DHS should direct the Privacy Office to ensure the complete HART authorization package is reviewed by the office prior to future system authorizations. (Recommendation 7)

The Secretary of DHS should direct the OBIM Director to establish and implement a timeline for maintaining a reliable inventory of information sharing and access agreements with partners that share data with HART. (Recommendation 8)

The Secretary of DHS should direct the OBIM Director to establish and maintain a process for ensuring that partners that provide data to HART have used the system's services to help to appropriately dispose of PII from the system, in accordance with applicable records retention schedules. (Recommendation 9)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. The department provided written comments, which are reprinted in appendix IV. In its comments, DHS concurred with all nine of our recommendations and provided estimated completion dates for implementing four of them.

DHS also provided additional considerations related to recommendations 1, 2, and 4. Specifically, regarding recommendations 1 and 2, the department stated that it has made some improvements related to cost and schedule estimation that we did not reflect in the report. For example, DHS stated that in January 2023 OBIM initiated improvements to its application of risk and updated supporting documentation to include actual source data when actuals are updated in the estimate. In addition, among other things, the department stated that in December 2022, it updated the HART schedule to clearly distinguish tasks assigned to federal employees and contractors.

We did not reassess the cost and schedule estimates based on these reported improvements because the updates had not been approved by DHS leadership. Instead, we reviewed the June 2022 program schedule because it served as the basis for the HART program's most recent acquisition program baseline, which was reviewed and approved by DHS leadership. We will reassess the reliability of the program's cost and schedule estimates, including the actions taken to address our recommendations, once the program establishes its new baseline and the estimates receive approval from DHS leadership.

In addition, while DHS concurred with recommendation 1, the department indicated that it disagrees with our ratings for three of the 18 best practices within of our cost assessment. Specifically, DHS stated that these three practices should have been rated as "substantially met" instead of "partially met." However, we maintain that the assessments are accurate for each of the three following areas.

- The department stated the best practice of "documented all cost-influencing ground rules and assumptions" within the cost estimating characteristic of "comprehensive" has been substantially met. Specifically, DHS stated that the cost estimate inputs had risk assumptions aligned to the ground rules and that the estimate was used to run a sensitivity analysis.

However, we found that while OBIM did have risk assumptions for cost elements in the estimate, instead of using these assumptions to develop a sensitivity analysis as described in the GAO Cost Guide, it

used a predetermined sensitivity range of possible costs without considering the unique risk assumptions of each cost element. As a result, management lacked insights into the linkage between the technical baseline parameters, assumptions, and cost model inputs that informed the sensitivity analysis. This inhibits management's ability to make well-founded decisions.

- The department also stated the best practice of "adjusted for inflation" within the cost estimating characteristic of "accurate" has been substantially met. Specifically, the department stated that the HART program did not use standard inflation on some cost elements due to the existence of negotiated costs or where inflation was already incorporated into the cost for that item. DHS stated that this was done to avoid applying an inflation factor twice.

However, as previously discussed with OBIM officials, cost estimates should be prepared in base-year dollars to eliminate the distortion that would otherwise be caused by overall price-level changes. This requires the transformation of historical or actual cost data into base-year dollars. If data are not properly normalized, the data set may be inconsistent with other data used in the estimate and the effects of external inputs may not be removed.

- DHS stated the best practice of "updated regularly to reflect program changes and actual costs" within the cost estimating characteristic of "accurate" has been substantially met. DHS stated that it entered actual costs into the estimate as they become available. In prior discussions, OBIM stated that it intended to update its documentation to identify sunk costs when updating the estimate. We agree that this would be an acceptable approach when DHS prepares the revised cost estimate to support a new program baseline.

In additional comments on our cost estimate analysis, the department stated that the DHS Cost Analysis Division developed an Independent Cost Assessment and it does not intend to conduct an Independent Cost Estimate of the HART program. As we discussed with DHS officials, conducting an Independent Cost Assessment would have been considered an acceptable alternative to an Independent Cost Estimate if we had found that the issues in the assessment were fully addressed. However, OBIM did not demonstrate that it had fully addressed the issues related to risks and subjectivity, or implemented the associated recommendations.

With regard to recommendation 2, while DHS concurred with the recommendation, it disagreed with our rating for one of the 10 best practices within our schedule assessment. Specifically, the

department stated the best practice “confirmed that the critical path is valid and included all activities that drive the program’s earliest completion date” within the schedule estimating characteristic of “well-constructed,” has been substantially met. The department stated that OBIM’s schedule update process accounts for differences in calculating the critical path and attested that there was not an issue with the critical path provided to us.

However, as discussed with DHS, our analysis showed that there were additional problems with the critical path. Specifically, there were lags and constraints on tasks on the critical path and it was unclear if the critical path contained level of effort tasks. Unless the schedule is fully horizontally traceable, the effects of delayed activities on successor activities cannot be determined. Further, level of effort activities should not drive the schedule.

In additional comments on recommendation 2, DHS stated that the HART program is meeting the intent of the assigning resources scheduling best practice through its Agile processes. The department added that this process provides the program manager greater insight into resource allocations and issues as the lower level requirements are tracked. For these reasons, DHS did not add resource-loading into the HART schedule.

However, we found that while the program had listed a government point of contact for some tasks in the schedule, this was not the person or people actually responsible for conducting the work for each of the tasks. In addition, the program did not demonstrate assigning and monitoring resources through its Agile processes. Resources must be considered in the creation of a schedule because their availability directly affects an activity’s duration. Further, if the schedule does not have resource assignments, management’s ability to monitor productivity, allocate idle resources, monitor resource-constrained activities, and level resources across activities is severely limited.

Lastly, with regard to recommendation 4, while DHS stated that it concurs with the recommendation, it requested that we consider the recommendation resolved. Specifically, the department stated that the Privacy Office described planned privacy control assessment methodologies. DHS noted that the implementation statements for each privacy control in the HART System Privacy Plan described how a control was implemented or assessed.

However, we disagree that the office took steps to clearly document its planned methodologies for determining if they were implemented

correctly or operating as intended. Specifically, 87 percent (i.e., 55 of the 63) of the privacy control sub-elements did not have documented planned methodologies prior to being assessed. Documenting methodologies for assessing privacy controls is essential to ensure that DHS can determine if these controls were properly implemented for HART.

In addition to the aforementioned comments, we received technical comments from DHS, the Transportation Security Administration, U.S. Customs and Border Protection, and OBIM officials, which we incorporated, as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-5017 or cruzcaim@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.



Marisol Cruz Cain
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our objectives were to (1) determine how the Homeland Advanced Recognition Technology (HART) program has changed since the 2019 baseline, (2) assess the extent to which the HART program's cost and schedule estimates followed best practices, and (3) assess the extent to which the Department of Homeland Security (DHS) implemented selected privacy requirements for the HART program.

To address the first objective, we reviewed HART planning documentation, such as schedule and cost estimates and the associated acquisition program baselines, to describe the schedule and cost changes that HART experienced since 2019. Specifically, we compared the schedule estimates supporting the 2019 and 2022 acquisition program baselines. To identify changes in cost, we compared the HART life cycle cost estimates supporting the May 2019 and May 2022 acquisition program baselines. In addition, we reviewed relevant documentation, such as monthly oversight meeting minutes, to describe changes to the program since the May 2022 baseline. Lastly, we interviewed HART program office officials regarding changes in the program schedule and cost.

To address the second objective, we reviewed the HART program's cost and schedule estimates dated March 2022 and June 2022, respectively, and related documents describing HART's cost and schedule estimation practices.¹

- To assess HART's cost estimate, we evaluated documentation supporting the estimate, such as the cost estimating baseline document, which defined the program's technical approach, and the program's risk register, which informed the risk and uncertainty analysis. We assessed this documentation against best practices identified in *GAO's Cost Estimating and Assessment Guide*.² These best practices map to the four characteristics of a high-quality, reliable cost estimate—comprehensive, well-documented, accurate, and credible. To understand HART's methodology, data, and approach, we interviewed relevant program officials, including the HART

¹In response to our request for the baseline integrated master schedule, the Office of Biometric Identity Management (OBIM) provided a schedule dated June 2022, a month after establishing the May 2022 acquisition program baseline.

²GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar. 12, 2020).

program manager and government cost lead for the Office of Biometric Identity Management (OBIM).

- To assess HART's schedule, we evaluated supporting documentation, such as the integrated master schedule, schedule risk analysis, and a schedule management plan. We assessed the schedule documentation against best practices identified in *GAO's Schedule Assessment Guide*.³ These best practices map to the four characteristics of a high-quality, reliable schedule estimate—comprehensive, well-constructed, credible, and controlled. We also interviewed program officials responsible for developing and managing the program schedule, including OBIM's schedule management lead, to understand their practices for creating and maintaining the schedule.

For our assessments of the HART program's cost and schedule estimates, we assessed each best practice as follows:

- Met—OBIM provided complete evidence that satisfies the entire criterion.
- Substantially met—OBIM provided evidence that satisfies a large portion of the criterion.
- Partially met—OBIM provided evidence that satisfies about one-half of the criterion.
- Minimally met—OBIM provided evidence that satisfies a small portion of the criterion.
- Not met—OBIM provided no evidence that satisfies any of the criterion.

Then, to determine the overall assessment for each of the four characteristics, we assigned each best practice assessment a score based on a 5-point scale: not met = 1, minimally met = 2, partially met = 3, substantially met = 4, and met = 5. We calculated the average of the individual best practice assessment scores to determine the overall assessment rating for each of the four characteristics as follows: not met = 1.0 to 1.4, minimally met = 1.5 to 2.4, partially met = 2.5 to 3.4, substantially met = 3.5 to 4.4, and met = 4.5 to 5.0.

³GAO, *GAO Schedule Assessment Guide: Best Practices for Project Schedules*, [GAO-16-89G](#) (Washington, D.C.: Dec. 22, 2015).

Finally, we provided OBIM and HART program officials with draft versions of our detailed analyses of the program's cost and schedule so that they could verify the information on which we based our findings.

We determined that the cost and schedule data provided by OBIM was not complete and reliable. We discuss the limitations of these data in the report and we have made appropriate attribution indicating the sources of these data.

To address the third objective, we identified privacy requirements based on a review and analysis of federal laws, policy, and guidance. Specifically, we reviewed the Privacy Act of 1974 and the privacy provisions of the E-Government Act of 2002,⁴ as well as the Office of Management and Budget's (OMB) Circular A-130 *Managing Information as a Strategic Resource*, which included requirements for federal agencies to implement specific requirements for managing personally identifiable information (PII). We also reviewed Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, related to conducting a privacy impact assessment (PIA).⁵

Next, we selected requirements by first analyzing nine areas of requirements included in OMB A-130 appendix II.⁶ The nine areas are comprised of 68 requirements. From these nine areas, we selected four areas that, based on our professional judgement, we determined contained requirements that could be applied to individual information systems such as HART (as opposed to agency-wide privacy activities).

⁴Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a) and E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921 (2002).

⁵OMB, Circular A-130, *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016) and Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Washington, D.C.: Sept. 26, 2003).

⁶OMB A-130 Appendix II includes 11 areas: (1) Fair Information Practice Principles, (2) Senior Agency Official for Privacy, (3) Agency Privacy Program, (4) Considerations for Managing PII, (5) Budget and Acquisition, (6) Contractors and Third Parties, (7) Privacy Impact Assessments, (8) Workforce Management, (9) Training and Accountability, (10) Incident Response, and (11) Risk Management Framework. We excluded two of these areas from consideration when selecting requirements. Specifically, we did not consider the Fair Information Practice Principles area because it is not an OMB requirement and we did not consider the Senior Agency Official for Privacy area because it was duplicative of requirements in the Agency Privacy Program area.

Those areas were: (1) considerations for managing PII, (2) contractors and third parties, (3) conducting a PIA, and (4) risk management framework.⁷ Collectively, these four areas included a total of 27 requirements.

From these 27 requirements, we excluded 15 that, based on our professional judgement, were not applicable to individual information systems. We also excluded requirements that overlapped with other selected requirements or with our prior reporting on contractor oversight at DHS.⁸ This resulted in 12 remaining requirements that we assessed HART against:

1. Review and approve the system security categorization.
2. Establish a required security categorization level for shared PII.
3. Incorporate privacy requirements in contracts.
4. Encrypt moderate-impact and high-impact information.
5. Implement a privacy control selection process.
6. Conduct a PIA.
7. Develop a privacy plan and control assessment methodologies.
8. Assess privacy controls.
9. Correct privacy-related deficiencies.
10. Review the system authorization package.
11. Impose conditions on shared PII through agreements.
12. Follow records retention schedules.

To determine the extent to which the HART program had implemented the selected requirements, we obtained and assessed HART program documents and privacy-related artifacts against each of the selected privacy requirements. In particular, we analyzed, among other things,

⁷National Institute of Standards and Technology developed the risk management framework to address broad information-security and risk-management activities to be followed in developing information systems, including categorizing the system's impact level; selecting, implementing, and assessing security controls; authorizing the system to operate; and monitoring the efficacy of controls on an ongoing basis. OMB's Circular A-130 requires agencies to use this framework to manage privacy risks.

⁸GAO, *DHS Privacy: Selected Component Agencies Generally Provided Oversight of Contractors, but Further Actions Are Needed to Address Gaps*, [GAO-22-104144](#) (Washington, D.C.: Dec. 16, 2021).

OBIM biometric guidelines, biometric records retention schedules, HART support contracts, information sharing and access agreements inventory and documentation, the PIA, and the system security and privacy plan.

In addition, we interviewed knowledgeable DHS officials regarding their efforts to implement privacy requirements for the system. Specifically, we interviewed officials from the HART program; OBIM; the DHS Privacy Office; the DHS Office of Strategy, Policy, and Plans; and the DHS Office of the Chief Information Officer.

We assessed the HART program's implementation of the 12 selected requirements as:

- fully implemented, if available evidence demonstrated implementation of all aspects of the requirement;
- partially implemented, if available evidence demonstrated implementation of some, but not all of the requirement, or;
- not implemented; if available evidence did not demonstrate implementation of any aspect of the requirement.

To assess the reliability of data contained in the system security and privacy plan, we (1) reviewed related documentation such as the user guide for the system in which DHS maintains system security and privacy plans; (2) examined these data for obvious outliers, incomplete entries, or unusual entries; and (3) interviewed knowledgeable program officials about the reliability of these data provided. We determined that these data were sufficiently reliable for the purposes of our reporting objective.

Moreover, to assess the reliability of the inventory of information sharing and access agreements provided by OBIM officials, we (1) reviewed related documentation and assessed the inventory for consistency with existing agency records; (2) examined these data for obvious outliers, incomplete entries, or unusual entries; and (3) interviewed knowledgeable program officials about the reliability of these data provided. We determined that the inventory was not reliable because it was incomplete. We discuss the related limitations in the report.

To determine whether the program had incorporated conditions for shared PII into the sharing agreements with partners, we first asked HART program officials to provide us with a list of information sharing and access agreements that pertain to data stored and shared by the system. The program provided us with two lists that collectively included 111 agreements. We selected the 37 agreements with domestic entities (e.g.,

the Department of State and Department of Defense) and excluded 74 agreements with international entities (e.g., United Kingdom, Canada, and Australia). We further narrowed the list of domestic agreements by excluding 11 agreements that duplicated across both lists, three agreements that were addendums to other full agreements, one agreement that was superseded by another agreement, one agreement that was internal to DHS, and three agreements that were listed but not provided. As a result, we selected a total of 18 agreements to review.

We also interviewed knowledgeable officials from DHS regarding their processes for developing and inventorying information sharing and access agreements. Specifically, we interviewed officials from OBIM; the DHS Office of Strategy, Policy, and Plans; and the DHS Office of the Chief Information Officer.

Lastly, we assessed the relevance of standards for internal controls for the audit. We determined that the control environment, risk assessment, control activities, information and communication, and monitoring components of internal controls were significant to our second and third objectives. Of specific relevance were internal control principles that emphasize that management should, among other things, use quality information to achieve the entity's objectives, and identify, analyze, and respond to significant changes that could impact the internal control system.

We conducted this performance audit from April 2022 to July 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Results of GAO's Assessment of the HART Program Cost Estimate Compared with Best Practices

According to the *GAO Cost Estimating and Assessment Guide*,¹ the four characteristics of a high-quality, reliable cost estimate are comprehensive, well-documented, accurate, and credible. The following table provides our assessment of the HART program's cost estimate compared to these characteristics and the associated best practices, as of March 2022.

Table 5: Assessment of the Homeland Advanced Recognition Technology Program's Cost Estimate Compared to Best Practices, as of March 2022

Cost estimating characteristic	Overall assessment	Best practice	Individual assessment
Comprehensive	Partially met	Included all life cycle costs	Partially met
		Based on a technical baseline description that completely defines the program, reflects the current schedule, and is technically reasonable	Partially met
		Based on a work breakdown structure that divides work into smaller elements at an appropriate level of detail	Substantially met
		Documented all cost-influencing ground rules and assumptions.	Partially met
Well-documented	Partially met	Documented the source, reliability of data, and the estimating methodology used to derive each element's cost	Partially met
		Easily replicated and understandable	Partially met
		Provided consistency between data, assumptions, and technical baseline description	Partially met
		Reviewed and accepted by management	Substantially met
Accurate	Partially met	Estimated for each work breakdown structure element using the best methodology from data collected	Partially met
		Adjusted for inflation	Partially met
		Contained few, if any, minor mistakes	Substantially met
		Updated regularly to reflect program changes and actual costs	Partially met
		Documented variances between planned and actual costs and lessons learned	Minimally met
		Based on historical data	Partially met
Credible	Partially met	Included a sensitivity analysis that identified a range of possible costs based on varying inputs	Partially met
		Included a risk and uncertainty analysis that identified the effects of changing key cost drivers	Partially met
		Employed cross-checks on major cost elements to validate results	Minimally met
		Compared to an independent cost estimate conducted by an outside group to determine whether other estimates produce similar results	Partially met

Legend: Met— The Office of Biometric Identity Management (OBIM) provided complete evidence that satisfies the entire criterion; Substantially met— OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion;

¹GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs*, [GAO-20-195G](#) (Washington, D.C.: Mar. 12, 2020).

**Appendix II: Results of GAO's Assessment of
the HART Program Cost Estimate Compared
with Best Practices**

Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program cost estimate and supporting documentation. | GAO-23-105959

Appendix III: Results of GAO’s Assessment of the HART Program Schedule Compared with Best Practices

According to the *GAO Schedule Assessment Guide*,¹ the four characteristics of a high-quality, reliable schedule are that it is comprehensive, well-constructed, credible, and controlled. The following provides our assessment of the HART program’s schedule estimate compared to these characteristics and the associated best practices, as of June 2022.

Table 6: Assessment of the Homeland Advanced Recognition Technology (HART) Program’s Schedule Estimate Compared to Best Practices, as of June 2022

Schedule estimating characteristic	Overall assessment	Best practice	GAO assessment
Comprehensive	Partially met	Captured all activities for managing the entire program	Partially met
		Assigned resources (e.g., labor and materials) needed to complete the activities to determine whether they will be available when needed	Minimally met
		Established the duration of all activities based on a realistic reflection of how long each activity will take	Substantially met
Well-constructed	Partially met	Sequenced all activities to ensure that they include predecessor and successor logic	Partially met
		Confirmed that the critical path is valid and included all activities that drive the program’s earliest completion date	Partially met
		Accommodated a reasonable amount of total float (time an activity can slip before the program’s end date is affected)	Substantially met
Credible	Substantially met	Verified that the schedule can be traced horizontally and vertically ^a	Substantially met
		Prioritized risks and identified necessary schedule contingency based on a robust schedule risk analysis	Partially met
Controlled	Partially met	Updated regularly using actual progress and logic to realistically forecast dates for program activities	Partially met
		Maintained a baseline schedule to measure, monitor and report actual performance and variances from the plan	Partially met

Legend: Met— The Office of Biometric Identity Management (OBIM) provided complete evidence that satisfies the entire criterion; Substantially met— OBIM provided evidence that satisfies a large portion of the criterion; Partially met—OBIM provided evidence that satisfies about one-half of the criterion; Minimally met—OBIM provided evidence that satisfies a small portion of the criterion; Not met—OBIM provided no evidence that satisfies any of the criterion.

Source: GAO analysis of HART program schedule and supporting documentation. | GAO-23-105959

^aHorizontal traceability demonstrates that the overall schedule is rational, has been planned in a logical sequence, accounts for the interdependence of detailed activities and planning packages, and provides a way to evaluate current status. Vertical traceability demonstrates the consistency of dates, status, and scope requirements between different levels of a schedule—summary, intermediate, and detailed.

¹GAO, *Schedule Assessment Guide: Best Practices for Project Schedules*, [GAO-16-89G](#) (Washington, D.C.: Dec. 22, 2015).

Appendix IV: Comments from the Department of Homeland Security



August 4, 2023

Marisol Cruz Cain
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-105959, "BIOMETRIC IDENTITY SYSTEM: DHS Needs to Address Significant Shortcomings in Program Management and Privacy"

Dear Ms. Cruz Cain:

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

DHS leadership is pleased to note GAO's recognition of the Department fully implementing five Office of Management and Budget privacy requirements. Implementing these requirements represents important steps towards protecting the personally identifiable information (PII) that will be matched, stored, and shared by Homeland Advanced Recognition Technology (HART).

As the Department's enterprise service provider of biometric identity services, the Management Directorate's (MGMT) Office of Biometric Identity Management (OBIM) considers the privacy of individuals' PII, and the security of the information in its data stores, to be the foundational elements of all developmental and operational activities. DHS's commitment to privacy and security is reflected in the legacy Automated Biometric Identification System (IDENT), and has been methodically integrated into HART as DHS develops and delivers this modernized system. Furthermore, Privacy Impact Assessments^{1,2} are in place and approved by the Department for the IDENT and

¹ DHS/OBIM/PIA-004, "Privacy Impact Assessment for the Homeland Advanced Recognition Technology System (HART) Increment 1 PIA," dated February 24, 2020: <https://www.dhs.gov/publication/dhsobimpia-004-homeland-advanced-recognition-technology-system-hart-increment-1>

² DHS/OBIM/PIA-001 (DHS/NPPD/PIA-002), "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," dated December 7, 2012: <https://www.dhs.gov/publication/dhsnppd-pia-002-automated-biometric-identification-system>

HART systems, and these systems are also subject to review of system security controls such as privacy controls, to achieve and maintain an approved authority to operate. These best practices safeguard the data OBIM uses for critical mission needs.

OBIM has already taken many steps to improve its program management of HART. As part of a contract modification awarded October 31, 2022, for example, OBIM government staff assumed the role of Lead Integrator of HART development, and subsequently reviewed and updated development and testing processes, took control and re-prioritized work, and modified the developer's scope to transition the work to other OBIM contractors under OBIM Government oversight to improve efficiencies. Since April 2023, OBIM also made significant changes regarding its executive level governance, to include: (1) initiating the restructuring of the OBIM Executive Steering Committee to provide more effective governance; (2) assigning an Executive level Program Manager; and (3) appointing the DHS Chief Information Officer as the HART Lead Technical Authority to help drive technical decisions throughout the Systems Engineering Lifecycle process.

The program continues to make improvements to its processes and documentation, such as the HART Life Cycle Cost Estimate (LCCE) and Integrated Master Schedule (IMS), to support decision-making. Further, DHS has made progress on addressing recommendations made by GAO in a previous report focused on HART.³ Of the seven recommendations issued in the previous report, GAO considers four closed as implemented,⁴ and the Department continues to work with GAO on implementing and closing the remaining open recommendations.

In the time since GAO conducted their Cost and Schedule Analysis for this engagement, improvements have also been made to the HART LCCE and HART IMS that are not reflected in the GAO's draft report. For example, for the HART LCCE, OBIM initiated improvements to its application of risk and improved documentation (i.e., updating actual source name and date in the LCCE when actuals are updated in the estimate) in January 2023. For the HART IMS, tasks were aligned to the OBIM Schedule Work Breakdown Structure in November 2022, and the HART IMS was updated to more clearly define whether tasks are assigned to federal employees or contractors in December 2022.

Further, in the draft report's assessment of OBIM's use of cost and schedule estimation best practices, GAO defines: (1) "partially met" as OBIM providing evidence that satisfies about one-half of the best practice criterion; and (2) "substantially met" as OBIM providing evidence that satisfies a large portion of the best practice criterion. DHS disagrees with GAO's assessment on four of the best practices, and describes below rationale to warrant a "substantially met" assessment for each.

³ GAO-21-386, "HOMELAND SECURITY: DHS Needs to Fully Implement Key Practices in Acquiring Biometric Identity Management System," dated June 8, 2021; <https://www.gao.gov/assets/gao-21-386.pdf>

⁴ <https://www.gao.gov/products/gao-21-386>

1. The cost estimation best practice of “Comprehensive” “Documented all cost-influencing ground rules and assumptions” has been substantially met, as OBIM reviewed the GAO Cost Estimating Guide with regards to the sensitivity analysis, and the methodology used meets the intent of the guidance. Specifically, the estimate variable inputs have risk assumptions aligned to the overarching ground rules and assumptions in the LCCE. These risk assumptions are used to calculate the point estimate for those variable inputs. This point estimate is then used to run the sensitivity analysis. OBIM discussed the Department’s methodology for this best practice with GAO during a call in May 2023.
2. The cost estimation best practice of “Accurate” “Adjusted for inflation” has been substantially met. The HART program does not use standard inflation on work breakdown structure items where no inflation is required, due to the existence of negotiated costs or where inflation is already incorporated into the number for that work breakdown structure item. This is done to avoid applying an inflation factor twice. OBIM discussed the Department’s methodology for this best practice with GAO during a call in May 2023.
3. The cost estimation best practice of “Accurate” “Updated regularly to reflect program changes and actual costs” has been substantially met. Actual costs are entered directly into the cost estimate line items, thereby superseding the estimated data. The estimated data from contracts is kept in the model for historical purposes. OBIM discussed the Department’s methodology for this best practice with GAO during a call in May 2023.
4. The schedule estimation best practice of “Well-constructed” “Confirmed that the critical path is valid and included all activities that drive the program’s earliest completion date” has been substantially met. As part of the formal status/review cycle of the schedule, the program makes updates to the schedule starting at a defined status date in each period, and updates are made to the schedule based on all changes up to that date. The three critical path tasks in question had changes that were past the defined status date. As such, notes were put in the schedule for the next update cycle. These notes would be used to incorporate the change into the following week’s update. This was explained in our Schedule Analysis comments provided to GAO in December 2022. The update process is the reason for the difference in calculating the critical path, not an issue with the critical path the program has calculated, and this was explained in our Schedule Analysis comments provided to GAO in December 2022. These efforts provided evidence that satisfies a large portion of the criterion of this best practice.

DHS remains committed to improving its program management and oversight of the HART program, as well as ensuring that OBIM continues to identify and address any

privacy risks in its systems as the Department works to achieve HART Program Initial Operational Capability.

The draft report contained nine recommendations with which the Department concurs. Enclosed you will find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

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

Sincerely,

JEFFREY M BOBICH

Digitally signed by JEFFREY M
BOBICH
Date: 2023.08.04 14:54:25 -04'00'

Jeffrey M. Bobich
Acting Chief Financial Officer
Office of the Chief Financial Officer

Enclosure

4

**Enclosure: Management Response to Recommendations
Contained in GAO-23-105959**

GAO recommended that the Secretary of Homeland Security direct the OBIM Director to:

Recommendation 1: Update the cost estimate for the HART program to account for all costs and incorporate the best practices called for in the GAO Cost Estimating and Assessment Guide.

Response: Concur. MGMT OBIM will update the HART Cost Estimating Baseline Document (CEBD) and HART LCCE to align with GAO's best practices, as appropriate. However, regarding the best practice of performing an independent cost estimate (ICE), it is important to clarify that the Cost Analysis Division (CAD) and the HART program office work closely together in the development of the program's LCCE during the program's annual updates to their LCCE, and CAD routinely conducts independent cost assessments (ICAs) on the program's cost estimate. The result of CAD's ICA provides the DHS Chief Financial Officer and Under Secretary for Management assurance that the LCCE is reliable and suitable for making critical acquisition decisions. Further, the goal of an ICE is to reach the same conclusion of high-quality cost estimating results and to provide decision makers with the same great insight that the Department is meeting with ICAs. Accordingly, the best practice of conducting an ICE would be a significant increase in CAD's efforts to produce similar results to those that CAD currently provides with less effort. For these reasons, OBIM will not conduct an ICE of the HART program.

As HART is currently in the initial rebaseline planning process, an estimated completion date (ECD) for the HART Increment 1 Rebaseline CEBD and HART Increment 1 Rebaseline LCCE cannot be provided at this time because they are contingent on available funding. However, DHS will be able to provide an ECD for the HART Increment 1 Rebaseline CEBD and HART Increment 1 Rebaseline LCCE after the HART Increment 1 Rebaseline Remediation Plan is completed in September 2023. With regards to Future Capabilities, the program is currently focused on Increment 1 development and delivery. Future Capabilities planning, to include updates to the HART CEBD and the HART LCCE, will be completed after HART Program Initial Operational Capability (IOC). These efforts include the following actions:

Actions	Estimated Completion Date (ECD)
HART Increment 1 Rebaseline Remediation Plan completion	September 29, 2023
HART Increment 1 Rebaseline CEBD update	TBD
HART Increment 1 Rebaseline LCCE completion	TBD
HART Future Capabilities CEBD update	TBD
HART Future Capabilities LCCE Completion	TBD

Overall ECD: TBD.

Recommendation 2: Revise the schedule estimate for the HART program that incorporates the best practices called for in the GAO Schedule Assessment Guide.

Response: Concur. OBIM will update the HART IMS to align to GAO's best practices, as appropriate. However, OBIM is already meeting the intent of the best practice of assigning resources (e.g., labor and materials) needed to complete the activities to determine whether they will be available when needed through the program's current processes. While all work breakdown structure areas in the HART IMS were resource assigned, the HART IMS was not resource-loaded. Rather, OBIM conducts resource demand management through OBIM's agile processes within a system called JIRA, in which the low-level requirements/stories are managed instead of the HART IMS (which captures higher-level epics and releases). OBIM's current agile processes control contractor and federal resource allocations, ensuring both are not overallocated. This process provides the program manager greater insight into resource allocations and issues as the lower-level requirements are tracked in JIRA. For these reasons, the Department will not add resource-loading into the HART IMS.

As HART is currently in the initial rebaseline planning process, an ECD for the HART Increment 1 Rebaseline IMS revision cannot be provided at this time because they are contingent on available funding. DHS will be able to provide an ECD for the HART Increment 1 Rebaseline IMS after the HART Increment 1 Rebaseline Remediation Plan is completed in September 2023. With regards to Future Capabilities, the program is currently focused on Increment 1 development and delivery. Future Capabilities planning, to include a revision to the HART IMS, will be completed after HART Program IOC. These efforts include the following actions:

Actions	ECD
HART Increment 1 Rebaseline Remediation Plan completion	September 29, 2023
HART Increment 1 Rebaseline IMS Revision completion	TBD
HART Future Capabilities IMS Revision completion	TBD

Overall ECD: TBD.

Recommendation 3: Coordinate with the Privacy Office to establish and implement a timeline for updating the HART PIA [privacy impact assessment] to fully describe the categories of individuals whose data will be stored in HART and the partners with whom the system shares information.

Response: Concur. OBIM Privacy will work with the DHS Privacy Office to highlight the identification of categories of individuals whose PII is stored in HART, and the partners with whom the system shares information, in the next HART PIA update.

ECD: July 31, 2024.

GAO recommended that the Secretary of Homeland Security direct the Privacy Office to:

Recommendation 4: Describe planned methodologies for determining that all privacy controls are implemented correctly and operating as intended for future control assessments of the HART program.

Response: Concur. Throughout GAO's work on this audit, the DHS Privacy Office described planned methodologies for determining that all privacy controls are implemented correctly and operating as intended for the HART program. Specifically, privacy controls are assessed through the entire privacy compliance documentation process, to include development of a Privacy Threshold Analysis (PTA), PIA, System of Records Notice (SORN), Privacy Act Statements, etc., as well as DHS privacy policies. Further, the implementation of the privacy controls is assessed during the privacy compliance documentation process.

The actual implementation of a Privacy Control as a specific process happens as a system is being built out/developed. The system/program, for example, builds in an auditing tool or a training program, while the PTA, PIA, and/or SORN are designed specifically to elicit responses from programs to assess whether the Privacy Control implemented/built into/added to a system is satisfactory. The PTA, PIA, and/or SORN documents that tool/program, and the Privacy Office assesses whether that Privacy Control's implementation is satisfactory. Because

the Privacy Controls either pass or fail, they are deemed satisfactory during the assessment of the PTA, PIA, or SORN. Further, the “Implementation Statement” section for each Privacy Control in the HART System Privacy Plan describes how the control is implemented/assessed (i.e., passes).

The following documentation was provided to GAO on October 25, 2022, as evidence of these processes:

- DHS Directive 047-01 “Privacy Policy and Compliance” dated July 7, 2011;⁵
- Instruction 047-01-001, “Privacy Policy and Compliance, dated July 25, 2011;⁶
- Several internal documents providing information on a crosswalk of Privacy Controls, a system security and privacy plan, and system screenshots.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

Recommendation 5: Develop a timeline for completing the planned HART privacy compliance review.

Response: Concur. The Chief Privacy Officer selected a new Privacy Oversight Director, who will enter on duty in September 2023, and will be responsible for completing Privacy Compliance Reviews (PCR). However, the DHS Privacy Office initial timeline for conducting a HART PCR was predicated on HART being fully implemented (HART Program IOC). Therefore, the DHS Privacy Office is unable to provide a timeline for completing the review until the HART Program IOC. These efforts include the following actions:

Actions	ECD
DHS Privacy Oversight Director entering on duty	September 29, 2023
HART Privacy Compliance Review timeline completed	TBD, one year after HART Program IOC

Overall ECD: TBD.

GAO recommended that the Secretary of Homeland Security direct the OBIM Director to:

Recommendation 6: Coordinate with the Privacy Office to establish and implement plans for correcting seven remaining privacy deficiencies identified in the HART PIA.

⁵ https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-directive-047-01_0.pdf

⁶ https://www.dhs.gov/sites/default/files/publications/privacy-policy-compliance-instruction-047-01-001_0.pdf

Response: Concur. OBIM Privacy will work with the DHS Privacy Office to plan, monitor, and address the seven remaining privacy recommendations identified in the HART PIA. Specifically, OBIM Privacy and the DHS Privacy Office will address corrective actions to close out the privacy recommendations once the DHS Privacy Office's Privacy Oversight Director enters on duty in September 2023. As the hiring process is not complete, a final timeline for this effort cannot be provided at this time. These efforts include the following actions:

Actions	ECD
DHS Privacy Oversight Director hired	September 29, 2023
OBIM and DHS Privacy Office review seven remaining privacy recommendations and establish timelines for correcting deficiencies	March 29, 2024
OBIM establishes and implements plans for correcting deficiencies for the seven remaining privacy recommendations	TBD per guidance from the DHS Privacy Oversight Director

Overall ECD: TBD.

GAO recommended that the Secretary of Homeland Security direct the Privacy Office to:

Recommendation 7: Ensure the complete HART authorization package is reviewed by the office prior to future system authorizations.

Response: Concur. The DHS Privacy Office will review the entire HART authorization package prior to the next "authority to operate" update. Specifically, the DHS Privacy Office will work with OBIM Privacy and the DHS Office of the Chief Information Officer/Office of the Chief Information Security Officer to ensure the HART authorization package is appropriately reviewed. The ECD is dependent on the HART authorization package moving forward as currently scheduled.

ECD: June 28, 2024.

GAO recommended that the Secretary of Homeland Security direct the OBIM Director to:

Recommendation 8: Establish and implement a timeline for maintaining a reliable inventory of information sharing and access agreements with partners that share data with HART.

Response: Concur. OBIM Privacy will revise its inventory listing of information sharing and access agreements with partners that share data with HART to ensure

the inventory provides reliable information on what Departmental agreements align to which partners, and whether these partners are current or planned users of HART. In addition, OBIM will maintain an inventory of agreements related to HART, and will establish a timeline for review and updates to the inventory listing and inventory on a consistent basis.

ECD: July 31, 2024.

Recommendation 9: Establish and maintain a process for ensuring that partners that provide data to HART have used the system's services to help to appropriately dispose of PII from the system, in accordance with applicable retention schedules.

Response: Concur. OBIM will establish and maintain a process for ensuring that partners that provide data to HART are using HART services to remove PII from the system in accordance with their National Archives and Records Administration-approved records schedules. This process will strengthen Government, mission-partner, and public trust by defining, managing, and remediating potential over-retention of PII in HART.

ECD: September 30, 2024.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contact

Marisol Cruz Cain, (202) 512-5017, cruzcainm@gao.gov

Staff Acknowledgments

In addition to the contacts listed above, the following staff made significant contributions to this report: Shannin O'Neill (assistant director), Hannah Brookhart (analyst in charge), Mathew Bader, Christopher Businsky, Emile Ettedgui, Rebecca Eyler, Yvette Gutierrez, Franklin Jackson, William Laing, Jennifer Leotta, Lee McCracken, Nolan Roosa, Lucas Scharf, Andrew Stavisky, Adam Vodraska, and Andrew Weiss.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



**ICE Did Not Accurately
Measure and Report
Its Progress in Disrupting
or Dismantling
Transnational Criminal
Organizations**





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

September 19, 2023

MEMORANDUM FOR: Patrick J. Lechleitner
Deputy Director and Senior Official Performing the
Duties of the Director
U.S. Immigration and Customs Enforcement

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

Signed by

Glenn Sklar GLENN E SKLAR
Principal Deputy Inspector General

Digitally signed by
GLENN E SKLAR
Date: 2023.09.15
23:33:10 -04'00'

SUBJECT: *ICE Did Not Accurately Measure and Report Its Progress
in Disrupting or Dismantling Transnational Criminal
Organizations*

For your action is our final report, *ICE Did Not Accurately Measure and Report Its Progress in Disrupting or Dismantling Transnational Criminal Organizations*. We incorporated the formal comments provided by your office.

The report contains three recommendations aimed at improving the Significant Case Report program's overall effectiveness. Your office concurred with all three recommendations.

Based on information provided in your response to the draft report, we consider recommendations 1 through 3 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your response or closure request to oigauditsfollowup@oig.dhs.gov.

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

Please contact me with any questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits, at (202) 981-6000.



DHS OIG HIGHLIGHTS

ICE Did Not Accurately Measure and Report Its Progress in Disrupting or Dismantling Transnational Criminal Organizations

September 19, 2023

Why We Did This Audit

ICE investigates, disrupts, and dismantles transnational criminal threats facing the United States. ICE HSI established the SCR process to identify the most critical investigations, measure and report its progress in disrupting or dismantling criminal organizations, and justify requests for additional resources to Congress. We conducted this audit to determine whether ICE HSI accurately reported to the public its progress in disrupting or dismantling TCOs and leveraged SCR data to inform resource allocations.

What We Recommend

We made three recommendations to help ICE HSI accurately measure and report annual performance data on disrupting and dismantling TCOs and use the data to inform resource requests.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) did not accurately measure and publicly report its progress in disrupting and dismantling transnational criminal organizations (TCO) from fiscal years 2017 through 2022. We reviewed a sample of 422 approved Significant Case Reports (SCR) and determined that 253 (60 percent) did not describe an entity that aligned with HSI's definition of a TCO. HSI included 171 of these non-TCO-related SCRs in its public reporting of TCO disruptions and dismantlements. This occurred because HSI officials relied on SCR approval data, which did not distinguish between TCO-related and non-TCO-related SCRs. As a result, ICE, Congress, and the public do not know how many TCOs HSI disrupted or dismantled from FY 2017 through FY 2022.

Additionally, we reviewed all resource requests that program offices submitted to HSI Office of Administrative Operations from FY 2017 through FY 2022. HSI program officials did not use SCR data in 125 of the 128 (98 percent) resource requests submitted during this period. This occurred because ICE and HSI's annual resource request guidance did not require HSI to consider SCR data. As a result of not including SCR data when applicable, ICE is missing an opportunity to share important information in its resource requests to Congress.

ICE Response

ICE concurred with all three recommendations, which we consider open and resolved.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

Transnational criminal organizations (TCO) place vulnerable Americans at risk while profiting from various schemes such as trafficking drugs, humans, or weapons; smuggling migrants; or laundering money. As the largest investigative arm within the Department of Homeland Security, U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) investigates, disrupts, and dismantles transnational criminal threats facing the United States. HSI defines¹ a TCO as: “A self-perpetuating association of individuals who operate across international borders for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means.” (See Figure 1.)

Figure 1. What Is a TCO?



Source: DHS Office of Inspector General analysis of Significant Case Report (SCR) handbooks

In 2005, the U.S. Government Accountability Office (GAO) reported² ICE did not have outcome-based performance goals (measures and targets) reflecting how its various investigative activities contribute to the component’s mission and objectives. In 2010, to address a recommendation from GAO’s report, ICE established the SCR process. The SCR process was intended to help HSI identify and categorize the most critical investigations, measure and report its progress in disrupting or dismantling criminal organizations, and justify requests for additional resources to Congress.

The SCR process begins when an HSI special agent identifies a significant criminal case that is targeting a TCO or national security threat. The agent then requests that the initial significant investigation report be designated as

¹ *HSI Significant Case Report Handbook*, HSI HB 22-01, January 3, 2022.

² GAO-06-48SU, *Better Management Practices Could Enhance DHS’s Ability to Allocate Investigative Resources* (December 2005).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

an SCR in ICE's Investigative Case Management (ICM) system. After this initial designation is approved, special agents may submit subsequent SCRs for HSI activities if the case results in a disruption or dismantlement.

- HSI designates an SCR as a disruption when the investigation impedes the normal and effective operation of the targeted organization or criminal activity.
- HSI designates an SCR as a dismantlement when action(s) taken eliminate the target organization's leadership, network, and financial base, such that the organization is incapable of reconstituting itself.³
- One criminal case may have more than one approved SCR.

When entering details about an SCR in ICM, special agents indicate the type of criminal activity the case relates to, such as national security, cyber-enabled crime, illicit trade, or foreign or domestic public corruption.

After a special agent submits an SCR for consideration, the SCR undergoes multiple levels of review, including by operations managers and an SCR panel consisting of representatives from multiple program areas. The Assistant Director for Domestic Operations approves each submission (see Figure 2).

Figure 2. SCR Process and Public Reporting



Source: DHS OIG analysis of HSI Office of Administrative Operations (OAO) strategic measure calculation and SCR handbooks

After SCRs are approved, HSI's OAO uses SCR data to measure and publicly report⁴ on HSI's work related to disrupting and dismantling TCOs. Specifically, one of the strategic measures HSI uses in its annual Congressional

³ HSI, *Significant Case Report Handbook* (October 2014, updated February 2016).

⁴ DHS Annual Performance Reports and Congressional Justifications.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Justification⁵ is the number/percent of significant⁶ HSI cases that resulted in a disruption or dismantlement, which is related to TCOs. HSI publicly reported its progress as a percentage from fiscal years 2017 through 2020 by dividing the sum of disruptions and dismantlements by all approved initial investigations. Starting in FY 2021, HSI changed to publicly reporting a total cumulative number of disruptions or dismantlements. According to HSI's public reporting, the office met its performance target for disrupting or dismantling TCOs every year except for FY 2019⁷ (see Table 1).

Table 1. ICE's FY 2017 – FY 2022 Performance Measure and Results for Significant Cases that Disrupted or Dismantled TCOs

Description	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022
Performance Target	15.8%	15.8%	15.9%	16.1%	366	540
HSI Results	22.9%	18.0%	15.1%	24.8%	698	1,083

Source: ICE Congressional Justifications and HSI data

Executive Order 13773⁸ requires Federal law enforcement agencies to prioritize and devote sufficient resources to investigate, apprehend, and prosecute TCO members to disrupt and dismantle these organizations. Through ICE's annual resource request process, HSI officials request funding necessary to achieve the objectives, commitments, and priorities of the Department, within fiscal guidance constraints. The SCR process also allows HSI to better justify requests for additional resources and enhances HSI's ability to align those resources with changing threats, priorities, and performance.⁹

⁵ Congressional Justifications outline agency goals and objectives and include annual funding requests.

⁶ To be considered significant, the investigation must involve a high-threat TCO engaged in criminal activity related to child exploitation; travel or finance (both drug-related and non-drug-related); illicit trade; counterterrorism; worksite enforcement; gangs; or national security.

⁷ HSI missed its target in FY 2019 due to a realignment of resources in support of unplanned initiatives that indirectly contributed to a decline in disruptions or dismantlements.

⁸ Executive Order 13773, *Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking*, February 9, 2017.

⁹ HSI memorandum, *New HSI Performance Measures and Significant Case Report (SCR) Module in TECS – Scheduled Release Date: November 15, 2010* (November 12, 2010).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We conducted this audit to determine whether ICE HSI accurately reported to the public its progress in disrupting or dismantling TCOs and leveraged SCR data to inform resource allocations.

Results of Audit

ICE HSI did not accurately measure and publicly report its progress disrupting or dismantling TCOs from FY 2017 through FY 2022. We reviewed a sample of 422 approved SCRs and determined that 253 SCRs (60 percent) did not describe an entity that aligned with HSI's definition of a TCO. Specifically, many of the approved SCRs that we identified as not TCO-related involved one individual committing a crime in the United States and not crossing any international borders. HSI included 171 of these non-TCO-related SCRs in its public reporting of TCO disruptions and dismantlements. This occurred because HSI officials relied on SCR approval data, which did not distinguish between TCO-related and non-TCO-related SCRs. As a result, ICE, Congress, and the public do not know how many TCOs HSI disrupted or dismantled from FY 2017 through FY 2022.

Additionally, HSI did not use SCR data to inform its resource requests in 125 of the 128 (98 percent) documents prepared as part of ICE's resource request process from FY 2017 through FY 2022. This occurred because ICE and HSI's annual resource request guidance did not require HSI to consider SCR data. As a result of not including SCR data when applicable, ICE is missing an opportunity to share important information in its resource requests to Congress.

HSI Inaccurately Reported Progress in Disrupting or Dismantling TCOs

The *GPRA Modernization Act of 2010*¹⁰ requires all Federal agencies to publicly report actual performance against established performance measures. However, from FY 2017 through FY 2022, HSI did not accurately publicly report¹¹ its progress against its established performance measure of disrupting or dismantling TCOs. Instead, the results that HSI publicly reported included cases that did not involve entities meeting its definition of a TCO.

¹⁰ Pub. L. 111-352. GPRA stands for the *Government Performance and Results Act of 1993*.

¹¹ DHS, *Annual Performance Report, FYs 2017–2019; FYs 2018–2020 Annual Performance Report; FYs 2019–2021 Annual Performance Report; FYs 2020–2022 Annual Performance Report*; Congressional Justifications.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

We selected a statistical sample of 258 cases from a total of 5,016 cases. Each case file contained one or more approved SCRs from FY 2017 through FY 2022, totaling 422 SCRs. We reviewed each of the 258 case files to determine whether the case met HSI's definition of a TCO, i.e., that the case 1) involved an association of individuals, and 2) involved crossing international borders. Of the 258 cases, we determined that 145 cases had 253 approved SCRs that did not describe an entity that aligned with HSI's definition of a TCO. These 253 approved SCRs included 52 SCRs that had no association of individuals, 54 SCRs that did not cross international borders, and 147 SCRs that had no association of individuals and did not cross international borders (see Table 2).

We can project, at a 90 percent confidence level, that 2,819 (56 percent) significant HSI cases¹² during this timeframe did not involve entities that met the definition of a TCO.

Table 2. SCRs Not Involving Entities That Met the TCO Definition

Criminal Category Description	(A) No Association of Individuals	(B) Did Not Cross International Borders	Both (A) and (B)	Total
Transnational Crimes Against Children	38	11	107	156
Counter-Proliferation	3	0	0	3
Illicit Trade, Travel, and Finance (Non-Drug-Related)	4	19	9	32
Cyber-Enabled Crime	0	1	0	1
Illicit Trade, Travel, and Finance (Drug-Related)	0	19	1	20
Worksite Enforcement/Labor Exploitation	0	3	0	3
Transnational Gangs	0	1	0	1
National Security	7	0	30	37
Total	52	54	147	253

Source: DHS OIG analysis of approved SCRs

¹² The range of possible values that might be present in the 5,016 cases includes a lower bound limit of 2,564 of 5,016 (51 percent) cases and an upper bound limit of 3,074 of 5,016 (61 percent) cases. This corresponds to a +/- 5 percent margin of error.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We determined that HSI included 171 of 253 approved SCRs that did not involve a TCO in annual reporting calculations of its key performance measure from FY 2017 through FY 2022. Of these, HSI reported at least 123 specifically as disruptions and dismantlements for the same time period (see Table 3). Because HSI publicly reported its progress as a percentage from FY 2017 through FY 2020 by dividing the sum of disruptions and dismantlements by all approved initial investigations, HSI included the remaining 48 initial investigation SCRs when reporting progress as a percentage.

Table 3. Comparison of Disruptions and Dismantlements Publicly Reported and Those OIG Identified as Inaccurately Reported

Description	FY 2017	FY 2018	FY 2019	FY 2020	FY 2021	FY 2022	TOTAL
Reported Results	420	347	322	618	698	1,083	3,488
Inaccurately Reported	13	15	7	18	23	47	123

Source: DHS OIG analysis of sampled approved SCRs and HSI performance results calculations

This occurred because HSI OAO staff relied on SCR approval data that did not distinguish between TCO-related and non-TCO-related SCRs. HSI OAO staff did not validate the data used to calculate progress toward HSI's key TCO performance measure to ensure it actually represented SCRs that met HSI's definition of a TCO. For HSI officials to approve an SCR, the SCR must meet the established criteria for the assigned category and subcategory. However, some categories and subcategories do not require that the SCR involve an entity that meets the definition of a TCO. For example, multiple subcategories related to crimes against children did not require an association of individuals operating across international borders. As shown in Table 2, we identified 107 approved SCRs related to crimes against children that only involved single domestic offenders. In another example, the Worksite Enforcement/Labor Exploitation category does not require an SCR to identify an association operating across international borders. As shown in Table 2, we identified three approved SCRs in this category that did not involve crimes across international borders.

As a result of inaccurate reporting, ICE, Congress, and the public do not know how many TCOs HSI disrupted or dismantled from FY 2017 through FY 2022.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

HSI Did Not Use SCR Data to Justify Resource Requests

According to a November 2010 HSI memorandum¹³ and the SCR handbooks, the SCR process allows HSI to generate data it can use to better inform its resource requests for future law enforcement activity. ICE and HSI's annual resource request guidance¹⁴ explained that justifications for budget requests can be more compelling by incorporating data and tangible outcomes. As part of ICE's annual resource request process, HSI OAO officials request that program offices develop and submit resource requests for resources needed to complete their missions. Resource requests should include a description, justification, cost, and impact of the resources on HSI's performance.

We reviewed all resource requests that program offices submitted to HSI OAO from FY 2017 through FY 2022. We determined HSI program officials did not use SCR data in 125 of the 128 (98 percent) resource requests submitted during this period. For example:

- In FY 2022, HSI requested \$3.0 million and 16 positions to ensure HSI Victim Assistance Program personnel had the necessary tools and resources to provide critical victim assistance. This program responded to victims' needs in a range of crimes, including human trafficking, child pornography and child sex tourism, and human rights abuses. Although SCR data from the Illicit Trade, Travel, and Finance (non-drug-related); Transnational Crimes Against Children; and National Security SCR categories may have further supported this request, HSI did not consider data from these categories or related subcategories.
- In FY 2020, HSI requested \$8.8 million and 12 positions for the Cyber Crimes Center's Cyber Crimes Unit to provide advanced capabilities, training, and personnel to effectively counter TCOs and malicious cyber threats. Although SCR data from the Cyber-Enabled Crime SCR category may have further supported this request, HSI did not consider data from this category or its subcategories.

¹³ HSI memorandum, *New HSI Performance Measures and Significant Case Report (SCR) Module in TECS – Scheduled Release Date: November 15, 2010* (November 12, 2010).

¹⁴ ICE Office of Budget and Program Performance (OBPP) FY 2021 Resource Allocation Plan (February 20, 2019); HSI Budget Formulation and Reporting (BFR) FY 2022 Resource Allocation Plan Quad Chart Data Call (February 2020); HSI BFR, Pre-FY 2023 Resource Allocation Plan, Quad Chart Data Call (November 2020); OBPP Budget Formulation FY 2023 Resource Allocation Plan (December 14, 2020); HSI BFR FY 2024 Pre-Resource Allocation Plan Quad Chart Data Call (November 2021).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- In FY 2020, HSI requested \$10.6 million and five positions for the Child Exploitation Investigations Unit to enhance its investigative capacity to combat child exploitation and keep up with emerging trends and technology. Although SCR data from the Transnational Crimes Against Children SCR category may have further supported this request, HSI did not consider data from this category or at least four related subcategories.

HSI program officials did not use SCR data because ICE and HSI's annual resource request guidance did not require HSI to consider SCR data. As a result of not including SCR data when applicable, ICE is missing an opportunity to share important information in its resource requests to Congress.

Recommendations

Recommendation 1: We recommend the Homeland Security Investigations Executive Associate Director require special agents to identify in the Investigative Case Management system whether each Significant Case Report submission involves an entity that meets HSI's definition of a transnational criminal organization.

Recommendation 2: We recommend the Homeland Security Investigations Executive Associate Director implement data validation processes to ensure accurate reporting of disruptions and dismantlements of transnational criminal organizations.

Recommendation 3: We recommend the Homeland Security Investigations Assistant Director of Administrative Operations develop and implement guidance for program offices to require the use of Significant Case Report data, where applicable, in their annual resource requests to Congress.

Management Comments and OIG Analysis

ICE concurred with all three recommendations, and we consider them open and resolved. Appendix A contains ICE's management comments in their entirety. We also received technical comments on the draft report and made revisions as appropriate. A summary of ICE's responses and our analysis follows.

ICE commented that it does not believe the method of selecting the random sample noted in the draft report was adequately documented. The report



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

clearly documents the sampling selection process and methodology in the Objective, Scope, and Methodology section. Additionally, ICE expressed concern that the report identifies a projection with a 90 percent confidence level and does not include a range for the projection. The range is included in footnote 12, as 51 to 61 percent. We also provided HSI an opportunity to review and validate the SCR testing results and made changes as appropriate in May and June 2023.

ICE Response to Recommendation 1: Concur. ICE HSI has updated its ICM system with a new “TCO involvement” yes/no checkbox that is mandatory when users create SCRs. ICE will develop associated instructions, training, and updated memorandums during FY 2024. Estimated Completion Date (ECD): September 30, 2024.

OIG Analysis of ICE Comments: ICE’s corrective action plan is responsive to the recommendation. In August 2023, DHS OIG observed enhancements to ICM as a result of this audit project and credits ICE for taking immediate steps toward resolving this recommendation. This recommendation will remain open and resolved until ICE provides evidence it developed associated instructions, training, and updated memorandums during FY 2024 as well as evidence of several monthly SCR panel reviews under the new processes in place.

ICE Response to Recommendation 2: Concur. HSI OAO will implement data validation processes for SCRs in ICM beginning in the first quarter of FY 2024. ECD: November 29, 2024.

OIG Analysis of ICE Comments: ICE’s corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved until ICE provides documentation showing that HSI OAO has implemented data validation processes to enhance the accuracy of its reporting against the established performance measure of the number of significant cases disrupting or dismantling TCOs.

ICE Response to Recommendation 3: Concur. HSI OAO will develop guidance and training documents to require the use of SCR data in program offices’ annual resource requests to Congress, as appropriate. Additionally, when reviewing budget request proposals, HSI budget analysts will recommend program offices use SCR data. ECD: January 31, 2024.

OIG Analysis of ICE Comments: ICE’s corrective action plan is responsive to the recommendation. This recommendation will remain open and resolved



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

until ICE provides documentation showing updated guidance and training materials requiring the use of SCR data in program offices' annual resource requests to Congress, as appropriate. Additionally, DHS OIG will need to see evidence that HSI budget analysts made recommendations for program offices to use SCR data, when appropriate.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

We conducted this audit to determine whether ICE HSI accurately reported to the public its progress in disrupting or dismantling TCOs and leveraged SCR data to inform resource allocations. The audit focused on SCRs approved by HSI officials from FY 2017 through FY 2022.

To answer our objective, we reviewed and analyzed relevant Federal laws and executive orders, congressional testimony, prior audit reports, and component policies and guidance. We also interviewed officials from program offices including:

- ICE's Budget and Program Performance Division's Budget Operations and Performance Analysis and Evaluation units to understand ICE's resource request and strategic measurement process;
- HSI OAO to understand how HSI identifies its annual resource needs and how this information flows from HSI to ICE; and
- HSI's Domestic Operations Division, including the SCR program manager, to understand the SCR program and the process for reviewing and approving SCR submissions.

We assessed HSI's internal control structure as it related to the audit objective. We identified and reported deficiencies in the control activities, monitoring, and information and communication components of internal control. Because we limited our review to addressing our audit objective, our work may not have identified all internal control deficiencies that may have existed at the time of this audit.

To determine whether HSI accurately reported to the public its progress in disrupting or dismantling TCOs, we requested and obtained 8,275 SCRs approved in ICM from FY 2017 through FY 2022. We verified accuracy of the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

date parameters and record totals from our ICM data request. We ensured no missing, unexplained, or duplicate records were present. We deemed the ICM SCR approval dataset to be reliable for the purposes of our audit work.

We worked with the DHS OIG Data Services Division to select a simple random statistical sample from the 8,275 approved SCRs, which corresponded to 5,016 unique cases. We used a 90 percent confidence level and 5 percent margin of error to select a statistical sample of 258 cases from these 5,016 cases. These 258 cases correspond to 422 approved SCRs. We tested each approved SCR to ensure it aligned with HSI guidance and to determine whether HSI accurately reported the SCR to the public as part of its annual performance measure. DHS OIG's Data Services Division reviewed and validated our statistical sample and its results, and we accurately captured those results in this report. We also provided HSI an opportunity to review and validate the SCR testing results and made appropriate changes as needed in May and June 2023.

To determine whether HSI used SCR data to inform its resource requests, we reviewed all 128 resource requests that program offices submitted to HSI OAO from FY 2017 through FY 2022.

We conducted this performance audit between September 2022 and June 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Office of Audits major contributors to this report are Shelley Howes, Director; Stephanie Brand, Audit Manager; Andrew Herman, Auditor-In-Charge; Joshua Simon, Senior Auditor; Justin Kerr, Senior Auditor; Maria Romstedt, Communications Analyst; Sandra Parsons, Assistant Inspector General for Innovation; Gaven Ehrlich, Supervisory Program Analyst; Azriel Krongauz, Data Scientist; Muhammad (Faizul) Islam, Statistician; and Oscar Andino, Independent Referencer.

DHS OIG's Access to DHS Information

During this audit, HSI provided timely responses to DHS OIG's requests for data and records and did not delay or deny access to information we requested.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
ICE Comments to the Draft Report

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536



**U.S. Immigration
and Customs
Enforcement**

August 28, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Max Aguilar **MAX L AGUILAR** Digitally signed by MAX L AGUILAR
Chief Financial Officer (Acting) and Deputy Executive Date: 2023.08.28 11:54:37 -04'00'
Associate Director for Management and Administration
U.S. Immigration and Customs Enforcement

SUBJECT: Management Response to Draft Report: "ICE Did Not
Accurately Measure and Report Its Progress in Disrupting or
Dismantling Transnational Criminal Organizations"
(Project No. 22-060-AUD-ICE)

Thank you for the opportunity to review and comment on this draft report. The U.S. Immigration and Customs Enforcement (ICE) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

ICE leadership is pleased to note OIG's recognition of ICE Homeland Security Investigations' (HSI) significant impact over the years in disrupting and dismantling transnational criminal organizations (TCOs). ICE HSI Special Agents, in collaboration with partners in the United States and abroad, develop evidence to identify and build criminal cases against TCOs, terrorist networks and facilitators, and other criminal elements that threaten the Homeland. HSI also works with prosecutors to take actions including arresting and indicting violators, executing criminal search warrants, and seizing criminally derived money and assets, and take other actions with the goal of disrupting and dismantling TCOs operating throughout the world. These efforts help protect the national security and public safety of the United States.

More specifically, HSI International Operations has a network of over 400 personnel, including over 225 special agents, deployed to 86 offices and 9 Department of Defense liaisons in 55 countries, including the United States, who conduct investigations against terrorist and other criminal organizations that threaten our national security. HSI International Operations disrupts and dismantles TCOs that seek to exploit America's legitimate trade, travel and financial systems, and enforces U.S. customs and immigration

www.ice.gov



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Response to Draft Report: "ICE Did Not Accurately Measure and Report Its Progress in Disrupting or Dismantling Transnational Criminal Organizations"
(Project No. 22-060-AUD-ICE)
Page 2

laws at and beyond our nation's borders to prevent threats from entering the United States.

These efforts include Transnational Criminal Investigative Units (TCIUs) in 11 countries. HSI TCIUs are comprised of foreign law enforcement officials, customs officers, immigration officers and prosecutors who undergo a strict vetting process to ensure that shared information and operational activities are not compromised. Aligned with the President's Strategy in Combatting Transnational Organized Crime,¹ TCIUs identify targets, collect evidence, share intelligence, and facilitate the prosecution of TCOs both in-country and through the U.S. judicial system.

While ICE leadership agrees it is important to accurately report on its performance measures for TCOs, leadership is concerned with the validity of the OIG's findings, given the dearth of documentation on the statistical method used for this audit. For example, ICE does not believe the method of selecting the random sample noted in OIG's draft report was adequately documented, so it is unclear whether the auditors used a stratified random sample or a simple random sample, and use of two different sampling methods could impact the reported results. Further, regarding OIG's statement on page 5 of the draft report, "We can project, at a 90 percent confidence level, that 2,819 (56 percent) significant HSI cases during this timeframe did not involve entities that met the definition of a TCO," it is not clear whether this sentence includes only a single point estimate instead of a range using the confidence interval. Therefore, ICE is unable to validate the assertion.

The draft report contained three recommendations with which ICE concurs. Enclosed find our detailed response to each recommendation. ICE previously submitted technical comments addressing several accuracy, contextual, sensitivity and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

Enclosure

¹ <https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime>



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Response to Draft Report: "ICE Did Not Accurately Measure and Report Its Progress in Disrupting or Dismantling Transnational Criminal Organizations"
(Project No. 22-060-AUD-ICE)
Page 3

Enclosure: Management Response to Recommendations Contained in 22-060-AUD-ICE

OIG recommended that the ICE HSI Executive Associate Director:

Recommendation 1: Require special agents to identify in the Investigative Case Management system whether each Significant Case Report submission involves an entity that meets HSI's definition of a transnational criminal organization.

ICE Response: Concur. On July 18, 2023, the ICE HSI Cyber and Operational Technology (COT) implemented a new "TCO involvement" yes/no checkbox that is now mandatory when users create Significant Case Reports (SCRs) in the Investigative Case Management (ICM) System. ICE will develop associated instructions, training, and update memorandums during fiscal year (FY) 2024. The first SCR panel review of FY 2024 will be held on October 18, 2023. This will sufficient time following completion of the planned September 18, 2023, panel review to prepare and provide guidance to Desk Officers and panel members with specific instruction in approving the TCO designation. Estimated Completion Date (ECD): September 30, 2024.

Recommendation 2: Implement data validation processes to ensure accurate reporting of disruptions and dismantlements of transnational criminal organizations.

ICE Response: Concur. HSI Office of Administrative Operation (OAO) will implement data validation processes for SCRs in the ICM system. Beginning in quarter one of FY 2024, HSI OAO will report SCR data that includes the newly implemented "TCO involvement" indicator in ICM. ECD: November 29, 2024.

OIG recommended that the ICE HSI Assistant Director of Administrative Operations:

Recommendation 3: Develop and implement guidance for program offices to require the use of Significant Case Report data, where applicable, in their annual resource requests to Congress.

ICE Response: Concur. HSI OAO will develop guidance to require the use of SCR data in program offices' annual resource requests to Congress, as appropriate. The guidance will be incorporated into the annual Resource Allocation Process training, which is typically scheduled in October of each FY. In addition, HSI budget analysts will make recommendations to the programs for the use of SCR data when conducting their review



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Management Response to Draft Report: "ICE Did Not Accurately Measure and Report Its Progress in Disrupting or Dismantling Transnational Criminal Organizations"
(Project No. 22-060-AUD-ICE)
Page 4

of budget request proposals. HSI OAO plans to complete the initial updated training to use of Significant Case Report data by December 29, 2023. ECD: January 31, 2024.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix B

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
ICE Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

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

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



OIG Hotline

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

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

ICE Should Improve Controls Over Its Transportation Services Contracts





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

September 25, 2023

MEMORANDUM FOR: Patrick J. Lechleitner
Senior Official Performing the Duties of the Director
U.S. Immigration and Customs Enforcement

FROM: Joseph V. Cuffari, Ph.D. **JOSEPH V CUFFARI** Digitally signed by
Inspector General Date: 2023.09.25
09:49:18 -04'00'

SUBJECT: *ICE Should Improve Controls Over Its Transportation
Services Contracts*

Attached for your action is our final report, *ICE Should Improve Controls Over Its Transportation Services Contracts*. We incorporated the formal comments provided by your office.

This report contains seven recommendations to improve U.S. Immigration and Customs Enforcement's oversight of its transportation services contracts. Your office concurred with all seven recommendations. Based on information provided in your response to the draft report, we consider all seven recommendations open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your closure request to OIGAuditsFollowup@oig.dhs.gov. We will distribute the final report to Congress and the public as appropriate with your formal comments included as an appendix.

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

Please contact me with any questions, or your staff may contact Kristen Bernard, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

ICE Should Improve Controls Over Its Transportation Services Contracts

September 25, 2023

Why We Did This Audit

ICE enforces the Nation's immigration laws and manages the safe and secure transportation of apprehended noncitizens for removal. From October 2019 through April 2022, ICE obligated \$799 million across 13 contracts for transportation of noncitizens. We conducted this audit to determine to what extent ICE complied with Federal, departmental, and component procurement guidance for monitoring and overseeing transportation contracts.

What We Recommend

We made seven recommendations to improve ICE's oversight of its transportation services contracts.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

U.S. Immigration and Customs Enforcement (ICE) did not fully comply with Federal and departmental guidance for monitoring and overseeing transportation contracts. Specifically, ICE did not always appoint contracting officer's representatives (COR) according to policy. Also, ICE did not consistently use quality assurance surveillance plans to monitor contractor performance. Lastly, ICE did not adequately review invoices to ensure expenses were correct, supported, and reasonable, resulting in \$408,875 in erroneous or unsupported payments and \$900,144 that could have been put to better use.

This occurred because ICE contracting staff do not have a consistent understanding of COR appointment requirements, nor does ICE have guidance on how to implement existing Federal and Department policies on COR appointments and methods of quality assurance. Also, CORs have multiple competing responsibilities that could have impacted their ability to conduct quality assurance and accurately review invoices. Without improvements, ICE cannot be assured that it is receiving services that conform to contract requirements.

ICE Response

ICE concurred with our recommendations. We consider all seven recommendations resolved and open.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

U.S. Immigration and Customs Enforcement's (ICE) Enforcement and Removal Operations manages the immigration enforcement process by identifying, arresting, and removing noncitizens who are in the United States unlawfully. This entails transporting noncitizens,¹ including single adults, unaccompanied children, and family units, who were apprehended by U.S. Customs and Border Protection and other agencies. ICE transports these noncitizens to locations such as ICE detention centers, Family Residential Centers, U.S. Department of Health and Human Services Office of Refugee Resettlement facilities, or the noncitizen's home country, depending on the circumstances surrounding the apprehension. This transportation occurs via ground or air transit.

To assist with ICE's mission of transporting apprehended noncitizens, the Office of Acquisition Management within ICE's Management and Administration Directorate contracts with vendors to provide transportation services. From October 2019 through April 2022, ICE reported that it obligated \$799 million and expended about \$746 million for 13 transportation services contracts. ICE awarded the contracts for transportation to be available when needed but did not track² the number of noncitizens transported per contract. See Table 1 for a summary.

Table 1. ICE's Transportation Contracts from October 2019 through April 2022 (in millions)

Contractor	Method of Transportation	Contract Type ³	Obligated Amount	Expended Amount
Contractor 1	Air	Hybrid	\$20.51	\$16.40
Contractor 2	Air	Hybrid	\$300.00	\$290.75
Contractor 3	Air	Firm-fixed price	\$4.77	\$4.77
Contractor 4	Air/Ground	Hybrid	\$285.60	\$255.15
Contractor 5	Ground	Firm-fixed price	\$23.71	\$22.96
Contractor 6	Ground	Firm-fixed price	\$13.94	\$13.78
Contractor 7	Ground	Firm-fixed price	\$27.16	\$25.33
Contractor 8	Ground	Hybrid	\$23.13	\$19.41

¹ Transportation services also include providing incidentals such as meals and water, clothing, travel kits, medical care, and lodging during transportation trips when applicable.

² We requested that ICE provide the number of noncitizens transported per contract, but ICE was unable to provide the data.

³ A hybrid contract contains firm-fixed price and time-and-materials, fixed unit and labor hour, or firm-fixed price and labor hour elements.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Contractor	Method of Transportation	Contract Type ³	Obligated Amount	Expended Amount
Contractor 9	Ground	Firm-fixed price	\$6.87	\$6.85
Contractor 10	Ground	Hybrid	\$14.44	\$14.36
Contractor 11	Ground	Hybrid	\$15.25	\$14.84
Contractor 12	Ground	Hybrid	\$37.02	\$34.54
Contractor 13	Ground	Firm-fixed price	\$26.57	\$26.57
Total	N/A	N/A	\$798.97	\$745.71

Source: Department of Homeland Security Office of Inspector General analysis of contract data provided by ICE from the Federal Financial Management System (FFMS)

The ICE Office of Acquisition Management follows the requirements within the Federal Acquisition Regulation (FAR)⁴ and departmental policies for contract administration and oversight. ICE's monitoring activities include site visits and quality assurance surveillance. In addition, ICE issues contract discrepancy reports and assesses liquidated damages when contractors do not perform. We conducted this audit to determine to what extent ICE complied with Federal, departmental, and component procurement guidance for monitoring and overseeing transportation contracts.

Results of Audit

ICE Did Not Comply with All Federal and Departmental Guidance for Monitoring and Overseeing Transportation Contracts

The FAR identifies roles and responsibilities for monitoring and oversight of Federal contracts. Contracting Officers (CO) are responsible for managing contractor performance and ensuring compliance with the terms of the contract. The FAR allows COs to appoint a contracting officer's representative (COR) to assist with administering the contract to ensure that the Government and contractor fulfill agreed upon terms. The COR's administrative duties consist of conducting surveillance to verify contractor performance, reporting deficiencies in performance, and reviewing invoices.⁵ The specific nature and extent of the duties vary from contract to contract; the level of involvement can

⁴ FAR 46.401(a). "Government contract quality assurance shall be performed at such times (including any stage of manufacture or performance of services) and places (including subcontractors' plants) as may be necessary to determine that the supplies or services conform to contract requirements."

⁵ Homeland Security Acquisition Manual Appendix W, *Contracting Officer's Representative (COR) Nomination and Appointment Correspondence*.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

range from minimal to extensive depending on the contract's complexity and type.

ICE Contracting Officers Did Not Always Appoint CORs in Accordance with DHS Acquisition Policy

According to DHS Acquisition Workforce Policy Number 064-04-003,⁶ CORs may be certified at Level II or Level III depending on the COR's training and experience and are appointed based on the type and complexity of the contract. A Level II COR is appointed to contracts that do not involve high risk or major investments, whereas a Level III COR is appointed to high-risk or major investment contracts. See Table 2 for DHS' COR certification level requirements.

Table 2. DHS COR Level Certification Requirements

COR Level	Contract Type	Initial Training Requirements	Minimum COR Experience
COR Level I	DHS does not certify Level I CORs	N/A	N/A
COR Level II	Other than high-risk or major investment contracts (such as firm-fixed price contracts)	40 hours	1 year
COR Level III	High-risk contracts or major investment contracts (such as hybrid contracts or time-and-materials contracts)	60 hours	2 years

Source: DHS OIG analysis of DHS Acquisition Workforce Policy Number 064-04-003

We reviewed 13 transportation services contracts and determined ICE did not always appoint CORs with the proper training and experience. Specifically, we found that ICE CORs for five high-risk contracts, with total reported expenditures of \$596.5 million, did not have the required Level III COR certification. For the remaining 8 contracts, ICE appointed an appropriately certified COR.

Additionally, we found COs did not always delegate duties to CORs using an appointment letter,⁷ as required by DHS acquisition policy. If a CO decides to appoint a COR, the CO must issue a letter to the COR outlining COR roles and

⁶ DHS Acquisition Workforce Policy Number 064-04-003, *The Federal Acquisition Certification for Contracting Officer's Representatives and Appointment and Revocation (Revision 2) Issued August 8, 2012*.

⁷ Homeland Security Acquisition Manual section 3042.270-3.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

responsibilities, and a copy of the COR appointment letter must be maintained in the contract file.⁸ DHS acquisition policy requires a separate COR appointment letter for each contract to which a COR is appointed. Also, according to senior ICE contracting staff, if an individual changes their role on a contract, such as when a primary COR is reappointed as an alternate COR (ACOR), an updated appointment letter should be issued.

COs made 42 COR and ACOR appointments for the 13 ICE transportation services contracts we reviewed. However, we found that 6 of 42 (14 percent) COR appointment letters were not in the contract files and could not be furnished upon request. Of the 36 COR appointment letters we received, 10 were not specific to the contract to which the COR was assigned. We also found that in six instances, ICE did not issue new appointment letters to reflect the COR's or ACOR's new role on the contract, as required. For example, ICE did not issue updated COR or ACOR letters when two ACORs became primary CORs and when four CORs became ACORs.

These issues occurred because ICE contracting staff did not have a consistent understanding of policies. For example, one ICE staff member said that “other than high risk”⁹ and “major investment” contracts did not have precise definitions, while another staff member said that COR levels are based on the dollar amount of the contract. We also attribute these issues to ICE acquisition policy not including procedures to implement Federal and departmental requirements for COR appointment letters. ICE's acquisition manual¹⁰ does not include specific guidance on how CORs should be appointed or how COR appointment letters should be retained in the contract files.

Without a clear understanding of the COR appointment policies, ICE may continue to appoint CORs who lack the training and experience necessary to accurately assess the contractor's performance. Further, until ICE's policies are revised to include procedures to implement the requirements for COR appointment letters, these letters may continue to be missing, outdated, or not specific to the contract. Additionally, if COR appointment letters do not clearly describe a COR's roles and responsibilities, ICE risks not receiving the level of services agreed to in the contract.

⁸ Homeland Security Acquisition Manual section 3004.803-70(c)(3).

⁹ In a 2011 memorandum on COR certification, the Office of Management and Budget considers contracts that are not firm fixed price, such as hybrid contracts, to be of high risk. See [Revisions to the Federal Acquisition Certification for Contracting Officer's Representatives \(FAC-COR\)](#), September 6, 2011.

¹⁰ The *ICE Acquisition Manual* issued June 2020 and revised in January 2022.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ICE CORs Did Not Always Adequately Monitor Contractor Performance

The FAR requires agencies to perform quality assurance to ensure the services received conform to contract requirements.¹¹ One tool that agencies use to monitor contracts is the quality assurance surveillance plan (QASP), which provides instructions to evaluate whether the contractor is meeting the performance standards identified in the contract's performance work statement. A QASP defines acceptable quality levels, describes methods to monitor contractor performance, and identifies the resources and documentation needed to assess performance.

ICE did not always prepare a QASP for CORs overseeing transportation services contracts. Specifically, ICE did not complete a QASP for 3 of 12¹² (25 percent) transportation services contracts we reviewed. Additionally, of the nine QASPs ICE prepared, one did not describe a surveillance method for the COR to verify contract performance.

CORs also did not always perform the monitoring activities outlined in the QASP. For example, one QASP required ICE to monitor the contractor's performance by interviewing contractor staff, noncitizens, and other government personnel, and by reviewing documentation in the performance standards such as training plans and certificates. However, the COR for the associated contract did not consistently conduct interviews or regularly obtain and review documentation. Instead of proactively conducting interviews, the COR often relied on ICE officers, the contractor, and noncitizens to come forward when they experienced issues.

According to the CO, three contracts did not have QASPs because it was not a contract requirement. In addition, CORs have multiple competing responsibilities, such as being appointed the COR or ACOR on multiple contracts, that could have impacted their ability to conduct quality assurance.

ICE's transportation services contracts have extensive performance work statements with numerous requirements. QASPs highlight specific requirements for contractor performance, allowing the COR to monitor the contract in a systematic manner. If ICE does not develop quality assurance tools such as a QASP, and CORs do not use them, then ICE may not be assured that the contractor is performing in accordance with contract requirements.

¹¹ FAR section 46.401(a).

¹² One contract did not have a QASP because it was a short-term contract.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ICE CORs Did Not Adequately Review Invoices

According to the Homeland Security Acquisition Manual, if delegated the responsibility to review invoices by the CO, the COR must ensure that the contractor completes and submits invoices in accordance with the contract.¹³ When a COR reviews and approves an invoice, the COR is certifying that the information is accurate and complete and that costs are allowable and reasonable. Costs are allowable if they comply with the terms of the contract — for example, billed rates on an invoice should match the rate specified in the contract — and are supported by adequate documentation to show that the costs claimed are allocable to the contract. A cost is reasonable if, in nature and amount, it does not exceed what would be incurred by a prudent person in the conduct of competitive business.

We reviewed approved invoices that four ICE transportation services contractors¹⁴ submitted in April 2022. When comparing the invoices to the contracts and supporting documentation, we found ICE paid \$408,875 in erroneous or unsupported charges. We identified the following issues:

- Contractor 5 charged an incorrect contract labor rate for transportation services, which resulted in an overcharge of \$8,549.
- Contractor 2 charged a higher flight hour rate before the rate's effective date, resulting in an overcharge of \$272,005.
- ICE could not provide supporting documentation for \$128,321 of Contractor 4's invoiced transportation expenses.

ICE also paid for costs that may not have been reasonable. For example, Contractor 4 provides charter bus services for transporting noncitizens. According to the COR, U.S. Border Patrol requested that buses be present each day at two Border Patrol stations due to a significant number of noncitizen encounters and the stations reaching maximum capacity. Contractor 4 secured the requested number of buses and submitted documentation supporting the cost as part of its invoices to ICE.

We reviewed Contractor 4's invoices from February 2022 through April 2022 and found that, although Border Patrol requested an average of eight buses each day, ICE regularly used only two or three of these buses each day to transport noncitizens from the two Border Patrol stations. The other requested

¹³ Although Homeland Security Acquisition Manual section 3032.7002 places ultimate responsibility for invoice review on COs, section 3001.602-2 allows COs to delegate some of their responsibilities to CORs.

¹⁴ See Table 1.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

buses remained in a “standby” status. Contractor 4’s invoices reflected that ICE paid more than twice as much for buses on standby than for buses that actually transported noncitizens. Specifically, charges for the standby buses represented 69 percent of the total charges Contractor 4 invoiced during this period. See Table 3 for a summary of the supporting documentation for Contractor 4’s bus services.

Table 3. Contractor 4 Bus Services from February through April 2022

Month	Trips Taken		Standby Charges		Totals	
	Buses	Amount	Buses	Amount	Buses	Amount
Feb. 2022	82	\$178,351	164	\$293,772	246	\$472,123
Mar. 2022	63	\$103,284	182	\$326,508	245	\$429,792
Apr. 2022	63	\$124,568	156	\$279,864	219	\$404,432
Total	208	\$406,203	502	\$900,144	710	\$1,306,347

Source: DHS OIG analysis of contract invoices

According to the COR appointment letter, the COR must review invoices for reasonableness. Although it is reasonable to have buses on standby to be ready for sudden surges of migrants, it may be unreasonable to pay for as many as nine buses almost daily, month after month, when ICE only uses two or three buses a day to transport noncitizens from the two Border Patrol stations. If ICE had balanced the number of buses it chartered with demand at those two Border Patrol stations, the funds used to pay the standby charges of \$900,144 could have been put to better use.

We attribute this lack of oversight to CORs having multiple competing responsibilities. One COR reported that their role as a COR is a secondary assignment to their primary work role and often, they do not have the time to review invoices in depth. Another COR serves either as the COR or an ACOR on 3 of the 13 contracts we reviewed. The invoices for these contracts are often substantial and contain charges associated with many detailed contract requirements. Without adequate staffing to review and approve invoices, ICE is prone to approving inaccurate and incomplete invoices, which can lead to unallowable costs.

Recommendations

Recommendation 1: We recommend the Executive Associate Director for Management and Administration ensure ICE appoints appropriately certified CORs to oversee high-risk transportation services contracts.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 2: We recommend the Executive Associate Director for Management and Administration ensure COs issue COR appointment letters to CORs who do not have them and reissue outdated COR appointment letters.

Recommendation 3: We recommend the Executive Associate Director for Management and Administration develop and implement procedures to ensure contracting staff issue COR appointment letters and maintain them in contract files.

Recommendation 4: We recommend the Executive Associate Director for Enforcement and Removal Operations develop and implement guidance to ensure that Enforcement and Removal Operations develops QASPs for contracts that include specific methods for monitoring contractor compliance with contract terms and develop procedures to ensure CORs use the QASPs as part of their oversight activities.

Recommendation 5: We recommend the Executive Associate Director for Enforcement and Removal Operations evaluate the workload for CORs and determine if sufficient resources are allocated to adequately oversee contracts and, based on the evaluation, develop, and implement a plan to more effectively manage or obtain additional personnel resources.

Recommendation 6: We recommend the Executive Associate Director for Management and Administration recover any monies, including the \$408,875 identified in this report, determined to have been paid toward inaccurate charges or costs not supported by documentation.

Recommendation 7: We recommend the Executive Associate Directors for Enforcement and Removal Operations and Management and Administration determine the reasonableness of the amount and frequency of standby bus charges.

Management Comments and OIG Analysis

ICE concurred with all seven recommendations. In its management response, ICE detailed efforts it has made to improve contract management. ICE provided technical comments to our draft report. We incorporated these comments into the report, as appropriate. A summary of ICE's responses and our analysis follows. We included ICE's management response in its entirety in Appendix A.

ICE Response to Recommendation 1: Concur. ICE's Office of Acquisition Management (OAQ) will review transportation services contracts to ensure



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

CORs are appropriately appointed in line with what has been determined to be high-risk, as defined by Attachment 3 of the Office of Management and Budget Memorandum, *Revisions to the Federal Acquisition Certification for Contracting Officer's Representatives (FAC-COR)*, dated September 6, 2011. Specifically, OAQ will confirm that each COR for transportation services contracts has a current certification level appropriate for the contract and tasks to be performed. OAQ will also assist programs under ICE Enforcement of Removal Operations (ERO) with nominating and maintaining COR support for applicable contracts. Estimated Completion Date (ECD): March 29, 2024.

OIG Analysis: We consider these actions responsive to the recommendation, which will remain open and resolved until ICE provides documentation that each COR for transportation services contracts has a certification level appropriate for the contract.

ICE Response to Recommendation 2: Concur. OAQ will ensure COs issue COR appointment letters to CORs who do not have them and reissue outdated COR appointment letters. Specifically, the OAQ Audit Liaison will work with each of the four OAQ operational division Section and Unit Chiefs to review their current contracts to ensure they have appointed CORs, in accordance with policy. ECD: March 29, 2024.

OIG Analysis: We consider these actions responsive to the recommendation, which will remain open and resolved until ICE provides documentation that each COR for transportation services contracts has an up-to-date COR appointment letter.

ICE Response to Recommendation 3: Concur. OAQ will send out written reminders that COs are to ensure they issue COR appointment letters and maintain these letters in contract files, as required by the DHS *Homeland Security Acquisition Manual (HSAM)*, dated October 2009, rev. July 31, 2023. As part of each contract award review, required by HSAM 3004.70, OAQ will ensure that COR appointment letters are issued. Additionally, OAQ will add this check for COR documentation to part of the *Quality Assurance Division Document Review Standards*, dated June 2023. ECD: March 29, 2024.

OIG Analysis: We consider these actions responsive to the recommendation, which will remain open and resolved until ICE provides a copy of its updated *Quality Assurance Division Document Review Standards* reflecting the proposed change.

ICE Response to Recommendation 4: Concur. OAQ will identify issues and/or concerns with draft QASPs as required for individual requirements and work with ERO to finalize draft QASPs. ECD: June 28, 2024.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis: We consider these actions responsive to the recommendation, which will remain open and resolved until ICE provides the guidance on QASP development and procedures to ensure CORs use them.

ICE Response to Recommendation 5: Concur. ICE ERO will conduct an evaluation of COR workload to determine if sufficient resources are allocated to adequately oversee contracts. If the evaluation determines there is an unequal distribution of work or insufficient resources, ICE ERO will create a plan to request additional resources, as appropriate. ECD: June 28, 2024.

OIG Analysis: We consider this action responsive to the recommendation, which will remain open and resolved until ICE provides documentation of its evaluation of COR workload.

ICE Response to Recommendation 6: Concur. On August 3, 2023, Contractor 2 made \$272,005 in invoice deductions to recover the government overpayment on this contract. ICE ERO will work with the COs to recover the remaining \$136,870 on Contracts 4 and 5 identified in our draft report. ECD: March 29, 2024.

OIG Analysis: We consider this action responsive to the recommendation, which will remain open and resolved until ICE provides documentation that accounts for the erroneous and unsupported charges.

ICE Response to Recommendation 7: Concur. ICE ERO will work with COs to conduct a review of standby bus charges, taking into account that the requirement for amount and frequency of standby bus charges relates to ICE ERO mission needs and is based on several unpredictable factors, including changing needs, timeline to acquire the necessary resources, and staffing resources. The COs will ensure a copy of ICE ERO's determination of reasonableness is included in the file as it relates to standby bus charges. ECD: March 29, 2024.

OIG Analysis: We consider this action responsive to the recommendation, which will remain open and resolved until ICE provides documentation of its review of standby bus charges.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Our audit objective was to determine to what extent ICE implemented controls to ensure its transportation services contractors adhere to the terms of their contracts, and whether ICE complied with Federal, departmental, and component procurement guidance and policy requirements for monitoring and overseeing the contracts.

To answer our audit objective, we researched and evaluated relevant criteria, guidance, processes, procedures, and controls related to how ICE manages and oversees its transportation contracts. We reviewed the following documents:

- FAR
- HSAM
- DHS Acquisition Workforce Policy 064-04-003
- DHS COR Guidebook

We conducted interviews in person and via video conferences with ICE personnel responsible for contract oversight and management. We conducted site visits to the ICE Field Office in San Antonio, Texas; ICE's Juvenile and Family Management Transportation and Compliance Unit in McAllen, Texas; and ICE Air Operations at Mesa, Arizona, to observe contract operations and to speak with CORs and ACORs. We also conducted a virtual site visit to the ICE Field Office in Los Angeles, California.

ICE provided a list of 11 transportation contracts that were active during our scope period of October 2019 through April 2022. We compared this list to active transportation contracts in the Federal Procurement Data System and found two additional contracts that were active during the scope period. Although active during the scope period, these two contracts were closed before our audit began. After reviewing the additional contract information, we determined that the 13 contracts represented the complete universe of ICE's active transportation services contracts within our scope. We also reviewed various attributes of these contracts, such as whether ICE appointed a COR at an appropriate level, whether ICE appointed the COR in writing via a COR appointment letter, and whether ICE developed a QASP to monitor the contract.

We judgmentally selected four transportation service contracts based on the type of services provided (i.e., ground, air, or combination of both) and obligated amounts for a more extensive review. We selected two ground contracts, one air contract, and one contract that provides both air and ground transportation. We reviewed supporting documentation for invoices submitted in April 2022 for the selected contracts. We expanded the invoice review on one contract to a portion of the February 2022 and March 2022 invoices to further analyze "standby" bus charges.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We relied on ICE's FFMS, the component's system of record, for obligations and expenditure data. We used total obligation and expenditures from ICE's FFMS for background purposes. We did not test the reliability of the total obligations and expenditures because the audit team relied on actual reviews of supporting documentation for reported invoices.

We assessed ICE's internal controls and compliance with laws and regulations applicable to its oversight of transportation services contracts. Our review was limited to addressing our audit objective and may not disclose all internal control deficiencies that may have existed at the time of this audit. However, our assessment disclosed deficiencies in ICE's design and implementation of controls to comply with Federal and departmental policies on COR appointment, contract monitoring, and invoice review.

We conducted this performance audit between April 2022 and June 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG's Access to DHS Information

During this audit, DHS provided timely responses to DHS OIG's requests for information and did not delay or deny access to information we requested.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix A
ICE Comments to the Draft Report

U.S. Department of Homeland Security
500 12th Street, S.W.
Washington, DC 20536



**U.S. Immigration
and Customs
Enforcement**

September 14, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Max Aguilar FOR **STEPHEN A LAURANCE III**
Chief Financial Officer (Acting) and Deputy Executive
Associate Director for Management and Administration
U.S. Immigration and Customs Enforcement

SUBJECT: Management Response to Draft Report: "ICE Should
Improve Controls Over Its Transportation Services Contracts"
(Project No. 22-037-AUD-ICE)

Digitally signed by
STEPHEN A. LAURANCE III
Date: 2023.09.14 16:02:12
-04'00'

Thank you for the opportunity to comment on this draft report. The U.S. Immigration and Customs Enforcement (ICE) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

ICE leadership is pleased to note OIG's recognition that ICE enforces the nation's immigration laws and manages the safe and secure transportation of apprehended noncitizens for removal, and that from October 2019 through April 2022, ICE obligated \$799 million across 13 contracts for transportation of noncitizens. However, it is also important to note that—since fiscal year (FY) 2021—ICE Management and Administration's Office of Acquisition Management (OAQ) also increased its training and support of Contracting Officer Representatives (CORs). Examples include:

- 1) Beginning in FY 2023, OAQ led an ongoing effort to complete an overhaul and consolidation of COR community resources on ICE's internal SharePoint page (inSight) to provide all ICE employees access to policy, trainings, templates, samples, etc.;
- 2) OAQ, in conjunction with ICE Enforcement and Removal Operations (ERO), led multiple COR-specific trainings from March 2023 to April 2023 on topics such as market research, COR financial matters, COR basics training, COR planning trainings, and an open forum for CORs with Contracting Officers (COs) and Contract Specialists;



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- 3) In March and June 2021, OAQ co-hosted COR-specific training on how to properly maintain files and support all contracts;
- 4) OAQ's Acquisition Innovation Advocate and policy team led several trainings from April 2021 (Procurement Innovation at the Office of the Chief Information Officer) to June 2023 (Market Research) for program personnel in support of ICE contracts on how to better support all contracts; and
- 5) In April 2023, OAQ created an internal SharePoint site, at the request of CORs, titled "ICE Acquisition Community Forum," to provide a place for CORs to ask any acquisition questions they have and to seek additional support.

In accordance with the Department of Homeland Security (DHS) mission and core values, ICE remains committed to improving overall business performance including providing a strategic approach to procurement that complies with federal and departmental standards and requirements for contracts. ICE maintains the highest ethical and professional standards and will continue to improve the quality of our work in service of the DHS mission.

The draft report contained seven recommendations with which ICE concurs. Enclosed find our detailed response to each recommendation. ICE previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration.

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

Enclosure



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Enclosure: Management Response to Recommendations Contained in OIG (22-037-AUD-ICE)

OIG recommended that the ICE Executive Associate Director for Management and Administration:

Recommendation 1: Ensure COs appoint appropriately certified CORs to oversee high-risk transportation services contracts.

Response: Concur. ICE OAQ will review transportation services contracts to ensure CORs are appropriately appointed in line with what has been determined to be high-risk, as defined by Attachment 3 of the Office of Management and Budget Memorandum, "Revisions to the Federal Acquisition Certification for Contracting Officer's Representatives (FAC-COR)," dated September 6, 2011.¹ Specifically, OAQ will confirm that each COR for transportation services contracts has a current certification level appropriate for the contract and tasks to be performed. OAQ will also assist programs under ICE ERO with nominating and maintaining COR support for applicable contracts. Estimated Completion Date (ECD): March 29, 2024.

Recommendation 2: Ensure COs issue COR appointment letters to CORs who do not have them and reissue outdated COR appointment letters.

Response: Concur. OAQ will ensure COs issue COR appointment letters to CORs who do not have them and reissue outdated COR appointment letters. Specifically, the OAQ Audit Liaison will work with each of the four OAQ operational division Section and Unit Chiefs to review their current contracts to ensure they have appointed CORs, in accordance with policy. ECD: March 29, 2024.

Recommendation 3: Develop and implement procedures to ensure contracting staff issue COR appointment letters and maintain them in contract files.

Response: Concur. ICE OAQ will send out written reminders that COs are to ensure they issue COR appointment letters and maintain these letters in contract files, as required by the DHS "Homeland Security Acquisition Manual" (HSAM), dated October 2009, rev. July 31, 2023.² As part of each contract award review, required by HSAM 3004.70, OAQ will ensure that COR appointment letters are issued. Additionally, OAQ will add this check for COR documentation to part of the "Quality Assurance Division Document Review Standards," dated June 2023. ECD: March 29, 2024.

¹ https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/procurement/revisions-to-the-federal-acquisition-certification-for-contracting-officers-representatives.pdf

² https://www.dhs.gov/sites/default/files/2023-08/homeland-security-acquisition-manual-full-0727_0.pdf



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG recommended that the Executive Associate Director for ERO:

Recommendation 4: Develop and implement guidance to ensure that ERO develops QASPs [Quality Assurance Surveillance Plans] for contracts that include specific methods for monitoring contractor compliance with contract terms/conditions and develop procedures to ensure CORs use the QASPs as part of their oversight activities.

Response: Concur. In consultation with OAQ, ERO will submit draft QASPs for review and approval as part of a complete requirements package. OAQ will identify any issues or concerns with draft QASPs as required for individual requirements and work with ERO to finalize draft QASPs. ECD: June 28, 2024.

OIG recommended that the ICE Executive Associate Directors for ERO and Management and Administration:

Recommendation 5: Evaluate the workload for CORs and determine if sufficient resources are allocated to adequately oversee contracts and, based on the evaluation, develop, and implement a plan to more effectively manage or obtain additional personnel resources.

Response: Concur. ICE ERO will conduct an evaluation of COR workload to determine if sufficient resources are allocated to adequately oversee contracts. If the evaluation determines there is an unequal distribution of work or insufficient resources, ERO will create a plan to request additional resources, as appropriate. ECD: June 28, 2024.

OIG recommended that the Executive Associate Director for Management and Administration:

Recommendation 6: Recover any monies, including the \$408,875 identified in this report, determined to have been paid toward inaccurate charges or costs not supported by documentation.

Response: Concur. On August 3, 2023, Contractor 2 made \$272,005 in invoice deductions to recover the government overpayment on this contract. ICE ERO will work with the COs to recover the remaining \$136,870 on Contracts 4 and 5 identified in the OIG's draft report. ECD: March 29, 2024.

OIG recommended that the Executive Associate Directors for ERO and Management and Administration:

Recommendation 7: Determine the reasonableness of the amount and frequency of standby bus charges.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response: Concur. ICE ERO will work with COs to conduct a review of standby bus charges, taking into account that the requirement for amount and frequency of standby bus charges relates to ERO mission needs and is based on several unpredictable factors, including changing needs, timeline to acquire the necessary resources, and staffing resources. The COs will ensure a copy of ERO's determination of reasonableness is included in the file as it relates to standby bus charges. ECD: March 29, 2024.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix B

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
ICE Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

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

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



OIG Hotline

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

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



October 2023

FEDERAL CONTRACTING

Agencies Can Better Monitor E-Verify Compliance

GAO Highlights

Highlights of [GAO-24-106219](#), a report to congressional requesters

Why GAO Did This Study

Since 2009, a clause in certain federal contracts requires contractors to use the E-Verify program to confirm their workers' employment eligibility. As of 2023, about 95,000 federal contractors were enrolled in E-Verify. Agencies have obligated hundreds of billions of dollars on contracts that appeared subject to the requirement.

GAO was asked to assess federal agencies' use of the E-Verify clause for federal contractors. This report focuses on the extent to which DOD, DHS, and HHS included the clause in selected contracts and monitored contractor compliance with the clause. It also addresses whether USCIS has taken action when contractors did not follow E-Verify program requirements.

GAO selected the three agencies because they accounted for nearly two-thirds of fiscal year 2021 contract awards that appeared subject to the E-Verify clause, the most recent data available at the time of GAO's review. GAO reviewed fiscal years 2019–2021 contract data, assessed a nongeneralizable sample of 24 contracts, and analyzed data on contractor E-Verify enrollment.

What GAO Recommends

GAO is making eight recommendations, including that OMB clarify agency responsibilities for monitoring contractor compliance with the E-Verify clause, and that DHS implement a process to refer contractors with terminated accounts to appropriate agency officials. DOD, DHS, HHS, and OMB concurred with the recommendations.

View [GAO-24-106219](#). For more information, contact Timothy J. DiNapoli at (202) 512-4841 or tinapolit@gao.gov, or Rebecca Gambler at (202) 512-8777 or gablerr@gao.gov.

October 2023

FEDERAL CONTRACTING

Agencies Can Better Monitor E-Verify Compliance

What GAO Found

The E-Verify program allows employers to electronically confirm that their employees are eligible to work in the U.S. The Federal Acquisition Regulation (FAR) requires agencies to include, with certain exceptions, a contract clause directing contractors to enroll in and use the program. The Departments of Defense (DOD), Homeland Security (DHS), and Health and Human Services (HHS) included the clause in 22 of the 24 contracts that GAO reviewed.

However, the three selected agencies' efforts to monitor contractor compliance with the E-Verify clause were inconsistent. Some officials thought they were not responsible for monitoring contractor compliance. The Office of Management and Budget (OMB) office that directs federal procurement policy told GAO that it expects agencies to monitor contractor E-Verify compliance. However, OMB has not clearly communicated this expectation to agencies.

E-Verify Participation Poster



Source: GAO (photo). | GAO-24-106219

U.S. Citizenship and Immigration Services (USCIS)—a component of DHS—administers E-Verify. USCIS may terminate E-Verify accounts, including those of federal contractors, for misuse and non-use. Misuse includes unresolved discrepancies that prevent confirmation of an employee's eligibility. Non-use includes not verifying any employees in a specified time frame. From 2020 to March 2023, USCIS terminated almost 300 contractor accounts for misuse and more than 5,000 such accounts for non-use. USCIS no longer terminates contractor accounts for non-use.

However, USCIS lacks a process to refer these contractors for further review, as required. The FAR states that DHS must refer contractors whose E-Verify accounts it terminates to suspension and debarment officials who determine whether contractors should be temporarily disqualified or excluded from government contracting. DHS officials acknowledged USCIS—the component responsible for these referrals—is not meeting this requirement. Agencies' suspension and debarment officials, therefore, are not able to determine whether these federal contractors' misuse of E-Verify merits further action. DHS officials said they plan to address this, but these plans are in the early stages.

Contents

Letter		1
	Background	4
	Agencies Included the E-Verify Clause in Most Selected Contracts, but Did Not Accurately Report It in FPDS	11
	Selected Agencies Varied in Monitoring Contractor E-Verify Compliance and Lack Data from USCIS for This Duty	18
	USCIS Terminated Federal Contractor Accounts without a Process to Refer Them to Suspension and Debarment Officials	26
	Conclusions	32
	Recommendations for Executive Action	33
	Agency Comments and Our Evaluation	34
Appendix I	Objectives, Scope, and Methodology	36
Appendix II	Comments from the Department of Defense	43
Appendix III	Comments from the Department of Homeland Security	45
Appendix IV	Comments from the Department of Health and Human Services	50
Appendix V	GAO Contacts and Staff Acknowledgments	52
Table		
	Table 1: Number of Selected Contracts Containing the E-Verify Clause	11
Figures		
	Figure 1: Roles and Responsibilities Related to Federal Contractor Use of E-Verify	10
	Figure 2: Evolution of E-Verify Dollar and Simplified Acquisition Thresholds	13

Figure 3: Contracting Officials' Reported Monitoring of Contractor Compliance with the E-Verify Clause for 24 Contracts GAO Reviewed	19
Figure 4: Federal Contractor E-Verify Accounts Terminated for Misuse and Non-use as of March 31, 2023	28
Figure 5: USCIS E-Verify Website Screenshot of How to Find Participating Employers, Taken May 25, 2023	30

Abbreviations

COTS	commercially available off-the-shelf
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DOD	Department of Defense
FAR	Federal Acquisition Regulation
FPDS	Federal Procurement Data System
HHS	Department of Health and Human Services
MOU	memorandum of understanding
OMB	Office of Management and Budget
USCIS	U.S. Citizenship and Immigration Services

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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.



October 3, 2023

The Honorable Chuck Grassley
Ranking Member
Committee on the Budget
United States Senate

The Honorable James Lankford
Ranking Member
Subcommittee on Government Operations and Border Management
Committee on Homeland Security and Governmental Affairs
United States Senate

Each year, federal agencies obligate hundreds of billions of dollars on federal contracts. Federal law generally prohibits employment of noncitizens who are not authorized to work in the U.S., and requires employers, including federal contractors, to take certain steps to verify that employees are not unauthorized workers.¹ U.S. Citizenship and Immigration Services' (USCIS) E-Verify program allows employers to electronically confirm the employment eligibility of their employees. According to USCIS, more than 1 million employers had enrolled in E-Verify as of May 2023, including about 95,000 federal contractors. The Federal Acquisition Regulation (FAR) requires federal agencies to include a clause directing federal contractors to use E-Verify in all contracts that exceed \$150,000, unless certain exceptions apply. In fiscal year 2021, agencies awarded approximately 74,000 contracts and orders with obligations totaling approximately \$185 billion that appeared to meet the FAR's requirement for inclusion of the E-Verify clause based on federal

¹The statute uses the term "unauthorized alien" to refer to an individual of non-U.S. nationality (i.e., foreign national or noncitizen) who is not work authorized through lawful permanent resident status, or otherwise by statute or by the Secretary of Homeland Security. 8 U.S.C. § 1324a(h)(3). The Immigration Reform and Control Act of 1986, among other things, made it unlawful for U.S. entities to knowingly hire, recruit or refer for a fee, or continue to employ noncitizens who are not authorized to work in the U.S. Additionally, employers are to comply with the employment verification system requirements in order to confirm the employment eligibility of, and conduct identity verification for, their workers. Section 274A of the Immigration and Nationality Act, Pub. L. No. 82-414, title II, ch. 8, § 274A, 66 Stat. 163 (1952), as added by Pub. L. No. 99-603, title I, subtitle A, § 101(a), 100 Stat. 3359, 3360-3372 (classified, as amended, at 8 U.S.C. § 1324a).

procurement data.² USCIS administers E-Verify and can take administrative actions when companies do not follow program requirements.

You asked us to assess federal agencies' use of the E-Verify clause for federal contractors. This report addresses the extent to which (1) selected federal agencies ensured the E-Verify clause was included in selected contracts and reported that information in the Federal Procurement Data System (FPDS); (2) selected federal agencies monitored federal contractor compliance with the E-Verify clause; and (3) USCIS has taken administrative actions against federal contractors that did not comply with E-Verify program requirements.

To answer our objectives, we selected the Departments of Defense (DOD), Homeland Security (DHS), and Health and Human Services (HHS) for review. We selected these three because, from fiscal years 2019 to 2021, they were among the federal agencies with the highest number of contracts and associated obligations that appeared to be subject to the FAR's requirement for inclusion of the E-Verify clause. Collectively, these three agencies accounted for nearly two-thirds of all new awards in fiscal year 2021 that appeared to be subject to the FAR's E-Verify requirement. We used the same criteria to select two components from each agency: the Defense Logistics Agency (DLA) and the Navy at DOD, the Federal Emergency Management Agency and the U.S. Coast Guard at DHS, and the Centers for Disease Control and Prevention and the National Institutes of Health at HHS.

Within the selected components, we selected a nongeneralizable sample of 24 contracts and orders that appeared to be subject to the requirement for including the E-Verify clause in the contract and that were awarded in

²The E-Verify clause is titled Employment Eligibility Verification in the FAR, but for the purposes of this report we refer to it as the E-Verify clause. The FAR generally requires contracting officers to include the E-Verify clause in contracts that exceed \$150,000 unless the contract: (1) has a period of performance of less than 120 days; (2) is only for work performed outside the U.S.; or (3) is only for commercially available off-the-shelf items (COTS) or commercial services that are part of the purchase of a COTS item. For a full description of the exceptions, see FAR 22.1803. To determine which contracts appeared to be subject to the requirement, our analysis therefore included contracts that exceeded \$150,000, had a period of performance of at least 120 days, were for work primarily performed within the U.S., and were not COTS items. Some contracts we excluded may require the E-Verify clause, such as contracts using simplified acquisition procedures. Some of the contracts included in our analysis may not meet the criteria for inclusion of the E-Verify clause, such as contracts for the purchase of commercial services that are part of the purchase of a COTS item.

fiscal year 2021—the most recent year for which we had full-year data available when we began our review.³ Hereafter, we refer to these contracts and orders collectively as contracts, unless otherwise specified. We selected four contracts from each component—randomly selecting two in which FPDS data indicated the E-Verify clause was included in the contract and two where the data indicated the clause was not present—for a total of eight contracts for each agency. We also randomly selected six subcontracts from our sample of 24 prime contracts—one from each component—to determine whether the prime contractors included the E-Verify clause in their subcontracts.⁴ We also interviewed representatives of six prime contractors to confirm whether they included the E-Verify clause in selected subcontracts and to determine their processes for including the E-Verify clause in applicable subcontracts.

To assess the extent to which selected federal agencies ensured the E-Verify clause was included in contracts when required and accurately reported that information in FPDS for our sample of contracts, we reviewed contract file documents and FPDS data for the selected contracts and subcontracts. We interviewed agency contracting officials responsible for the selected contracts, including 24 contracting officers. Additionally, we interviewed General Services Administration officials responsible for administering FPDS to determine when the inclusion of the E-Verify clause in a contract should be reported within the system.

To address federal monitoring of contractor compliance (E-Verify enrollment and use) and USCIS actions for noncompliance, we reviewed the FAR and selected agency guidance relating to E-Verify. We analyzed USCIS data on selected contractors' enrollment and use of E-Verify. We also analyzed USCIS data on federal contractor E-Verify account terminations for fiscal years 2009—when the FAR was amended to require federal contractors to use E-Verify under certain federal contracts—to March 2023. We assessed USCIS's efforts to provide

³Our selection methodology included both contracts and orders placed under indefinite-delivery contracts. Indefinite-delivery contracts may be used when the exact times and/or exact quantities of required products or services are not known at the time of award. An indefinite-delivery contract provides for the issuance of orders, which are used to procure specific products or services during the period of the contract.

⁴A prime contractor is the entity with which the federal government has entered into a contract. A subcontractor is a supplier, distributor, or vendor that furnishes supplies or services for the performance of a prime contract or a subcontract. The FAR generally requires that when the E-Verify clause is included in a prime contract, the prime contractor must include the requirements of the clause in subcontracts valued above \$3,500 for services or construction to be performed in the U.S. FAR 22.1802(b)(4), 52.222-54(e).

agencies with tools and information on contractor participation in E-Verify. We also assessed USCIS's actions for noncompliance, including account terminations and referrals related to such terminations.⁵ We also interviewed agency suspension and debarment officials; USCIS officials with E-Verify-related responsibilities; and Office of Management and Budget (OMB), Office of Federal Procurement Policy staff responsible for federal procurement policy about agency roles and responsibilities related to federal contractor use of E-Verify.⁶ See appendix I for additional details about our objectives, scope, and methodology.

We conducted this performance audit from August 2022 to October 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

E-Verify Legislative and Regulatory History

The Immigration Reform and Control Act of 1986 made it unlawful for employers to knowingly hire, recruit or refer for a fee, or continue to employ noncitizens who are not authorized to work in the U.S.; and required employers to verify employees' work authorization. The employment eligibility verification process—the Form I-9 process—requires employers to review documents presented by new employees to establish their identity and employment eligibility.⁷ The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 created pilot programs,

⁵FAR 22.1802(e) states that DHS and the Social Security Administration may terminate a contractor's memorandum of understanding (MOU) and deny access to the E-Verify system in accordance with the terms of the MOU. FAR 22.1802(e) further states that if DHS or the Social Security Administration terminates a contractor's MOU, the terminating agency must refer the contractor to a suspension or debarment official for possible suspension or debarment action. USCIS officials told us that sometime between 2007 and 2013, the Social Security Administration asked to be removed from the E-Verify MOU, and DHS agreed to do so. Thus, at present, the Social Security Administration takes no actions related to FAR 22.1802(e). The Social Security Administration still plays a role in resolving issues related to the accuracy of employee-submitted data.

⁶Throughout this report we refer to OMB and the Office of Federal Procurement Policy collectively as OMB.

⁷Section 274A of the Immigration and Nationality Act, Pub. L. No. 82-414, title II, ch. 8, § 274A, 66 Stat. 163 (1952), as added by Pub. L. No. 99-603, title I, subtitle A, § 101(a), 100 Stat. 3359, 3360-3372 (classified, as amended, at 8 U.S.C. § 1324a).

including the Basic Pilot Program that later became the E-Verify program, for employment eligibility confirmation.⁸ USCIS administers the E-Verify program. E-Verify is a largely voluntary program for most employers. However, executive departments and agencies are required to use it by OMB directive, and certain federal contractors are required to use it by regulation, as a condition of their contracts.⁹

In 2009, the FAR was amended to require that federal contractors use E-Verify to electronically verify the employment eligibility of employees working under certain federal contracts. Specifically, the FAR generally requires contracting officers to include the E-Verify clause in all solicitations and contracts that exceed \$150,000 unless the contract:

- has a period of performance of less than 120 days;
- is only for work performed outside the U.S.; or

⁸Pub. L. No. 104-208, div. C, title IV, subtitle A, §§ 401-405, 110 Stat. 3009, 3009-655 to 3009-666 (classified, as amended, at 8 U.S.C. § 1324a note). The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 created employment eligibility confirmation pilot programs that were to terminate 4 years after going into effect, unless Congress provided otherwise. Under the Basic Pilot Program and now the E-Verify Program, a person or other entity that elects to participate agrees to conform to certain procedures in the case of the hiring (or recruitment or referral) for employment in the U.S. of each covered individual, to include obtaining from the individual (and the individual shall provide) and recording on the I-9 or similar form the individual's social security number (if he or she has one), and if the individual does not attest to U.S. citizenship under the Immigration and Nationality Act § 274A(b)(2), such identification or authorization number as the Secretary of Homeland Security shall specify, and retaining the original and making it available for inspection for the specified period and in the manner required of I-9 forms under Immigration and Nationality Act § 274A(b)(3). See 8 U.S.C. § 1324a note. The Basic Pilot Program was first extended in 2002 by the Basic Pilot Extension Act of 2001. The E-Verify program was most recently extended until September 2023. Pub. L. No. 107-128, 115 Stat. 2407 (2002); Consolidated Appropriations Act, 2023, Pub. L. No. 117-328, Div. O, title III, § 301, 136 Stat. 4459, 5227 (2022).

⁹Pursuant to a 2007 OMB directive, all federal departments and agencies are to verify their new hires through E-Verify. Stephen S. McMillin, Acting Dir., Office of Mgmt. & Budget, *Memorandum for the Heads of Departments and Agencies: Verifying the Employment Eligibility of Federal Employees*, M-07-21 (Aug. 10, 2007). For statutory background, see 8 U.S.C. § 1324a note, as amended (in particular, section 402(e) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996). Pursuant to policies and procedures in FAR subpart 22.18, federal contractors must use E-Verify to electronically verify the employment eligibility of employees working under certain federal contracts. In addition, we previously reported that a number of states enacted laws or issued executive orders mandating that some or all employers within the state use E-Verify to verify the employment eligibility of new hires as a condition of business licensing or contracting in that state. See GAO, *Employment Verification: Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, [GAO-11-146](#) (Washington, D.C.: Dec. 17, 2010).

-
- is only for commercially available off-the-shelf (COTS) items or commercial services that are part of the purchase of a COTS item.¹⁰

The E-Verify clause generally requires that federal contractors enroll in the program and use it to verify the employment eligibility of new employees and employees assigned to the contract within certain time frames. The clause also requires federal prime contractors to include the E-Verify clause in certain subcontracts.¹¹ The E-Verify clause does not require federal contractors to verify the employment eligibility of certain previously verified individuals, such as employees who have specified security clearances or credentials.¹²

In 2018, the General Services Administration (which manages FPDS) added the Employment Eligibility Verification option within the “Additional Reporting” data field within FPDS to indicate if a contract contains the E-Verify clause. According to FPDS guidance, agencies are to report the applicable response to this data field for all contracts awarded on or after July 11, 2018.

USCIS Roles and Responsibilities Related to Federal Contractor Use of E-Verify

Federal contractors and other employers sign an E-Verify memorandum of understanding (MOU) with DHS to participate in the program. USCIS’s Immigration Records and Identity Services Directorate is responsible for ensuring employers comply with the terms outlined in the MOU. For federal contractors, the E-Verify MOU establishes that (1) compliance with the MOU is a performance requirement under the terms of the federal contract or subcontract; and (2) termination of the MOU may negatively affect the contractor’s performance of contractual responsibilities.

USCIS maintains data on employers’ enrollment and use of the E-Verify system, including their status as federal contractors. When employers

¹⁰For a full description of the exceptions, see FAR 22.1803.

¹¹Specifically, the E-Verify clause requires the prime contractor to include the requirements of the E-Verify clause in each subcontract that is for services (except for commercial services that are part of the purchase of a COTS item, performed by the COTS provider, and are normally provided for that COTS item) or construction, and that has (1) a value of more than \$3,500 and (2) includes work performed in the U.S. FAR 52.222-54(e).

¹²The E-Verify clause states that the contractor is not required to use E-Verify for any employee: (1) whose employment eligibility the contractor previously verified through E-Verify; (2) who holds an active U.S. government security clearance; or (3) who has credentials pursuant to Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors. FAR 52.222-42(d).

enroll in E-Verify, they must self-identify whether they are a federal contractor and indicate whether they have a contract that contains the FAR E-Verify clause. USCIS creates resources, such as an enrollment guide, to help federal contractors and other users understand their E-Verify-related responsibilities to enroll in and use the E-Verify system. USCIS also provides resources and data to federal contracting officials to help them monitor contractor compliance with the E-Verify clause.

USCIS can take several administrative actions if an employer, including a federal contractor, does not comply with the terms of its E-Verify MOU. For example, USCIS can email employers to remind them of their responsibilities, request to review their hiring documentation, refer the employer to law enforcement agencies such as U.S. Immigration and Customs Enforcement, or terminate the employer's E-Verify account.¹³ USCIS officials stated that they can terminate an E-Verify account upon an employer's request for administrative reasons, such as company mergers. USCIS may also terminate an employer's E-Verify account for non-use and misuse of the E-Verify system—violations of the MOU's terms.

- **Non-use termination.** USCIS's termination guidance defines non-use as when an enrolled employer never uses the system to verify employees, creates additional accounts it does not use, or stops verifying employees for an extended period after initial use. According to USCIS procedures, it may terminate accounts for employers that have not verified any employees or updated their account information for 3 years.¹⁴

¹³According to USCIS officials, in these circumstances, USCIS terminates the MOU and removes the employer's access to its E-Verify account. Throughout this report, we refer to this as terminating the account or terminating the MOU based on USCIS documentation and interviews.

¹⁴We discuss the implications of non-use terminations as they pertain to federal contractors later in this report.

Unresolved tentative nonconfirmations.

A tentative nonconfirmation occurs when E-Verify is initially unable to confirm an employee's eligibility to work in the U.S. Employers are required to inform the employee of the tentative nonconfirmation and the employee's right to take action to resolve it. If an employee decides to take action to resolve it, the employer must electronically refer the tentative nonconfirmation case in E-Verify to either the Social Security Administration, the Department of Homeland Security, or both. If an employee decides not to take action to resolve the tentative nonconfirmation, the employer must close the case in the E-Verify system. The U.S. Citizenship and Immigration Services (USCIS) considers a tentative nonconfirmation to be unresolved when an employer fails to refer or close a tentative nonconfirmation within 10 government business days.

Source: GAO analysis of USCIS E-Verify documentation. | GAO-24-106219

- **Misuse termination.** USCIS's termination guidance defines misuse as when an employer fails to comply with E-Verify procedures in the MOU or has not cooperated with USCIS. Examples of termination for misuse include evidence of discrimination, failure to protect employee personally identifiable information, and unresolved tentative nonconfirmations.

As part of its account termination procedures, USCIS provides employers with a 30-day notice of intent to terminate that provides the basis for the termination and instructions for how to prevent it. The FAR requires that if DHS terminates a federal contractor's MOU, it must refer that contractor to a suspension or debarment official for possible suspension or debarment action.¹⁵ This referral process is addressed in more detail below.

Federal Agency Roles and Responsibilities Related to Federal Contractor Use of E-Verify

Within the agencies we selected for review, department-level procurement policy is set by DHS's Office of the Chief Procurement Officer, DOD's Office of Defense Pricing and Contracting, and HHS's Office of Acquisitions. Individual components within each agency also have offices responsible for component-level contracting policy. Finally, each component has multiple contracting offices, led by an office chief (or similar role) overseeing contracting staff. Agency contracting officers are

¹⁵FAR 22.1802(e) states, "DHS and the Social Security Administration may terminate a contractor's Memorandum of Understanding (MOU) and deny access to the E-Verify system in accordance with the terms of the MOU. If DHS or the Social Security Administration terminates a contractor's MOU, the terminating agency must refer the contractor to a suspension or debarment official for possible suspension or debarment action. During the period between termination of the MOU and a decision by the suspension or debarment official whether to suspend or debar, the contractor is excused from its obligations under paragraph (b) of the clause at 52.222-54. If the contractor is suspended or debarred as a result of the MOU termination, the contractor is not eligible to participate in E-Verify during the period of its suspension or debarment. If the suspension or debarment official determines not to suspend or debar the contractor, then the contractor must reenroll in E-Verify." As noted above, according to USCIS, the Social Security Administration asked to be removed from the E-Verify MOU and DHS agreed to do so. Thus, at present, the Social Security Administration takes no actions related to FAR 22.1802(e). The Social Security Administration still plays a role in resolving issues related to the accuracy of employee-submitted data.

generally responsible for ensuring that contractors comply with the terms of the contract, such as the E-Verify clause.

As discussed above, if DHS terminates a contractor's MOU, DHS must refer the contractor to an agency suspension or debarment official for a possible suspension or debarment action.

- **Suspension** temporarily disqualifies a contractor from government contracting and government-approved subcontracting pending the completion of an investigation or legal proceeding.
- **Debarment** excludes a contractor from government contracting and government-approved subcontracting for a reasonable, specified period of time—generally no more than 3 years.

Under the FAR, agencies are to establish procedures for suspension and debarment referrals.¹⁶ According to the Interagency Suspension and Debarment Committee, a suspension and debarment referral is a written request, supported by documentary evidence, and presented to the agency suspension and debarment official for consideration. Upon receiving a referral, agency suspension and debarment officials are responsible for deciding whether it is in the government's or the public's interest to suspend or debar federal contractors for certain causes, using procedures in the FAR.¹⁷ When more than one agency has an interest in the suspension or debarment of a contractor, the Interagency Suspension and Debarment Committee resolves the lead agency issue and coordinates the resolution among all interested agencies prior to the initiation of any suspension, debarment, or related action.¹⁸

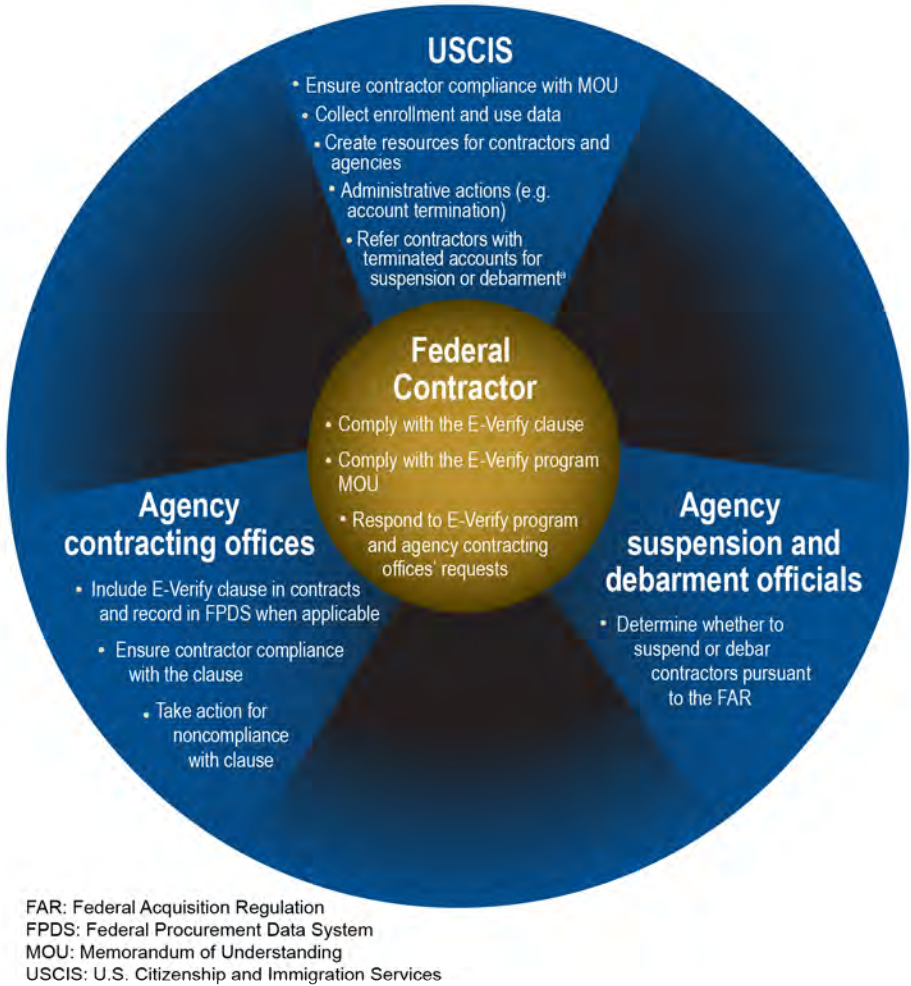
¹⁶FAR 9.406-3(a); FAR 9.407-3(a).

¹⁷See FAR subpart 9.4. We have reported on a variety of issues involving suspensions and debarments under the FAR. See GAO, *Federal Contracts and Grants: Agencies Have Taken Steps to Improve Suspension and Debarment Programs*, [GAO-14-513](#) (Washington, D.C.: May 21, 2014); and *Suspension and Debarment: Characteristics of Active Agency Programs and Governmentwide Oversight Efforts*, [GAO-13-707T](#) (Washington, D.C.: June 12, 2013).

¹⁸FAR 9.402(d). The Interagency Suspension and Debarment Committee is an interagency body created by Executive Order 12,549, 51 Fed. Reg. 6,370 (Feb. 18, 1986), consisting chiefly of representatives from executive branch organizations that work together to provide support for suspension and debarment programs throughout the government. The committee reports to Congress annually on the status of the federal suspension and debarment system, pursuant to section 873 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009. Pub. L. No. 110-417, § 873(a)(7) (2008) (codified as amended at 31 U.S.C. § 6101 note).

Figure 1 illustrates the roles and responsibilities of USCIS, agencies' contracting and suspension and debarment officials, and federal contractors related to the use of E-Verify.

Figure 1: Roles and Responsibilities Related to Federal Contractor Use of E-Verify



Source: GAO analysis of USCIS and FAR documents. | GAO-24-106219

^aFAR 22.1802(e) establishes that if DHS terminates a federal contractor's E-Verify MOU, DHS must refer the federal contractor to a suspension or debarment official for a possible suspension or debarment action. USCIS lists on its website those federal contractors whose E-Verify MOUs have been terminated.

Agencies Included the E-Verify Clause in Most Selected Contracts, but Did Not Accurately Report It in FPDS

DOD, DHS, and HHS contracting officials generally included, when required, the E-Verify clause in selected contracts. At the component level, DLA contracting officials did not consistently do so but took steps to address the factors that contributed to omission of the clause during our review. Contracting officials from the three agencies, however, did not always report the E-Verify clause’s presence in FPDS as instructed by FPDS guidance and cited several factors contributing to this inconsistency. Based on fiscal year 2021 data, we also identified potential accuracy issues government-wide with the FPDS field that reflects the presence of the E-Verify clause.

Selected Agencies Included the E-Verify Clause in Most Contracts in Our Sample

Contracting officials at the agencies we reviewed—DOD, DHS, and HHS—included the E-Verify clause in 22 out of 24 contracts in our sample (see table 1). For the six subcontracts included in our review, we found that prime contractors inserted the E-Verify clause in five of them.¹⁹

Table 1: Number of Selected Contracts Containing the E-Verify Clause

Agency	Number of selected contracts with the E-Verify clause	Total number of selected contracts that should have included the E-Verify clause
Department of Defense (DOD)	6	8
Department of Homeland Security (DHS)	8	8
Department of Health and Human Services (HHS)	8	8
Total	22	24

Source: GAO analysis of DOD, DHS, and HHS contract files and interviews with contracting officials. | GAO-24-106219

Note: Our sample selection included both definitive contracts and orders placed under indefinite-delivery contracts. For the purposes of the analysis, if we selected an order under an indefinite-delivery contract, and if the indefinite-delivery contract included the E-Verify clause and indicated that orders under the contract were subject to the terms and conditions of the contract, we considered the E-Verify clause to be included in the order. Indefinite-delivery contracts may be used when the exact times and/or exact quantities of required products or services are not known at the time of award. An indefinite-delivery contract provides for the issuance of orders, which are used to procure specific products or services during the period of the contract.

Contracting officials at the agencies we reviewed relied on a variety of resources to determine whether to include the E-Verify clause in applicable contracts. They stated that they generally relied on the FAR to

¹⁹We asked the contractor for the remaining subcontract why it did not include the E-Verify clause in the subcontract. Contractor representatives told us that they generally include the E-Verify clause in their subcontracts, but did not include it in the one in our sample because it was an independent consultant agreement. The agreement’s period of performance of about 9 months ended in September 2022.

make this decision. The FAR requires inclusion of the E-Verify clause in all contracts that exceed \$150,000, with certain exceptions as discussed above.²⁰ Contracting officials also highlighted other resources:

- **DHS E-Verify job aid and related guidance.** Contracting officials at three of the six components we reviewed noted that they use DHS's E-Verify job aid, which includes detailed instructions on when to include the E-Verify clause in contracts in accordance with the FAR. DHS emailed the federal contracting community in October 2019 with guidance on ensuring contractor compliance with E-Verify requirements and subsequently issued the job aid in March 2021. Officials at the two HHS components we reviewed—Centers for Disease Control and Prevention and the National Institutes of Health—stated that they also refer to an HHS acquisition policy reminder, which they said was based on DHS's E-Verify guidance.
- **Contract clause matrixes.** Contracting officials at the Coast Guard, DLA, and the Navy said that their agencies use component-specific contract clause matrixes—a list of clauses that may be required in the contract—for E-Verify guidance. For example, the Navy and Coast Guard use contract clause matrixes that contain a list of potentially applicable clauses based on certain contract parameters. According to Navy and Coast Guard officials, these matrixes help contracting officials select all applicable contract clauses, including the E-Verify clause.
- **Electronic contract writing systems.** Contracting officials at five components said that they rely on electronic contract writing systems to prompt them to include the E-Verify clause in applicable federal contracts.
- **Pre-award reviews.** Contracting officials at five components told us they rely on supervising procurement officials to conduct pre-award reviews to ensure that contracts include all applicable contract clauses, including the E-Verify clause.

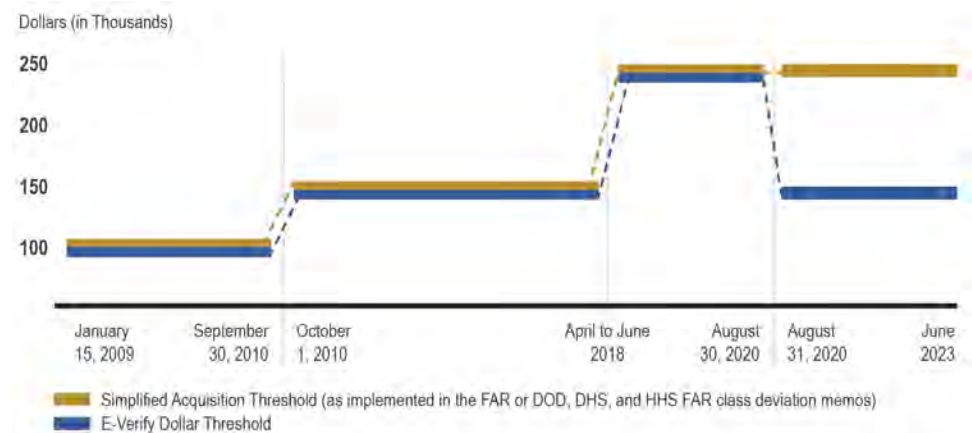
In contrast to the other components, DLA contracting officials did not include the E-Verify clause in two of the four contracts we reviewed that were awarded in 2021. They attributed these omissions to confusion about the relationship between the E-Verify dollar threshold and the simplified acquisition threshold.²¹ The two thresholds were set at the

²⁰FAR 22.1803.

²¹For purchases at or below the simplified acquisition threshold, agencies may use streamlined procurement procedures, called simplified acquisition procedures.

same dollar amount until August 2020, when the FAR was revised to implement an increase to the simplified acquisition threshold under the National Defense Authorization Act for Fiscal Year 2018 (see fig. 2).²²

Figure 2: Evolution of E-Verify Dollar and Simplified Acquisition Thresholds



Source: GAO analysis of Federal Acquisition Regulation (FAR) documents and Department of Defense (DOD), Department of Homeland Security (DHS), and Department of Health and Human Services (HHS) FAR class deviation memos. | GAO-24-106219

Note: The National Defense Authorization Act of Fiscal Year 2018 increased the simplified acquisition threshold to \$250,000, but the increase was not implemented in the FAR—and the dollar threshold for the E-Verify clause was not separated from the simplified acquisition threshold—until August 31, 2020. In the interim, individual agencies implemented the statutory increase to the simplified acquisition threshold through class deviations to the FAR. For example, DOD issued a FAR class deviation memo to implement the increase as of April 2018 and DHS and HHS did so as well as of June 2018.

DOD, the General Services Administration, and the National Aeronautics and Space Administration issued a final rule in July 2020 to amend the FAR to reflect the statutory increase of the simplified acquisition threshold to \$250,000, with an effective date of August 31, 2020.²³ At the same time, however, the final rule revised the FAR to establish that the E-Verify dollar threshold would remain at \$150,000.²⁴

²²National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 805 (2017).

²³The FAR is prepared, issued, and maintained jointly by the Secretary of Defense, the Administrator of General Services, and the Administrator, National Aeronautics and Space Administration, under their statutory authorities, and in consultation with the Administrator of the Office of Federal Procurement Policy. See 41 U.S.C. ch. 13; FAR 1.103.

²⁴See 85 Fed. Reg. 40,064, 40,065, 40,067 (July 2, 2020).

DLA contracting officials said that they updated their acquisition guidance to reflect the increased simplified acquisition threshold, but did not update it to reflect that the E-Verify dollar threshold remained at \$150,000. This led to confusion among DLA contracting staff regarding when to include the E-Verify clause in contracts. DLA officials also said that they use an automated contract writing system for most awards below the simplified acquisition threshold. However, the system was not set up to insert the E-Verify clause in all applicable contracts because it also was not updated to reflect that the E-Verify dollar threshold remained at \$150,000. As a result, the officials told us that they incorrectly omitted the E-Verify clause in contracts between \$150,000 and \$250,000 that met the E-Verify requirements from August 2020 to April 2023.

After we brought these omissions to their attention, DLA contracting officials took several actions to ensure the E-Verify clause is included in future contracts as appropriate. For example, they updated DLA's automated contract writing system to reflect the \$150,000 threshold for the E-Verify clause, and DLA officials said that contracting officials would determine whether or not the contract meets the FAR's requirement for inclusion of the E-Verify clause and include the clause accordingly. DLA also updated its acquisition guidance in June 2023 to reflect the \$150,000 E-Verify dollar threshold.

DLA contracting officials cited other non-DLA sources they use, which we found also contained incorrect information on the dollar threshold for the E-Verify clause. For example, they said that they rely on the Defense Acquisition University's contract clause matrix, which incorrectly listed the simplified acquisition threshold as the threshold for the E-Verify clause. In addition, USCIS's E-Verify website and Supplemental Guide for Federal Contractors also incorrectly listed the simplified acquisition threshold as the threshold for the use of the E-Verify clause. We contacted the Defense Acquisition University and USCIS about these discrepancies and they revised these sources to include the correct E-Verify dollar threshold.

Contracting Officials Did Not Accurately Report the E-Verify Clause in FPDS for Selected Contracts

In our analysis of 24 contracts, we found that DOD, DHS, and HHS contracting officials did not always accurately report information in FPDS about whether the E-Verify clause was included in a contract, as instructed by FPDS guidance. We selected the 24 contracts in our sample based on their FPDS records indicating that they appeared to be subject

to the FAR's requirement for including the E-Verify clause.²⁵ Of the 24 contracts we selected, 12 had FPDS records indicating that the clause was not included, and 12 had FPDS records indicating it was.²⁶

For the 12 contracts with FPDS records indicating that the clause was not included, we found that 10 included the clause, meaning the FPDS records were inaccurate for these contracts. Specifically, the Coast Guard, Federal Emergency Management Agency, Navy, National Institutes of Health, and Centers for Disease Control and Prevention each awarded two contracts or orders in our sample that included the clause in the selected contract or, in the case of orders, in the base contract, but did not report the clause's presence in FPDS. As discussed earlier, the other two contracts were awarded by DLA and did not include the E-Verify clause in the contract, even though they were subject to the clause under the FAR's requirement.²⁷ DOD, DHS, and HHS contracting officials provided a variety of reasons for this inaccuracy. The most commonly cited reason was human error. DLA contracting officials also cited confusion surrounding the E-Verify dollar threshold, which, as previously discussed, led them to not include the clause in the contract.

For the 12 contracts we selected where the FPDS records indicated the clause was included, we saw evidence in the contract documents that the clause was included, which corroborated the FPDS reporting. DOD, DHS, and HHS contracting officials cited several resources that contributed to their understanding of how to accurately report use of the clause. For example, the FPDS Data Element Dictionary states that system users should select the applicable reporting requirement for the contract, with the E-Verify clause as one of the available responses. Other documents, such as the DHS E-Verify job aid and the Defense Federal Acquisition Regulation Supplement's Procedures, Guidance, and Information, also include guidance on when, how, and where to mark the E-Verify response in FPDS. Some components also took additional steps to ensure that the use of the E-Verify clause was appropriately reported in FPDS. For example, the National Institutes of Health and Centers for Disease Control and Prevention used third-party service providers to identify

²⁵See our objectives, scope, and methodology in appendix I for additional details on how we selected the 24 contracts in our sample.

²⁶The relevant data element within FPDS that is intended to reflect whether the E-Verify clause was included in a contract is the "Employment Eligibility Verification (52.222-54)" response in the Additional Reporting field.

²⁷See FAR 22.1803.

FPDS discrepancies, and a Federal Emergency Management Agency policy office added the FPDS field for the E-Verify clause to its post-award review processes.

Although agency reporting in FPDS for these 12 contracts accurately reflected that the clause was included in the base contract, we found that agencies did not always accurately report the use of the E-Verify clause in orders issued under indefinite-delivery contracts. Specifically, the FPDS records for four orders we reviewed showed that the orders were not properly reported in FPDS to indicate that the underlying contract included the E-Verify clause.²⁸ The FPDS Data Element Dictionary and the DHS E-Verify job aid indicate that the FPDS field for the E-Verify clause needs to be marked each time an E-Verify-eligible order is placed under an indefinite-delivery contract that includes the E-Verify clause. However, contracting officials told us that they were unaware of the need to mark this FPDS field for such orders.

According to *Standards for Internal Control in the Federal Government*, agencies should communicate quality information externally to help achieve agency objectives.²⁹ Furthermore, the FPDS Data Element Dictionary instructs contracting officials to record the E-Verify clause's presence in FPDS for applicable contracts, including orders under indefinite-delivery contracts. Congress and executive branch agencies rely on FPDS to assess the effects of government-wide acquisition policies and processes. Without taking steps at DOD, DHS, and HHS to ensure contracting staff accurately report information about the E-Verify clause in FPDS for applicable contracts and orders, these agencies and Congress will not have accurate information on these agencies' use of the E-Verify clause for federal contractors.

FPDS Data Appears to Indicate Government-Wide Accuracy Issues with E-Verify Field

Beyond the 24 contracts, we also reviewed FPDS data on the number of contracts awarded government-wide in fiscal year 2021 that would appear

²⁸We also reviewed the FPDS records for the base indefinite-delivery contracts under which these orders were placed. In each case, the FPDS records indicated that the base contracts included the E-Verify clause.

²⁹GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

to be subject to the FAR's E-Verify requirement.³⁰ Our analysis did not allow us to conclusively determine whether the E-Verify clause should have been included in each contract, and thus whether use of the E-Verify clause was accurately reported in FPDS. It did, however, indicate that contracting officials across the government did not always report use of the E-Verify clause in FPDS when the contract appeared to be subject to the FAR's E-Verify requirement. Specifically, of the approximately 74,000 fiscal year 2021 contract awards that appeared to be subject to the FAR's E-Verify requirement and for which we might therefore expect the clause to be included, only about 15 percent were reported in FPDS as using the E-Verify clause.

For the six components we selected for our review, where FPDS indicated there were contracts and orders that were subject to the FAR's requirement for use of the E-Verify clause, our analysis found:

- National Institutes of Health and Centers for Disease Control and Prevention contracting officials reported use of the E-Verify clause in FPDS about 53 percent and about 43 percent of time, respectively.
- Coast Guard and Federal Emergency Management Agency contracting officials reported use of the E-Verify clause in FPDS about 36 percent and about 16 percent of the time, respectively.
- Navy and DLA contracting officials reported use of the E-Verify clause in FPDS about 6 percent and about 2 percent of the time, respectively.

There are three potential reasons why contracting officials may not report use of the E-Verify clause in FPDS for contracts that appear to be subject to the FAR E-Verify requirement. First, some of the contracts we included in our analysis may not actually be subject to the requirement for including the E-Verify clause, such as contracts for the purchase of commercial services that are part of the purchase of a COTS item. Second, agencies may have incorrectly omitted the E-Verify clause from the contract, despite the contract being subject to the FAR requirement to include the clause. Third, agencies may have included the clause correctly, but reported inaccurate information to FPDS. For example, as indicated earlier, contracting officials for 12 of the 24 contracts we

³⁰Specifically, we identified contracts that agencies reported in FPDS as exceeding \$150,000, having a period of performance of at least 120 days, having work primarily performed within the U.S., and involving the purchase of non-COTS items.

reviewed did not report use of the clause in the FPDS Additional Reporting field, which they attributed in part to human error.

According to the FAR and related guidance, agency chief acquisition officers must annually submit to the General Services Administration a certification of whether, and to what degree, their agency contract data in FPDS are accurate and complete.³¹ OMB, in collaboration with other federal agencies, establishes which data fields must be included in this annual verification and validation process. According to an OMB memorandum, the goals of this process include ensuring that FPDS data are reported properly so that the government has the right information when planning and awarding contracts and that the public has reliable data to track how its tax dollars are spent.³² However, the Additional Reporting field is not currently included among the data fields subject to this annual verification and validation process. The Digital Accountability and Transparency Act of 2014 also calls for improving the quality of data submitted to USAspending.gov—a public-facing website that pulls federal procurement data from FPDS—by holding federal agencies accountable for the completeness and accuracy of the data submitted.³³ Without OMB directing agencies to ensure the accuracy of their data in FPDS's Additional Reporting field, users of federal procurement data—such as Congress and the public—do not have the information required to know whether federal contracts included the E-Verify clause as required.

Selected Agencies Varied in Monitoring Contractor E-Verify Compliance and Lack Data from USCIS for This Duty

DHS, DOD, and HHS contracting officials differed in whether they took steps to monitor contractor compliance with the E-Verify clause (enrollment in and use of the program) in part because they had different understandings of their responsibilities. Contracting officials who took steps to monitor contractor compliance relied on USCIS reports that identified contractor enrollment and use, but USCIS discontinued these reports in March 2022 in part due to data limitations. Since then, USCIS has communicated limited information to agencies for monitoring contractor compliance with E-Verify.

³¹FAR 4.604(c).

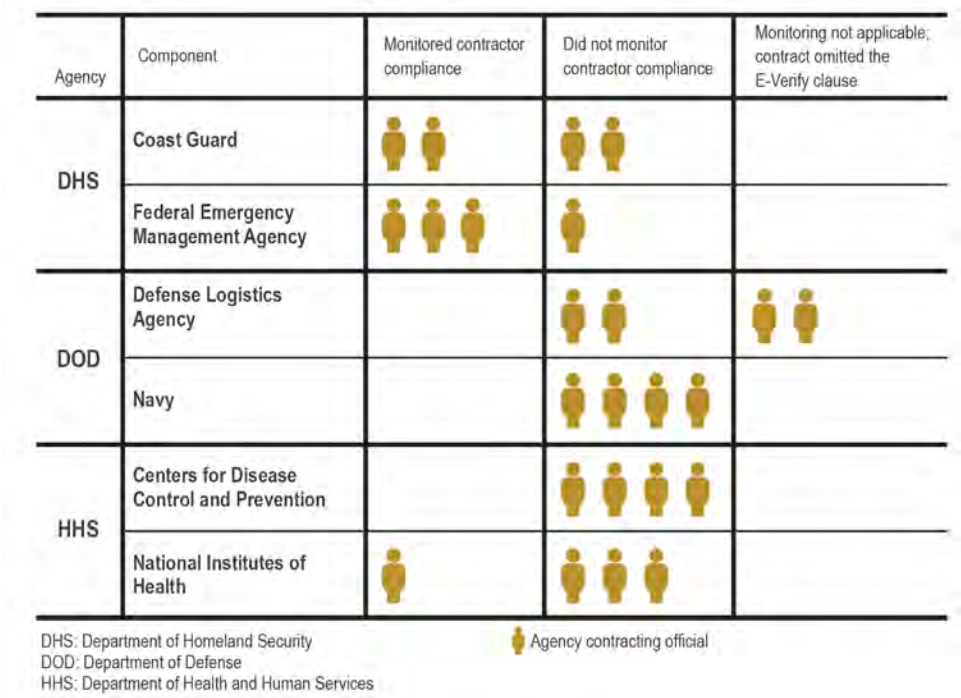
³²Office of Management and Budget, *Improving Federal Procurement Data Quality – Guidance for Annual Verification and Validation*, Office of Federal Procurement Policy Memorandum to Chief Acquisition Officers, Senior Procurement Executives, and Small Agency Council Members (Washington, D.C.: May 31, 2011).

³³Pub. L. No. 113-101 (2014) (codified as amended at 31 U.S.C. § 6101 note).

Selected Agencies Varied in Monitoring Contractor Compliance in Part Due to Differing Understandings of Responsibilities

DHS, DOD, and HHS contracting officials we interviewed differed as to whether they took any steps to monitor their contractors’ compliance with the E-Verify clause for the 24 contracts in our sample. For example, within DHS, a majority of the contracting officials we interviewed said they took some steps, whereas none of the DOD contracting officials we interviewed did so (see fig. 3).

Figure 3: Contracting Officials’ Reported Monitoring of Contractor Compliance with the E-Verify Clause for 24 Contracts GAO Reviewed



Source: GAO interviews of selected agency contracting officials; GAO (icons). | GAO-24-106219

When contracting officials did take steps to monitor contractor compliance, they took a variety of actions, such as consulting USCIS reports on contractors’ E-Verify enrollment and use. USCIS began issuing these quarterly reports in fiscal year 2020 to senior procurement officials throughout the government but stopped issuing them in 2022 due to data limitations, as discussed below. The reports included a list of federal contractors and whether they enrolled in and used E-Verify, among other things. DHS’s E-Verify job aid states that agencies should review the quarterly reports and take specific follow-up actions where the data indicate a contractor may not be complying with requirements of the E-

Verify clause. For example, the job aid states that agencies notify the contractor and then follow-up with USCIS if the contractor confirms they have enrolled in or used E-Verify.

Among contracting staff who did take steps to monitor contractor compliance, three of six reported that they had identified potential noncompliance with E-Verify in the past. All three said they had resolved the issues through informal actions, such as emailing the contractor. Only one of the five suspension and debarment offices we interviewed indicated they had ever received a referral to consider suspension or debarment of a federal contractor for E-Verify-related noncompliance. According to officials from that suspension and debarment office, that referral was subsequently closed with no action in part because the contract had already ended.

Agency officials we spoke with identified a variety of reasons why they did not take steps to monitor whether contractors enrolled in and used E-Verify in compliance with the E-Verify clause.³⁴ Among contracting officials we spoke with who said they did not monitor contractor compliance, 12 of 16 officials said it was because there is no requirement to do so or they thought another agency was responsible.³⁵ Further, DOD acquisition policy officials told us that contracting officials' roles are limited to including the clause in contracts and reporting that information in FPDS. They stated that monitoring contractor compliance with the E-Verify clause is DHS's responsibility as the program administrator for E-Verify.

Defense Contract Management Agency officials—who administer some DOD contracts when delegated—agreed with DOD acquisition policy officials' comments that contracting officials are not responsible for monitoring contractor compliance with the E-Verify clause. In explaining their rationale, they referenced a statement in the final rule that

³⁴We summarize the most common reasons given by these officials. Some officials gave various reasons that were not reflected by the group at large, such as the contract being cancelled soon after it was awarded or assuming that contractors would comply with the E-Verify clause as a contractual requirement.

³⁵Officials who said they thought another agency was responsible generally said they either expected DHS (as the E-Verify program administrators) or the Defense Contract Management Agency (which administers some DOD contracts when delegated) to be responsible for ensuring contractors complied with the E-Verify clause. Defense Contract Management Agency officials said they manage certain contract administration functions as delegated and that E-Verify compliance had never been one of these delegated responsibilities.

established the FAR E-Verify clause related to whether the proposed rule considered the costs associated with contracting officer time and effort. According to the statement, “contracting officer duties under the final rule consist almost exclusively of inserting the clause into appropriate solicitations and contracts,” and therefore, the associated effort for contracting officers would be marginal.³⁶ Defense Contract Management Agency officials told us they interpreted this statement to mean that a contracting officer is not responsible for monitoring contractor compliance with E-Verify. However, staff from OMB responsible for directing government-wide procurement policy said that this statement was not a direction to agencies on how to implement the E-Verify clause, but was rather part of the response to public comments on the proposed rule. They told us they would not expect agencies to take direction from a response to public comments on a proposed rule.

Instead, OMB pointed to USCIS’s previously produced FAR contractor reports, which were intended to provide agencies with information so that they could take action to resolve potential noncompliance. As noted earlier, some contracting officials we spoke with used these reports to help monitor compliance. However, USCIS officials said agencies varied in whether they followed up on these reports with USCIS, as the job aid states they should do. For example, they said HHS contracting officials have followed up, while DOD contracting officials have not. USCIS officials said it is challenging to coordinate with agencies when they perceive that some agency officials place a low priority on ensuring E-Verify compliance among contractors. Further, USCIS stopped issuing the reports in 2022, as discussed below.

Nearly all of the 24 federal contractors in our sample were enrolled in E-Verify, according to MOUs provided to us by USCIS. For the one contractor that we found was not enrolled, the agency’s contracting officials did not take timely action in response to information in USCIS’s report that indicated the contractor was not enrolled. In particular, according to USCIS, one of the 24 contractors—awarded a contract in September 2021—had not enrolled in E-Verify. A USCIS report to agencies dated March 2022 stated that this contractor, among others, was potentially noncompliant with E-Verify requirements. However, the contracting officials did not take action until they checked USCIS’s report

³⁶See 73 Fed. Reg. 67,651, 67,698 (Nov. 14, 2008). The statement was made by the Civilian Agency Acquisition Council and Defense Acquisition Regulations Council, in response to a public comment about whether the proposed rule considered the cost associated with contracting officer time and effort.

in response to our review and saw that the contractor was not enrolled. The officials told us they contacted the contractor using a USCIS form letter. The contractor subsequently enrolled in E-Verify in February 2023.

The FAR states that contracting officer responsibilities include ensuring compliance with the terms of a contract.³⁷ OMB staff told us they agreed with the DHS E-Verify job aid's guidance, which suggests that agencies review the USCIS quarterly reports and take follow-up actions as needed to ensure contractor compliance. OMB staff said that until we brought it to their attention, they were unaware of any challenges related to agency confusion over their responsibilities for monitoring E-Verify compliance.

According to OMB staff, OMB monitors issues in the federal contracting community and takes steps as necessary to resolve confusion and disagreement that it becomes aware of regarding agency responsibilities under the FAR. OMB staff said they have taken different approaches to resolve confusion on other topics depending on the circumstances. For example, they said OMB has issued clarifying guidance to address serious risks and issued "myth-busting" memos to resolve more minor inefficiencies caused by misunderstandings.

Though OMB staff expect agencies to use USCIS reports to monitor contractor E-Verify compliance, contracting officials were not always aware of this expectation. According to *Standards for Internal Control in the Federal Government*, control activities are generally more precise when they are routine and consistent rather than sporadic.³⁸ Without action to ensure that agencies have a consistent understanding government-wide of expectations for monitoring compliance with the E-Verify clause, agencies are at risk of not monitoring contractor E-Verify compliance and failing to take action to resolve potential contractor noncompliance.

USCIS Has Communicated Limited Information to Agencies for Monitoring Contractor E-Verify Compliance

We found that some selected agencies relied on quarterly USCIS reports to help ensure federal contractor compliance with the E-Verify clause. Beginning in fiscal year 2020, USCIS produced these reports to share E-Verify program data with senior procurement executives government-wide and help agencies ensure contractor compliance. Among the contracting officials who reported taking steps to monitor contractor compliance, five of six officials said they used the reports when doing so. DHS and HHS

³⁷FAR 1.602-2.

³⁸[GAO-14-704G](#).

acquisition policy officials also stated that contracting officials throughout their departments generally relied on the USCIS reports when monitoring contractor compliance with E-Verify.

While these reports were useful to some contracting officials, USCIS officials told us they stopped issuing the reports after March 2022 because they identified quality issues with the data underlying the reports. These issues included mismatches between employer names in various databases used to generate the reports and employers having duplicate E-Verify accounts.

According to USCIS officials, one reason E-Verify accounts were hard to match to other federal procurement data was due to changes in the unique identifier used to identify federal contractors and other entities with which the government does business. Prior to April 2022, the federal government used the Data Universal Numbering System for this purpose, which was a proprietary system managed by a federal contractor. In April 2022, federal agencies transitioned to using a new identifier called the Unique Entity Identifier, which is assigned by the General Services Administration's System for Award Management. USCIS began requiring that federal contractors provide the new identifier when enrolling in E-Verify as of August 2022, according to program officials. USCIS has encouraged federal contractors with preexisting E-Verify accounts to update their accounts with the new identifier, but according to program officials, USCIS can not currently require them to do so. As a result, it is challenging for USCIS to match E-Verify data to other federal procurement data. USCIS officials told us that requiring all federal contractors to provide their new identifier would necessitate a public notice and comment process that they characterized as burdensome. They would prefer if the General Services Administration instead added an "E-Verify organization ID" field to its award management system to facilitate data matching. Officials from the General Services Administration told us they avoid including information that may not be applicable to all users.

In addition to the data quality issues USCIS identified, we also identified potential clarity issues with information contained in the reports. For example, the reports contained a column about contractors' "E-Verify usage compliance." The E-Verify clause generally requires that federal contractors use E-Verify to verify the employment eligibility of new employees and employees assigned to the contract within certain time frames. However, the usage compliance column in the report does not reflect whether contractors are using E-Verify as described in the FAR

clause. Instead, the column reflects whether a contractor verified at least one employee at any time after enrolling. USCIS officials told us that collecting information to gauge whether a contractor had complied with the FAR in using E-Verify would be burdensome, so the usage compliance column was intended to provide some information about contractors' use given the constraints of their data. However, we found that the column's name may be unclear or misleading to contracting officials.

USCIS officials initially told us they intended to improve some of the reports' known issues and restart the reports in the first quarter of fiscal year 2023. However, in March 2023, USCIS officials told us they intended to wait for the results of our review to determine how, if at all, to modify the reports and issue them going forward. They also said they have limited insight into how the federal contracting community used the reports, among other USCIS resources related to contractors' use of E-Verify, and anticipated our review would provide clarity in that regard.

According to *Standards for Internal Control in the Federal Government*, an agency should use quality information to achieve its objectives, in particular by obtaining relevant data in a timely manner based on identified information requirements.³⁹ According to a USCIS document summarizing the missions of the division that houses the E-Verify program, improving federal contractor compliance with the E-Verify clause is one of the division's key initiatives. USCIS officials told us that it is a key initiative because federal contractors may need special assistance and instruction to ensure they understand and comply with their E-Verify responsibilities. They stated that the E-Verify reports had been part of that initiative before they stopped issuing them, along with presentations to federal contractors and contracting officials, and information shared on USCIS's public website. Without USCIS taking action to ensure it collects quality information regarding contractors' use of E-Verify, agencies' insight into the extent to which federal contractors are in compliance with requirements to enroll in and use E-Verify will be limited.

In addition to problems with the quality of data, contracting officials we interviewed at selected agencies also identified challenges related to USCIS's communication related to monitoring contractor compliance with E-Verify. Thirteen of the 24 contracting officials we spoke with said they

³⁹[GAO-14-704G](#).

did not have the information they would need to monitor contractors' compliance with the E-Verify clause, such as what steps they should take or where that information could be found. HHS officials told us that contracting officers find it challenging that the E-Verify website does not prominently share information directed to agency officials.

In the absence of the report, USCIS has not communicated to federal agencies what steps they could take to monitor contractor compliance with the E-Verify clause. USCIS officials told us that agency contracting officials should take independent steps to monitor contractor compliance with the E-Verify clause. For example, they said that agency contracting officials should request information directly from contractors. They also stated that agency contracting officials could request information from USCIS, though with the caveat that the quantity of requests could be burdensome for E-Verify staff. However, as of May 2023, USCIS officials told us they had not communicated these expectations to the federal contracting community. The most recent E-Verify job aid, dated March 2022, still states that agency contracting officials should use USCIS's reports. After we raised this issue with USCIS, in May 2023, USCIS posted information online that informed agencies it had ceased issuing the report. However, the information did not include guidance for what steps agencies could take to monitor contractor compliance with E-Verify going forward.

USCIS has not developed a plan to communicate quality information to agencies for the purpose of monitoring contractors' enrollment in and use of E-Verify. According to *Standards for Internal Control in the Federal Government*, an agency should communicate quality information to external parties to help achieve its objectives.⁴⁰ OMB staff told us that DHS—the agency responsible for administering E-Verify—should provide the tools and resources necessary for agencies to monitor contractor compliance with the E-Verify clause. Without USCIS taking action to ensure it communicates quality information to agencies, agency contracting officials will face challenges ensuring federal contractors' compliance with the E-Verify clause.

⁴⁰[GAO-14-704G](#).

USCIS Terminated Federal Contractor Accounts without a Process to Refer Them to Suspension and Debarment Officials

USCIS has terminated federal contractor E-Verify accounts for misuse—violations of the E-Verify MOU—but recently paused terminating accounts for non-use.⁴¹ Although USCIS has terminated such accounts for misuse and adds termination information to its public website, it does not have a process to refer federal contractors whose E-Verify accounts it has terminated to agency suspension and debarment officials.

USCIS Terminates Federal Contractor Accounts for Misuse, But Paused Non-use Terminations

As of March 2023, USCIS officials told us that, since fiscal year 2021, they had terminated around 300 federal contractor accounts for misuse without reinstatement.⁴² USCIS defines misuse as any violation of the terms of the E-Verify MOU or not cooperating with USCIS. According to USCIS, each termination for misuse occurred when the contractor refused to close or refer cases of unresolved tentative nonconfirmations—discrepancies between employee-submitted information and DHS or Social Security Administration data that prevent the confirmation of an employee's work eligibility.

USCIS officials stated that an unresolved tentative nonconfirmation could be the result of errors, or could indicate discrimination against employees. An example of an error might be an employer neglecting to close a tentative nonconfirmation after an employee decides not to take action to resolve it. An example of potential discrimination might be an employer not providing certain employees with the option to take action to resolve a tentative nonconfirmation, as required under E-Verify. For each termination for misuse, USCIS officials stated that they emailed or called the employer multiple times to notify it of its noncompliance, and provided each employer with a 30-day termination notice. USCIS will reinstate an employer's account if the employer provides a written request. Employers then have 30 days to rectify the issue that resulted in the termination for misuse, such as by closing a tentative nonconfirmation.

⁴¹As mentioned earlier in the report, employers self-identify as federal contractors within the E-Verify system.

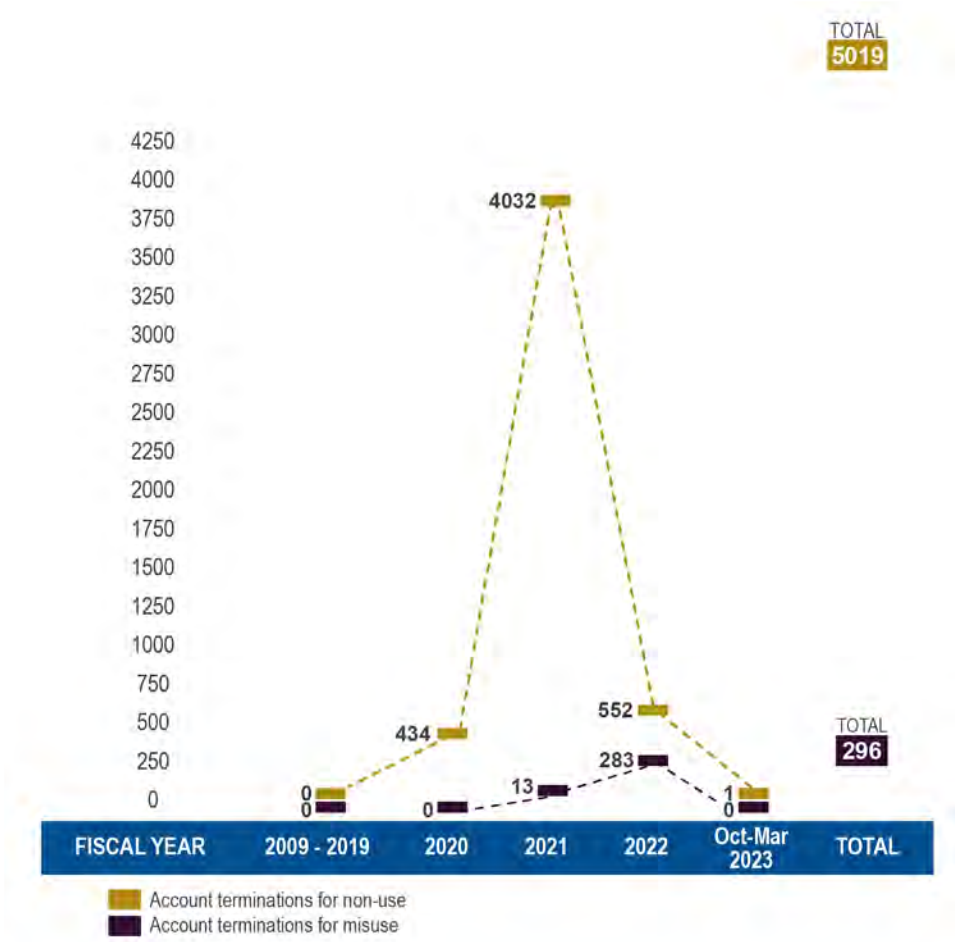
⁴²According to USCIS, its termination data include accounts that it terminated and has not reinstated. Once USCIS reinstates an employer's account, that account no longer appears in the termination data. USCIS officials said that they are working on a way to track historical termination data and hope to implement it before the end of fiscal year 2023.

Prior to fiscal year 2023, USCIS also terminated federal contractor accounts for non-use. USCIS defines non-use as any employer that fails to verify any employees or update its account over a 3-year period. From fiscal year 2020 through March 2023, USCIS identified terminating more than 5,000 federal contractor accounts for non-use. USCIS officials told us that they reinstated an employer's account if the employer took steps to rectify the issue, such as logging into the E-Verify system.

Beginning in fiscal year 2023, USCIS paused terminating federal contractors' E-Verify accounts for non-use. USCIS officials stated that they exempted federal contractors from non-use terminations in November 2022 because there may be legitimate reasons why a self-identified federal contractor did not use the E-Verify system within a 3-year period. Specifically, federal contractors are required to use E-Verify when they have an active federal contract with the E-Verify clause, but are not required to use E-Verify when they do not have an active contract with the clause. If a company has not held a federal contract with the E-Verify clause for 3 years, it would not be required by federal regulation to use E-Verify. By not terminating those accounts for non-use, USCIS officials said that those federal contractors would be able to verify employees in the future if they were awarded a new federal contract with the E-Verify clause.

USCIS told us that from fiscal years 2009 through 2019, they did not terminate accounts—including those of federal contractors—for misuse or non-use because USCIS chose not to enforce the termination option in the E-Verify MOU for these accounts (see fig. 4).

Figure 4: Federal Contractor E-Verify Accounts Terminated for Misuse and Non-use as of March 31, 2023



Source: GAO analysis of U.S. Citizenship and Immigration Services (USCIS) termination data. | GAO-24-106219

Note: According to U.S. Citizenship and Immigration Services (USCIS), its termination data represent federal contractor accounts that USCIS terminated and did not reinstate as of March 31, 2023. Once USCIS reinstates an employer's account, that account no longer appears in the termination data.

USCIS officials stated that they began to terminate accounts for misuse and non-use in fiscal years 2020 and 2021 due to USCIS leadership's policy goals. The first goal was to clean up the number of inactive accounts starting in fiscal year 2020 to reduce account maintenance and USCIS's administrative compliance activities, such as calling or emailing

employers.⁴³ The second goal, which began in May 2021, was to reduce the number of accounts with unresolved tentative nonconfirmations. USCIS officials stated that they have not terminated as many federal contractor accounts for misuse from October 2022 to March 2023, because they have already addressed most accounts with unresolved tentative nonconfirmations. They added that they continue to take administrative compliance actions such as calling or emailing federal contractors when issues arise. Although they are no longer terminating federal contractor accounts for non-use, as previously noted, they said they consider terminating accounts for misuse as necessary.

USCIS Does Not Have a Referral Process for Terminated Federal Contractor Accounts

USCIS does not have a process to refer federal contractors whose E-Verify accounts it has terminated to federal agencies' suspension and debarment officials. The FAR requires that when DHS terminates a federal contractor's E-Verify MOU, and therefore denies the contractor access to the E-Verify system, it must refer the contractor to a suspension or debarment official for a possible suspension or debarment action.⁴⁴ DHS officials from the Office of the General Counsel stated that USCIS is responsible for implementing this referral process since it is the component responsible for terminating E-Verify MOUs. Instead of a referral, however, USCIS officials told us that as of March 2020, they started providing account termination information about employers, including federal contractors, within a searchable database that is accessible from the E-Verify website entitled "How to Find Participating Employers" (see fig. 5).

⁴³USCIS officials stated that some of these employers may have ceased operations or merged and created other E-Verify accounts.

⁴⁴FAR 22.1802(e). While the FAR directs this requirement to DHS, USCIS is the DHS component that administers the E-Verify program, makes determinations of whether to terminate MOUs, and carries out those terminations.

Figure 5: USCIS E-Verify Website Screenshot of How to Find Participating Employers, Taken May 25, 2023



[Employers](#)
[Employees](#)
[About E-Verify](#)
[Key Links](#)

[Home](#) > [About E-Verify](#) > [E-Verify Data](#) > How To Find Participating Employers
 [Share This Page](#)

How To Find Participating Employers

Use the E-Verify search tool to find employers who are currently enrolled in E-Verify. Your search will display the following information:

- Employer name** – The name the employer used when they enrolled in E-Verify. This can be the business' legal name, a trade name, or an abbreviation.
- Doing Business As (DBA) name** – The name an employer uses publicly. The public may see the DBA, but the employer may have used another name when they enrolled in E-Verify.
- Account Status** – Indicates whether the account is currently enrolled or terminated.
- Enrollment date** – The date the E-Verify Memorandum of Understanding is signed.
- Termination Date** – The E-Verify Memorandum of Understanding termination date.
- Workforce size** – Appears as long as the employer reported they have at least five employees.
- Number of hiring sites** – The locations where employers hire employees and where they complete Form I-9.
- Hiring site locations (by state)** – The geographic location(s) of hiring sites, by state, reported by the employer.

Parameters:

- USCIS updates the search tool data every quarter. However, employer status may be updated as needed.
- Employers report their own data at the time they enroll in E-Verify. The accuracy and completeness of the data depend on what was submitted by employers at the time of enrollment and as reported throughout the employer's relationship with E-Verify.
- [Review Employer Data Parameters](#)

Search

Business Name

Primary Industry Type

Hiring Site Locations (by state)

Account Status

Items per page

SEARCH

RESET

Employer	Doing Business As	Account Status	Date Enrolled	Date Terminated	Workforce Size	Number of Hiring Sites	Hiring Site Locations (by state)

Source: U.S. Citizenship and Immigration Services (USCIS) website. | GAO-24-106219

This page of the website functions as a database of employers participating in E-Verify and provides, among other things, the following information:

- **Employer name.** The name the employer used when it enrolled in E-Verify. This can be the business's legal name, a trade name, or an abbreviation.
- **Account status.** Indicates whether the account is currently enrolled or terminated.
- **Enrollment date.** The date that the employer signed the E-Verify MOU.
- **Termination date.** The E-Verify MOU termination date.

The information on USCIS's employer participation website does not include certain items of information identified in DHS's guidance for suspension and debarment referrals. DHS's *Suspension and Debarment Instruction* defines a referral as a written request for action supported by documentary evidence, and presented to the suspension and debarment official.⁴⁵ However, the website does not provide:

- documentary evidence outlining the circumstances of the termination; and
- a request for action for terminated federal contractors.

According to DHS officials from the Office of the General Counsel and the Office of the Chief Procurement Officer, USCIS's inclusion of account termination information in its E-Verify employer participation website does not constitute a referral to a suspension or debarment official under FAR 22.1802(e). For example, a DHS official stated that the fact that USCIS terminated a contractor's account would not itself be a referral without supporting documentation outlining the circumstances of the termination.

Additionally, based on our interviews with DHS, DOD, and HHS suspension and debarment officials, the information on the E-Verify website does not meet suspension and debarment officials' expectations for referrals. All of the DHS, DOD, and HHS suspension and debarment officials (five of five) we interviewed said that they do not consider the information on USCIS's website to constitute a referral.

⁴⁵Department of Homeland Security, *Suspension and Debarment Instruction*, 146-01-00, Revision Number 01 (Apr. 10, 2018).

USCIS officials told us that posting termination information on the E-Verify website would meet the FAR's referral requirement. DHS officials told us, however, that USCIS has not met the FAR's referral requirement due to a misunderstanding of the suspension and debarment process. After we alerted DHS to this issue, DHS officials told us in July 2023 that USCIS plans to take several steps to comply with the FAR referral requirement, including (1) developing a process to make referrals to suspension and debarment officials; and (2) assessing whether there may be a need to increase staffing at USCIS's Office of Contracting to support this process. They also said they planned to update termination notices to inform federal contractors that their termination may result in a suspension or debarment referral, which officials hope would improve compliance. As of July 2023, officials stated that they were early in the process for these plans and could not yet provide documentation or a time frame for when they may be complete.

USCIS has terminated thousands of federal contractors' accounts since fiscal year 2020, including hundreds for misuse, without a referral process consistent with DHS standards. Until USCIS documents and implements a referral process, agency suspension and debarment officials will not be able to determine whether federal contractors' misuse of E-Verify merits suspension or debarment.

Conclusions

Including the E-Verify clause in applicable contracts, as required by the FAR, helps ensure that federal contracts performed in the U.S. will be staffed by individuals who are authorized to work in the U.S. While DOD, DHS, and HHS generally included the clause in the contracts we selected, these agencies did not always accurately report in the federal procurement data system that the contracts contained the clause. Without ensuring contracting officials know when and how to accurately indicate in federal procurement data the clause's inclusion in an applicable contract, users of the federal procurement data system—including federal agencies and Congress—do not have accurate information regarding the use of the E-Verify clause. Moreover, our review of government-wide federal procurement data suggests that many contracts that appear to be subject to the FAR's requirement for the inclusion of the clause may not include it. Similar to the findings from our sample, it is possible that the clause was included in these contracts but not accurately reported in federal procurement data. Taking additional steps to ensure the accuracy of federal procurement data—such as incorporating the relevant federal procurement data field in government-wide annual verification and validation reports overseen by OMB—would help ensure the information in the federal procurement data system accurately reflects the presence

of the E-Verify clause in applicable contracts on a government-wide basis.

Due in part to differing understandings of their responsibilities, the selected agencies in our review varied in their efforts to monitor contractor enrollment in and use of E-Verify. Without a consistent understanding of government-wide expectations for doing so, agencies are at risk of not monitoring contractors and failing to take action to resolve potential contractor noncompliance. Further, most contracting officials we interviewed who were monitoring contractor compliance relied on quarterly USCIS reports for this purpose. However, USCIS stopped issuing these reports in early 2022 due to data quality challenges. Until USCIS collects and communicates the necessary quality data to agencies, it cannot ensure that federal agencies have reliable information to overcome the challenges they have encountered monitoring compliance with the E-Verify clause.

While USCIS is developing a process for referring a federal contractor to a suspension and debarment official following termination of the contractor's E-Verify MOU, as required by the FAR, it has not yet established a time frame for doing so or documentation outlining its plans. As a result, USCIS is not currently meeting this requirement. In turn, suspension and debarment officials are unable to perform their duties in determining whether or not the reasons for terminating an account merit suspension or debarment. By collecting quality information, improving communications, and developing a clear referral process, DHS and USCIS could better support agencies' efforts to monitor E-Verify compliance.

Recommendations for Executive Action

We are making a total of eight recommendations, including one to DOD, two to DHS, one to HHS, two to OMB, and two to USCIS. Specifically:

The Secretary of Defense should ensure that DOD's Principal Director of Defense Pricing and Contracting takes steps to ensure that contracting staff correctly select the Employment Eligibility Verification response in FPDS for applicable contracts and orders. (Recommendation 1)

The Secretary of Homeland Security should ensure that DHS's Chief Procurement Officer takes steps to ensure that contracting staff correctly select the Employment Eligibility Verification response in FPDS for applicable contracts and orders. (Recommendation 2)

The Secretary of Health and Human Services should ensure that HHS's Deputy Assistant Secretary for Acquisitions takes steps to ensure that contracting staff correctly select the Employment Eligibility Verification response in FPDS for applicable contracts and orders. (Recommendation 3)

The Director of OMB should ensure that Office of Federal Procurement Policy's Administrator takes steps to identify the extent to which there are government-wide issues with the accuracy of FPDS's Additional Reporting field, and takes appropriate management measures as necessary, such as including the field in the annual verification and validation process as it pertains to E-Verify. (Recommendation 4)

The Director of OMB should ensure that Office of Federal Procurement Policy's Administrator issues guidance for agencies clarifying its expectations that they should monitor contractor enrollment in and use of E-Verify with resources provided by USCIS. (Recommendation 5)

The Director of USCIS should identify and implement an approach to collect quality information on federal contractors enrolled in E-Verify for the purpose of helping agencies monitor contractor compliance, such as by collecting Unique Entity Identifiers from federal contractors with existing E-Verify accounts. (Recommendation 6)

After implementing an approach to collect quality information, the Director of USCIS should develop and implement an approach to communicate quality information to agencies for the purpose of monitoring contractor compliance with E-Verify. (Recommendation 7)

The Secretary of Homeland Security should ensure that USCIS's Director takes steps to document and implement a process for referring federal contractors to a suspension or debarment official if USCIS terminates their E-Verify MOU. (Recommendation 8)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD, DHS, HHS, the General Services Administration, and OMB for review and comment. DOD, DHS, and HHS provided written comments, which are reproduced in appendixes II, III, and IV, and OMB responded via email. DOD, DHS, and HHS concurred with the recommendations made to each of their agencies and identified steps they plan to take to address the recommendations. OMB concurred with the two recommendations directed to it. DHS, HHS, and OMB also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, the Secretary of Homeland Security, the Secretary of Health and Human Services, the Administrator of the General Services Administration, and the Director of OMB. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact Timothy J. DiNapoli at (202) 512-4841 or dinapolit@gao.gov or Rebecca Gambler at (202) 512-8777 or gablerr@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.



Timothy J. DiNapoli
Managing Director, Contracting and National Security Acquisitions



Rebecca Gambler
Director, Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

This report addresses the extent to which (1) selected federal agencies ensured the E-Verify clause was included in selected contracts and reported in the Federal Procurement Data System (FPDS); (2) selected federal agencies monitored whether federal contractors comply with the E-Verify clause; and (3) U.S. Citizenship and Immigration Services' (USCIS) has taken administrative actions against federal contractors that did not comply with E-Verify program requirements.

To address our first objective, we selected the Departments of Defense (DOD), Homeland Security (DHS), and Health and Human Services (HHS). We selected these three because according to FPDS data, they were among the agencies with the highest number of contracts, orders, and associated obligations from fiscal years 2019 to 2021 that appeared to be subject to the Federal Acquisition Regulation's (FAR) requirement for inclusion of the E-Verify clause.¹ We selected fiscal years 2019 to 2021 because we wanted multiple years of data to ensure we had an accurate understanding of how agencies' E-Verify-eligible awards and associated obligations changed over time and these 3 years were the most recent fiscal years for which data were available at the time of our review. The three agencies accounted for nearly two-thirds of all awards in fiscal years 2019 to 2021 that appeared to be subject to the FAR's E-Verify requirement.

The FAR's E-Verify criteria generally require federal contracting officers to include the E-Verify clause in federal contracts that exceed \$150,000 unless the contract: (1) has a period of performance of less than 120 days; (2) is only for work performed outside the U.S.; or (3) is only for commercially available off-the-shelf (COTS) items or commercial services that are part of the purchase of a COTS item.² We initially contemplated including federal grants in our analysis, so we cross-referenced the agencies' contract data in FPDS against grants data in USASpending.gov to prioritize agencies that also had higher numbers of grants. After reviewing the FAR and interviewing DOD, DHS, and HHS officials, we

¹Executive departments and agencies are responsible for collecting and reporting data to FPDS as required by the FAR. See FAR subpart 4.6. FPDS collects and disseminates procurement data to Congress, agencies, and the private sector. The government uses the reported data to measure and assess the impact of federal procurement on the nation's economy, the extent to which awards are made to businesses in the various socioeconomic categories, the impact of full and open competition on the acquisition process, and other procurement policy purposes. Unless otherwise specified, we collectively refer to contracts and orders as contracts in this appendix.

²FAR 22.1803.

determined that the FAR's E-Verify clause requirement does not apply to grants. Grants are administered under separate regulations than the FAR, principally, the Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.³ Therefore, we ultimately decided to exclude grants and subgrants from our review.

We applied the same selection methodology to select two components from each of the three agencies for a total of six components. Selected components included the Defense Logistics Agency (DLA) and the Navy for DOD, the Federal Emergency Management Agency and the U.S. Coast Guard for DHS, and the Centers for Disease Control and Prevention and the National Institutes of Health for HHS. According to FPDS, these components are among those with the highest number of contract awards and associated obligations from fiscal years 2019 to 2021 that appeared to be subject to the FAR's requirement for inclusion of the E-Verify clause. Within each component, we randomly selected 4 fiscal year 2021 contracts that met E-Verify criteria for a nongeneralizable sample of 24 contracts. The results of our analysis are not generalizable, but they provided insight into challenges selected agencies were faced with, such as including the E-Verify clause in applicable contracts and reporting use of the E-Verify clause in FPDS. We selected contracts awarded in fiscal year 2021 as it was the most recent year for which we had full data available when we began our review.

To select the contracts from each component, we randomly selected two contracts in which FPDS data indicated the E-Verify clause was included and two in which the data indicated the clause was not present. For each selected contract or order, we analyzed contract documentation to determine whether it included the E-Verify clause, and federal procurement data to identify whether agency contracting officials marked the E-Verify response in FPDS's Additional Reporting field. We also randomly selected six subcontracts from our sample of prime contracts—one from each component—and analyzed subcontract documentation to determine if the prime contractor included the E-Verify clause in these subcontracts.

We took several steps to assess the reliability of the federal procurement data. These steps included successfully tracing information in the 24 selected prime contracts back to multiple data elements in each contract's or order's record in FPDS, performing electronic testing for obvious errors

³2 C.F.R. part 200.

in accuracy and completeness, and analyzing agencies' FPDS data certifications. We determined the data were sufficiently reliable for the purposes of determining whether each selected contract and subcontract met the FAR's criteria for inclusion of the E-Verify clause. The data were not reliable for determining whether the E-Verify clause was included in the contract, but we corrected for these reliability issues by reviewing the 24 selected contracts and interviewing DOD, DHS, and HHS contracting officials.

We excluded some contract categories from our nongeneralizable sample. For example, we excluded contracts for commercial products because the FAR's requirement for use of the E-Verify clause generally excludes contracts that are only for COTS items and contracts for commercial services that are part of the purchase of a COTS item. We excluded orders placed under basic ordering agreements because they accounted for a small number of orders in fiscal year 2021.⁴ We also excluded orders under government-wide acquisition contracts and federal supply schedule contracts—both of which are specific types of contracts that can be used by agencies government-wide—because that analysis would have required contract documents from non-DOD, DHS, and HHS agencies. For five of our initial selections, we randomly selected a contract or order that met our criteria for exclusion from the sample, such as a contract for COTS items. For those five selections, we excluded the contract or order and moved to the next contract or order on the randomized list.

We also analyzed FPDS data to estimate the percentage of contracts awarded in fiscal year 2021 that appeared to be subject to the E-Verify requirement but for which contracting officials had not recorded the presence of the clause in FPDS, both government-wide and for the six selected components. We identified contracts that appeared to be subject to the E-Verify requirement using the same criteria described above. However, unlike our sample selection criteria described above, we excluded contracts that used simplified acquisition procedures because FPDS data do not indicate if these contracts are for commercial products. We then reviewed how many of these contracts did and did not have the Additional Reporting Field—Employment Eligibility Verification (52.222-54) option selected in FPDS. Some contracts we excluded may require the E-Verify clause, such as contracts using simplified acquisition

⁴Basic ordering agreements are written instruments negotiated between agencies and contractors that describe, among other things, the methods for determining pricing, issuing, and delivering future orders under the agreements.

procedures. Some of the contracts included in our analysis may not require the E-Verify clause, such as contracts for the purchase of commercial services that are part of the purchase of a COTS item.

We also identified and assessed the FAR's E-Verify requirements and department-wide and selected components' acquisition regulations, policies, and training documentation for ensuring the E-Verify clause is included, as appropriate, in selected contracts, orders, and subcontracts. We analyzed the FPDS Data Element Dictionary; DHS's E-Verify job aid; and the Defense Federal Acquisition Regulation Supplement's Procedures, Guidance, and Information to identify guidance for agency reporting on the use of the E-Verify clause in FPDS's Additional Reporting field. Based on these guidance documents and our analysis of the 24 selected contract files, we determined that contracting officials should have marked the E-Verify response in FPDS for each selected contract. We also compared department-wide and government-wide acquisition policies related to ensuring the accuracy of FPDS data against federal internal control standards. We determined that the information and communication component of *Standards for Internal Control in the Federal Government*, specifically the underlying principle that management should externally communicate the necessary quality information to achieve their objectives, was significant to this objective.⁵ We analyzed the Digital Accountability and Transparency Act of 2014, the FAR, and related guidance to identify government-wide requirements that agency procurement data should be accurate and complete.⁶

We interviewed DOD, DHS, and HHS acquisition policy and contracting officials across 30 offices about possible reasons the E-Verify clause was not included in a particular contract or order, despite the contract apparently meeting the FAR's E-Verify criteria, or why inclusion of the E-Verify clause was not accurately reported in FPDS's Additional Reporting field, if applicable. These officials also confirmed our assessment about whether each selected contract or order included the E-Verify clause and if each selected contract's or order's record in FPDS accurately reflected inclusion of the E-Verify clause in the Additional Reporting field. We interviewed General Services Administration officials responsible for administering FPDS to understand the addition of the E-Verify response to the Additional Reporting field and the extent to which the value in the

⁵GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

⁶See Pub. L. No. 113-101 (2014) (codified as amended at 31 U.S.C. 6101); FAR 4.604(c).

Additional Reporting field propagates from an indefinite delivery contract to an order. We also interviewed representatives of six prime contractors to confirm whether they included the E-Verify clause in selected subcontracts and to determine their processes for including the E-Verify clause in applicable subcontracts.

To address our second objective, we analyzed USCIS data to assess the extent to which contractors in our sample enrolled in and used E-Verify. These data included information on the contractors' dates of enrollment, enrollment status at the time of our review (i.e., whether their accounts were active or terminated), and information on whether contractors had used E-Verify to verify employees. We assessed the reliability of these data by comparing them with the selected contracts and FPDS records. We also interviewed USCIS officials to understand the known limitations of the data and their reporting on contractor enrollment and use of E-Verify. We determined that the data were sufficiently reliable for the purposes of describing contractor enrollment in E-Verify. However, we determined the data were not reliable for assessing whether contractors verified employees as described under the E-Verify clause. We determined the data were not reliable because, while they included information on whether contractors had verified any employees, they did not include information on whether the contractors verified employees in accordance with the E-Verify clause. For example, the data could demonstrate that a contractor verified one employee without including information about whether those employees were assigned to a federal contract, or whether the contractor should have verified additional employees to comply with the E-Verify clause. As a result, we did not include data in our report on whether contractors verified employees in accordance with the FAR's E-Verify requirements.

We analyzed tools, resources, and reports that USCIS created to communicate E-Verify program data and help agencies monitor contractor compliance with E-Verify. We compared USCIS efforts against federal internal control standards. We determined that the information and communication component of *Standards for Internal Control in the Federal Government*, specifically the underlying principles that management should obtain and externally communicate the necessary quality information to achieve their objectives, were significant to this objective.⁷

⁷[GAO-14-704G](#).

In addition, we analyzed contract performance assessment reports for the contracts in our sample to determine the extent to which contracting staff reported that they took actions for contractor noncompliance with the E-Verify clause. We interviewed DOD, DHS, and HHS acquisition policy and contracting officials about their policies and procedures for ensuring contractor compliance with E-Verify. We spoke with officials to understand both their general policies for ensuring contractor compliance, and the extent to which contracting staff took steps to monitor contractor compliance for the contracts in our sample. We also interviewed DOD, DHS, and HHS suspension and debarment officials across five offices about whether they had received referrals for contractor noncompliance with E-Verify, and any actions taken in response. We interviewed USCIS officials about their oversight of E-Verify and any coordination with federal contracting officials to monitor contractor compliance. We interviewed OMB staff about their expectations for the federal contracting community regarding ensuring contractor compliance with E-Verify. We interviewed representatives of six prime contractors regarding any steps agencies had taken to ensure their compliance with E-Verify. We compared agency efforts against federal internal control standards. We determined that the design of control activities component of *Standards for Internal Control in the Federal Government*, specifically that management should consider the consistency of performance, were significant to this objective.

To address our third objective, we collected and reviewed key policy and guidance documentation related to administrative compliance actions. These documents included the 2013 E-Verify Memorandum of Understanding for Employers, 2022 USCIS's *Termination & Reinstatement Policy & Procedures*, 2022 USCIS's *Behavior Descriptions*, as well as other relevant guidance documents to identify how USCIS takes action for noncompliance.

We analyzed USCIS federal contractor E-Verify account termination data for fiscal years 2009 through 2023 to assess the extent to which USCIS had terminated federal contractor accounts. We selected fiscal year 2009 as the starting point for collecting this data since this is the year the FAR was amended to require federal contractors to enroll in and use E-Verify under certain contracts (the exceptions are discussed in this report). These data included information on the number of contractor accounts terminated by fiscal year and the reason for termination. To assess the reliability of the data, we interviewed USCIS data analysts and reviewed existing information about the data collection program. We determined that the data were sufficiently reliable for the purposes of describing the

number and type of USCIS's account terminations. We compared USCIS's termination actions with its termination policies.

We also reviewed FAR 22.1802(e) and assessed DHS's policies for ensuring that it refers federal contractors whose memorandums of understanding (MOU) it has terminated to suspension and debarment officials. We reviewed USCIS's E-Verify website and compared that information with DHS's guidance for making suspension and debarment referrals in *Suspension and Debarment Instruction* 146-01-00.⁸

We interviewed USCIS officials about steps they take to address contractor noncompliance with the E-Verify MOU, including account termination and referral for suspension or debarment. We also interviewed officials within DHS's Office of the General Counsel and Office of the Chief Procurement Officer, as well as DOD, DHS, and HHS suspension and debarment officials, about USCIS's process for notifying suspension and debarment officials about terminations of federal contractor E-Verify MOUs.

We conducted this performance audit from August 2022 to October 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

⁸Department of Homeland Security, *Suspension and Debarment Instruction*, Instruction Number 146-01-00, Revision Number 01 (Apr. 10, 2018).

Appendix II: Comments from the Department of Defense



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

Ms. Marie A. Mak
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Ms. Mak,

This is the Department of Defense (DoD) response to the GAO Draft Report
GAO-23-106219, "FEDERAL CONTRACTING: Agencies Can Better Monitor E-Verify
Compliance," dated August 16, 2023 (GAO Code 106219).

Enclosed is DoD's response to the subject report. My point of contact is Mr. Larry
McLaury who can be reached at 571-309-0940 or via email at [osd.pentagon.ousd-a-s.mbx.asda-
dp-c-contractpolicy@mail.mil](mailto:osd.pentagon.ousd-a-s.mbx.asda-dp-c-contractpolicy@mail.mil).

Sincerely,

TENAGLIA Digitally signed by
TENAGLIA.JOHN.
JOHN.M.1 M.1154945926
154945926 Date: 2023.09.07
17:06:21 -04'00'

John M. Tenaglia
Principal Director,
Defense Pricing and Contracting

Enclosure:
As stated

Enclosure

GAO DRAFT REPORT DATED AUGUST 16, 2023
GAO-23-106219 (GAO CODE 106219)

**“FEDERAL CONTRACTING: AGENCIES CAN BETTER MONITOR
E-VERIFY COMPLIANCE”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

RECOMMENDATION 1: The Secretary of Defense should ensure that DoD’s Principal Director of Defense Pricing and Contracting (DPC) takes steps to ensure that contracting staff correctly select the Employment Eligibility Verification response in FPDS for applicable contracts and orders.

DoD RESPONSE: Concur. DPC will publish a policy memorandum directing the acquisition workforce to review the Federal Acquisition Regulation (FAR) 22.18, “Employment Eligibility Verification,” and to insert FAR Clause 52.222-54, “Employment Eligibility Verification” in all required contracts. Additionally, the memorandum will cite Defense FAR Supplement, Procedures, Guidance, and Information 204.606(x)(C)(3), “Reporting Information: FPDS Entry – Legislative Mandates Section,” to remind the acquisition workforce to identify in FPDS if FAR Clause 52.222-54, “Employment Eligibility Verification,” or FAR clause 52.212-5, “Contract Terms and Conditions Required to Implement Statutes or Executive Orders—Commercial” are included in the contract.

Appendix III: Comments from the Department of Homeland Security

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



September 18, 2023

Timothy J. DiNapoli
Managing Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Rebecca Gambler
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-23-106219, "FEDERAL CONTRACTING: Agencies Can Better Monitor E-Verify Compliance"

Dear Mr. DiNapoli and Ms. Gambler:

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

DHS leadership is pleased to note GAO's recognition of the critical role the U.S. Citizenship and Immigration Services (USCIS) plays in managing E-Verify as an electronic means for verifying employment eligibility of workers in the United States, which processes nearly 50 million cases annually and is one of the government's highest-rated services for user satisfaction.¹ Beginning in 2017, the Department also took several actions to drive contractor compliance with the requirements of Federal Acquisition Regulation (FAR) clause 52.222-54, "Employment Eligibility Verification," such as increasing communication to both contractors and subcontractors on the clause's requirements and providing several training webinars to the acquisition workforce. GAO also acknowledged recent USCIS efforts to improve program integrity by instituting Memorandum of Understanding (MOU) termination procedures for employers that do not properly use the E-Verify system.

¹ <https://www.e-verify.gov/about-e-verify>

DHS remains committed to ensuring Federal contractor compliance with FAR E-Verify requirements. To that end, the E-Verify web pages², “Supplemental Guide For Federal Contractors,”³ and presentation materials for federal contractors were updated in June 2023 to reflect amended FAR clause threshold requirements. The existing “E-Verify Notice of Intent to Terminate” and “Final Termination” notice templates were also updated in August 2023 to emphasize the suspension and debarment referral process for contractors should their MOU be terminated. DHS will continue to ensure that the requisite clause is included in applicable contracts and accurately reported in the Federal Procurement Data System (FPDS).

The draft report contained eight recommendations, including four for DHS with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity, and editorial issues under a separate cover for GAO’s consideration.

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

Sincerely,

JIM H CRUMPACKER²
Digitally signed by JIM H
CRUMPACKER
Date: 2023.09.18 09:17:55 -0400

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

² <https://www.e-verify.gov/employers/federal-contractors/who-is-affected-by-the-e-verify-federal-contractor-rule>
and <https://www.e-verify.gov/employers/federal-contractors/federal-contractors-qas>

³ <https://www.e-verify.gov/supplemental-guide-for-federal-contractors>

**Enclosure: Management Response to Recommendations
Contained in GAO-23-106219**

GAO recommended that the Secretary of Homeland Security:

Recommendation 2: Ensure that DHS's Chief Procurement Officer takes steps to ensure that contracting staff correctly select the Employment Eligibility Verification response in FPDS for applicable contracts and orders.

Response: Concur. The DHS Office of the Chief Procurement Officer (OCPO) has several processes in place to assist contracting officers to correctly insert FAR clause 52.222-54 in solicitations and contracts, and properly report in FPDS. These include:

- The "Job Aid on Employment Eligibility Verification (E-Verify)," dated March 2022, that provides agency contracting officials with guidance on properly reporting employment eligibility verification requirements in contracts and orders.
- A slide deck, "Additional Reporting - Employment Eligibility Verification (E-Verify),"⁴ on reporting employment eligibility verification that is used to reinforce accurate reporting in FPDS and which is posted on Acquisition.gov under "Data Initiatives" for use by all Federal agencies. DHS Components are also provided this same information by OCPO during annual training on FPDS and other government-wide systems.
- Internal automated edit checks to FPDS reporting on each DHS contract action that searches specific data elements reported on DHS contract actions, and then prompts contracting officials if these data elements indicate that a contract action should, or should not, include the employment eligibility verification identifier in FPDS on each contract action. If there is a mismatch with the report criteria, the contracting official receives an email notification requesting that they check what was reported in FPDS to ensure the data is correct.

To supplement these actions, OCPO will issue an Acquisition Alert to Heads of the Contracting Activities to reiterate the FAR requirements to insert the clause 52.222-54 in solicitations and contracts when required, and to properly code the contract actions in FPDS. Estimated Completion Date (ECD): January 31, 2024.

⁴https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.acquisition.gov%2Fsites%2Fdefault%2Ffiles%2Fpage_file_uploads%2FE-Verify%2520final_ppts&wdOrigin=BROWSELINK

GAO recommended that the Director of USCIS:

Recommendation 6: Identify and implement an approach to collect quality information on federal contractors enrolled in E-Verify for the purpose of helping agencies monitor contractor compliance, such as by collecting Unique Entity Identifiers from federal contractors with existing E-Verify accounts.

Response: Concur. In August 2022, the USCIS E-Verify program started collecting Unique Entity Identifiers (UEI) for enrolled employers that identify as federal contractors with the FAR 52.222-54 clause, and updated behavior reports to identify such employers who do not have their UEI number recorded in E-Verify. However, this information collection is currently an optional field, as E-Verify does not have authorization to require E-Verify enrollees to provide this information. To require this field, the agency must provide public notice of its intent to collect the information and receive Office of Management and Budget (OMB) approval, as required by the Paperwork Reduction Act, 44 United States Code § 3501 *et seq.*

The E-Verify program expects to finalize changes to its information collection, including the UEI, by December 31, 2024. Once USCIS receives OMB approval and issues a notice requiring the collection of the UEI for E-Verify enrolled and self-identified federal contractors with the FAR 52.222-54 clause, the E-Verify program will communicate with these contractors to instruct them to update their profile. E-Verify compliance staff will also analyze behavior reports to follow up with the federal contractors who have not completed the required field. ECD: June 30, 2025.

Recommendation 7: Develop and implement an approach to communicate quality information to agencies for the purpose of monitoring contractor compliance with E-Verify.

Response: Concur. Once the E-Verify program has completed work to collect UEIs from enrolled federal contractors by June 2025 as previously noted, they will begin creating and posting reports with relevant information for agencies for the purpose of monitoring contractor compliance with the FAR 52.222-54 clause. Coordinating through the DHS OCPO and the OMB's Office of Federal Procurement Policy, the USCIS Office of Contracting (OCON) will request the names and contact information of Federal Contracting Agencies' procurement subject matter experts who monitor compliance with the FAR clause. The E-Verify program will then communicate with procurement subject matter experts when reports have been posted to a web-based portal available to federal procurement officials, or other appropriate system, and the E-Verify program, in consultation with OCON, will disseminate relevant information regarding how to monitor contractor E-Verify compliance. ECD: June 30, 2025.

GAO recommended that the Secretary of Homeland Security:

Recommendation 8: Ensure that USCIS's Director takes steps to document and implement a process for referring federal contractors to a suspension or debarment official if USCIS terminates their E-Verify MOU.

Response: Concur. In August 2023, the E-Verify program updated its existing "Notice of Intent to Terminate" and "Final Termination" notice templates to include language notifying the employer of the suspension and debarment referral process for federal contractors with the FAR 52.222-54 clause should USCIS terminate their E-Verify MOU. In September 2023, the E-Verify program also drafted a standard operating procedure and referral template that refers self-identified federal contractors with the FAR 52.222-54 clause in one or more of their contracts whose MOU has been terminated to the USCIS Office of Contracting Suspension and Debarment Director (OCON SDD). The OCON SDD will analyze the E-Verify referral and supporting documentation, confirm the employer is a federal contractor, and will refer cases to the DHS Suspension and Debarment Official for action or use delegated authority to take appropriate action on these cases. Once this process is finalized by USCIS and DHS, all future E-Verify MOU terminations for federal contractors with the FAR 52.222-54 clause will follow this process. ECD: March 29, 2024.

Appendix IV: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

September 19, 2023

Tim DiNapoli
Managing Director, Contracting and
National Security Acquisitions
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Rebecca Gambler
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. DiNapoli and Ms. Gambler:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, **"FEDERAL CONTRACTING: Agencies Can Better Monitor E-Verify Compliance" (GAO-23-106219)**.

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Melanie Anne Egorin

Melanie Anne Egorin, PhD
Assistant Secretary for Legislation

Attachment

**GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN
SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT
REPORT ENTITLED - FEDERAL CONTRACTING: AGENCIES CAN BETTER
MONITOR E-VERIFY COMPLIANCE (GAO-23-106219)**

The U. S. Department of Health and Human Services (HHS) appreciates the opportunity to review and provide comments on the Government Accountability Office's (GAO) draft report.

Recommendation

The Secretary of Health and Human Services should ensure that HHS's Deputy Assistant Secretary for Acquisitions takes steps to ensure that contracting staff correctly select the Employment Eligibility Verification response in FPDS for applicable contracts and orders.

HHS Response

HHS concurs with the GAO recommendation.

The Office of Acquisition (OA) will issue guidance/and or conduct training to ensure that HHS Contracting Officers are correctly coding the Employment Eligibility Verification response in FPDS for applicable contracts and orders. Additionally, OA will review FPDS reporting and coordinate with OPDIVs and STAFDIVs to verify that Contracting Officers correctly select the Employment Eligibility Verification response in FPDS for applicable contracts and orders. This supplemental review and verification will be conducted quarterly in fiscal year 2024.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Timothy J. DiNapoli, (202) 512-4841 or dinapolit@gao.gov
Rebecca Gambler, (202) 512-8777 or gablerr@gao.gov

Staff Acknowledgments

In addition to the contacts named above, the following staff members made key contributions to this report: Marie A. Mak (Director), Janet McKelvey (Assistant Director), Ashley Davis (Assistant Director), Jeff Hartnett (Analyst-in-Charge), Matthew T. Crosby, Michele Fejfar, Suellen Foth, Kelsey Griffiths, Tonya Humiston, Sasan J. “Jon” Najmi, William Reed, Edward J. SanFilippo, and Christopher D. Wolf.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.



November 2023

DEPARTMENT OF HOMELAND SECURITY

Reporting on Border Security Metrics Could Be Improved

GAO Highlights

Highlights of [GAO-24-106277](#), a report to congressional committees

Why GAO Did This Study

The U.S. has approximately 6,000 miles of land borders, 95,000 miles of coastline, and more than 300 ports of entry where travelers and cargo are inspected. Securing U.S. border areas is a key part of DHS's mission. Its ability to measure border security activities is essential to managing its responsibilities effectively.

The 2017 NDAA requires DHS to report annually on 43 border security metrics. The act also includes a provision for GAO, within 270 days of receipt of the first report and biennially for the following 10 years, to review and report on DHS's report.

GAO issued its initial report in March 2019. This third report evaluates DHS's 2021 *Border Security Metrics Report* compared to its 2019 report. Specifically, this report assesses DHS's 2021 report for (1) progress since 2019 in reporting the metrics outlined in the 2017 NDAA and engagement with its components and Congress on the report, and (2) efforts to improve the quality of information in DHS's 2021 report. To do this, GAO assessed the methodology and data in DHS's report, analyzed DHS's use of statistical models, and interviewed officials from DHS offices and components involved in developing the metrics.

What GAO Recommends

GAO is making four recommendations, including that DHS engage with components and Congress to more fully report border security metrics; assess its statistical model of deterrence; and update the model, as appropriate. DHS concurred with these recommendations.

View [GAO-24-106277](#). For more information, contact Rebecca Gambler at (202) 512-8777 or GamblerR@gao.gov.

November 2023

DEPARTMENT OF HOMELAND SECURITY

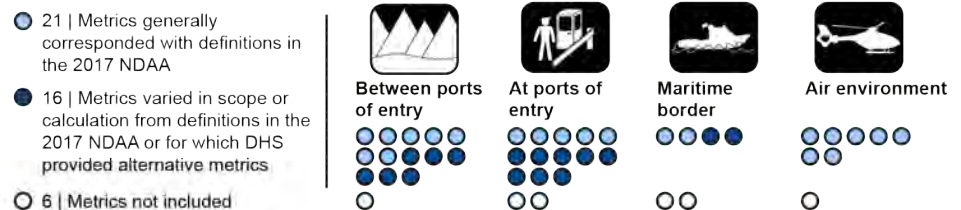
Reporting on Border Security Metrics Could Be Improved

What GAO Found

The National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA) requires the Department of Homeland Security (DHS) to develop an annual report containing 43 specific metrics to measure the effectiveness of border security. In its 2021 *Border Security Metrics Report*, DHS reported on 37 of 43 metrics, the same set of metrics in DHS's 2019 report. As shown below, GAO found that 21 of the 37 metrics in the 2021 report generally corresponded with their definitions in the 2017 NDAA—three more than in its 2019 report.

Department of Homeland Security's (DHS) Reporting on the 43 Metrics Required by the National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA)

Metrics included in DHS's 2021 *Border Security Metrics Report* by domain



Source: GAO analysis of DHS's 2021 *Border Security Metrics Report*, GAO icons. | GAO-24-106277

DHS may be missing opportunities to fully report the metrics and improve the usefulness of the report. DHS components collect the data that underlie the metrics, but GAO found that in some cases, DHS did not fully report available data. For example, DHS reported data on passenger inspections, but did not report available data on cargo and commercial traffic, as outlined in the 2017 NDAA. By engaging with DHS components that collect relevant data, DHS could more fully report the metrics as defined by the 2017 NDAA. Additionally, DHS did not generally provide periodic briefings to Congress to help refine its metrics reporting, as its 2021 report states it would do. GAO identified instances where such engagement could help DHS identify next steps and address challenges it has faced reporting metrics. Such engagement could also help DHS ensure the information it reports is useful to Congress.

DHS improved the quality of some information in its 2021 report by implementing a prior GAO recommendation to include measures of statistical uncertainty for all metrics that rely on its statistical model. Implementing GAO's remaining prior recommendations to develop and implement a process to systematically review the reliability of data and then communicating relevant limitations would position DHS to maximize the quality of information. It would also provide Congress and the public with contextual information needed to evaluate the metrics.

DHS uses a statistical model of deterrence—the rate at which individuals who are apprehended attempting to cross the border decide not to make another attempt—to report three metrics related to unlawful entries. GAO found that DHS did not assess and update its deterrence model between when it was developed in 2016 and the 2021 report. However, DHS data show that aspects of the population of individuals attempting to unlawfully cross the border have changed, including by volume and country of origin. Those changes increase the risk that the deterrence model is no longer as reflective of current border conditions.

Contents

Letter		1
	Background	6
	DHS Made Limited Progress Reporting Required Metrics and Did Not Fully Engage Components or Congress	11
	DHS Improved the Quality of Some Information in Its 2021 Report but Has Not Fully Assessed Its Deterrence Model or Identified Limitations for Reported Metrics	25
	Conclusions	38
	Recommendations for Executive Action	38
	Agency Comments and Our Evaluation	39
Appendix I	Other Metrics for Measuring the Effectiveness of Border Security	40
Appendix II	Border Security Metrics as Defined in the National Defense Authorization Act for Fiscal Year 2017	48
Appendix III	Comments from the Department of Homeland Security	57
Appendix IV	GAO Contact and Staff Acknowledgments	61
Tables		
	Table 1: Examples of Border Security Metrics by Domain and Department of Homeland Security (DHS) Component	7
	Table 2: Metrics in the 2021 and 2019 <i>Border Security Metrics Reports</i> (BSMR) and Their Correspondence with the Fiscal Year (FY) 2017 NDAA	12
	Table 3: Border Security Metrics in the 2021 <i>Border Security Metrics Report</i> That Generally Corresponded with Their Definitions in the National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA)	13
	Table 4: Factors Contributing to Differences between Metrics in the 2021 <i>Border Security Metrics Report</i> and Their Definitions in the National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA)	15

Table 5: Six Metrics the Department of Homeland Security (DHS) Omitted from its 2021 <i>Border Security Metrics Report</i> (report)	17
Table 6: Timing of <i>Border Security Metrics Reports</i> Issued Pursuant to the National Defense Authorization Act for Fiscal Year (FY) 2017, as of July 2023	24
Table 7: Other Metrics the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security Between Ports of Entry	41
Table 8: Other Metrics the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security at Ports of Entry	44
Table 9: Other Metric the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security at the Maritime Border	46
Table 10: Other Metric the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security in the Air Environment	47

Figures

Figure 1: Number and Type of Metrics Included in the Department of Homeland Security's (DHS) 2021 <i>Border Security Metrics Report</i>	9
Figure 2: Framework for the Department of Homeland Security's (DHS) Statistical Model for Unlawful Entry Metrics	27
Figure 3: Model the Department of Homeland Security (DHS) Uses to Estimate a Deterrence Rate	30

Abbreviations

AMO	Air and Marine Operations
CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
IDA	Institute for Defense Analyses
2017 NDAA	National Defense Authorization Act for Fiscal Year 2017
OFO	Office of Field Operations
OIS	Office of Immigration Statistics

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product 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.



November 13, 2023

The Honorable Gary C. Peters
Chairman
The Honorable Rand Paul, M.D.
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Mark E. Green, M.D.
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

Securing the nation's borders against illegal entries, smuggling of drugs and contraband, and terrorist activities is a key part of the Department of Homeland Security's (DHS) mission. According to DHS, the U.S. has approximately 6,000 miles of land borders, 95,000 miles of coastline, and 328 ports of entry.¹ DHS's ability to measure border security inputs, outputs, and outcomes is essential for the department to make evidence-based decisions about resource allocation and manage its border security responsibilities effectively. In our prior work, we have reported on the need for DHS to improve its measures for assessing its border security efforts.²

The National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA) requires DHS to develop an annual report containing 43 specific metrics to measure the effectiveness of border security between ports of entry, at ports of entry, at the maritime border, and with respect to the air

¹Ports of entry are officially designated facilities (seaports, airports or land border locations) that provide for the controlled entry into, or departure from, the U.S.

²See, for example, GAO, *Northern Border Security: CBP Identified Resource Challenges but Needs Performance Measures to Assess Security Between Ports of Entry*, [GAO-19-470](#) (Washington, D.C.: June 26, 2019); and *Coast Guard: Actions Needed to Enhance Performance Information Transparency and Monitoring*, [GAO-18-13](#) (Washington, D.C.: Oct. 27, 2017).

environment.³ These metrics span several DHS components, and the law requires DHS to consult with the heads of appropriate DHS components and to ensure that it uses authoritative sources to develop the metrics.⁴ DHS is required to provide the report to the appropriate congressional committees and the Comptroller General. As of October 2023, DHS has issued six *Border Security Metrics Reports* in response to the 2017 NDAA reporting requirement. This report focuses on DHS's fifth report, the 2021 *Border Security Metrics Report*, which DHS issued in April 2022.⁵

In addition, the 2017 NDAA includes a provision for us to analyze the suitability and statistical validity of the data and methodology in DHS's first report and complete biennial reviews for the following 10 years.⁶ As part of our review, we are to, as appropriate, include recommendations on improvements needed to the metrics and the feasibility of other suitable metrics. We met the requirement to issue our first assessment of DHS's first report in March 2019.⁷ We found that DHS reported on 35 of the 43 metrics called for by the NDAA and generally used quality information in those metrics, but did not identify some data limitations. We made four recommendations to improve the quality of the information presented in the *Border Security Metrics Report*. DHS agreed with our recommendations.

³Pub. L. No. 114-328, div. A, title X, subtitle G, § 1092, 130 Stat. 2000, 2429-36 (2016) (classified at 6 U.S.C. § 223). In particular, see 6 U.S.C. § 223(b), (c), (d), (e). The 2017 NDAA refers to the fourth domain (air environment) as "Air and Marine security metrics in the land domain," which it defines as aviation assets and operations of Air and Marine Operations. 6 U.S.C. § 223(e).

⁴DHS is also required to consult or work with other relevant agencies, as appropriate.

⁵Department of Homeland Security, *Border Security Metrics Report: 2021* (Washington, D.C.: Apr. 27, 2022). The 2021 report responds to the reporting requirement for fiscal year 2021 and contains data through fiscal year 2020. In prior *Border Security Metrics Reports*, DHS used "fiscal year" to refer to the report, but did not do so for the 2021 report. For the purposes of this report, we refer to all *Border Security Metrics Reports* by the year indicated by DHS in the title.

⁶6 U.S.C. § 223(g)(2). This provision requires that GAO conduct a review and submit a report to Congress within 270 days of receipt of DHS's first report, and biennially for the following 10 years with respect to every other DHS report.

⁷GAO, *Border Security: DHS Should Improve the Quality of Unlawful Border Entry Information and Other Metric Reporting*, [GAO-19-305](#) (Washington, D.C.: Mar. 21, 2019).

We issued our second assessment of DHS's third report (known as the 2019 report) in November 2021.⁸ We found that DHS had implemented one of our recommendations by conveying the sensitivity of key assumptions for the statistical model it uses to calculate certain metrics, but had not yet implemented our other three recommendations. We discuss the status of DHS's actions to address our recommendations later in this report.

This report assesses DHS's 2021 *Border Security Metrics Report* compared to its 2019 report.⁹ Specifically, it assesses DHS's 2021 report for (1) progress since 2019 in reporting the metrics as outlined in the 2017 NDAA and engaging with its components and Congress, and (2) efforts to improve the quality of information. This report also provides information on other metrics we have identified in our reports since 2021 that may be used to measure the effectiveness of border security. Appendix I contains a description of these other metrics.

To address our first objective on DHS's progress since 2019 in reporting the metrics as outlined in the 2017 NDAA in its 2021 *Border Security Metrics Report*, we compared DHS's 2021 report to its 2019 report. We compared information in these two DHS reports.¹⁰ Through this comparison, we identified the metrics that DHS included and omitted from each report and how they had changed since the 2019 report. For metrics DHS included in its 2021 report, we identified key differences in the scope or methodology from the 2019 report. Further, we assessed how the metrics DHS included were similar to, or different from (i.e., corresponded to), the metrics as defined in the 2017 NDAA. As part of this assessment, we leveraged information from our prior assessment of DHS's 2019 report.¹¹ Where we identified changes to the scope or methodology of the reported metrics or clear differences between the metrics DHS reported and those defined in the NDAA, we obtained perspectives from DHS officials to determine the reasons.

⁸GAO, *Border Security Metrics: Progress Made, but DHS Should Take Additional Steps to Improve Information Quality*, [GAO-22-104651](#) (Washington, D.C.: Nov. 16, 2021).

⁹This report does not assess DHS's 2022 *Border Security Metrics Report*, which the department issued in July 2023.

¹⁰To identify any additional changes that may have occurred in the 2020 *Border Security Metrics Report*, but not the 2021 report, we also reviewed the 2020 report.

¹¹[GAO-22-104651](#).

Additionally, we analyzed documentation and interviewed DHS officials regarding their efforts to improve the reporting of metrics as outlined in the 2017 NDAA, including through engagement with DHS components and Congress. We interviewed U.S. Customs and Border Protection (CBP) officials and reviewed documentation to obtain information on a possible alternative approach that DHS is considering to model unobserved events and report unlawful entry metrics.¹² To assess engagement with DHS components, we interviewed officials from the Office of Immigration Statistics (OIS), CBP, and the U.S. Coast Guard.¹³ As part of these interviews, we sought to understand the extent of their communication while developing the *Border Security Metrics Report*.

To further understand the engagement that officials described, we analyzed how OIS communicated with CBP to request data for the 2021 *Border Security Metrics Report*. We assessed this information against OIS's most recent strategic plan and 2017 NDAA requirements to understand OIS's role in developing the report.¹⁴ To assess DHS's engagement with Congress, we analyzed documentation from DHS to Congress regarding the *Border Security Metrics Report*, spoke with congressional staff, and interviewed DHS officials on the extent they held briefings with Congress. We further compared this information against the 2021 *Border Security Metrics Report*, DHS's directive on information quality, and guidance implementing that directive.¹⁵ In addition, we compared this information against the principle related to using quality information in *Standards for Internal Control in the Federal Government*.¹⁶

To address our second objective on DHS's efforts to improve the quality of information used in its metrics, we first compared information on the

¹²Some of the metrics required by the 2017 NDAA necessitate advanced statistical methods because they involve estimating unobserved events, such as the number of undetected unlawful entries. These include certain metrics related to unlawful entries between ports of entry that we discuss later in this report.

¹³We interviewed CBP officials from the Office of Field Operations, Air and Marine Operations, and U.S. Border Patrol.

¹⁴U.S. Department of Homeland Security, Office of Policy, Office of Immigration Statistics, *Strategic Plan Fiscal Years 2016-2020* (Sept. 2016). Pub. L. No. 114-328, § 1092, 130 Stat. at 2429-36 (classified at 6 U.S.C. § 223).

¹⁵Department of Homeland Security, *Information Quality*, Directive 139-02 (Washington, D.C.: Nov. 21, 2019); and *Information Quality Implementation*, Instruction 139-02-001 (Washington, D.C.: Nov. 27, 2019).

¹⁶*Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

unlawful entry metrics in the 2021 *Border Security Metrics Report* to the 2019 report. We analyzed changes to information related to the statistical model DHS used to estimate these metrics and interviewed OIS officials regarding the changes. Based on our analysis, we assessed DHS's progress in implementing the recommendation from our March 2019 report related to conveying statistical uncertainty of the unlawful entry metrics.¹⁷

Additionally, we analyzed the code files underlying a separate statistical model from the one described above.¹⁸ DHS uses this model to estimate a deterrence rate, which the department's broader statistical model for estimating unlawful entry metrics requires. We identified changes DHS made to the code it used for the 2021 *Border Security Metrics Report*. We interviewed OIS and CBP officials to obtain information on their efforts to assess, update, or replace the deterrence model. We compared this information to statistical principles and our key practices on artificial intelligence, which includes predictive statistical modeling.¹⁹ We also compared this information to documentation requirements of internal control standards and the principle related to management identifying information requirements through an iterative process in *Standards for Internal Control in the Federal Government*.²⁰

Further, we updated the assessments about the quality of information that we made in our March 2019 and November 2021 reports. Specifically, we identified the metrics for which DHS used different methodologies or data sources in the 2021 *Border Security Metrics Report* compared with the 2019 report. For metrics that used different methodologies or data sources, we collected information from DHS to determine what processes are in place to ensure the overall reliability and quality of the information reported. Additionally, we conducted interviews with DHS headquarters officials from OIS and DHS component officials from CBP—including the Office of Field Operations (OFO), Air and Marine Operations (AMO), and U.S. Border Patrol—as well as the Coast Guard. In these interviews, we obtained information about any changes made to the methodology or

¹⁷[GAO-19-305](#).

¹⁸DHS refers to this model as its deterrence model.

¹⁹Gareth James, et al., *An Introduction to Statistical Learning: with Applications in R*, 2nd ed. (New York: Springer, 2021), 29-37.; GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, [GAO-21-519SP](#) (Washington, D.C.: June 30, 2021).

²⁰[GAO-14-704G](#).

data collection that would affect how DHS reported the metrics. During our interviews with OIS officials, we also obtained information on steps OIS takes to assess the reliability of data included in the report and to identify relevant limitations. We analyzed this information to assess DHS's progress in addressing the recommendations we made in our March 2019 report.²¹

To identify other metrics that may be used to measure border security effectiveness, we reviewed border security-related reports that we and DHS's Office of Inspector General issued from October 2021 to September 2023.²² We also obtained information on the status of recommendations we previously identified in our March 2019 and November 2021 reports.

We conducted this performance audit from October 2022 to November 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

DHS Components with Responsibilities Related to Border Security

Within DHS, CBP and the Coast Guard have the primary responsibility for border security. CBP and its subcomponents are charged with securing U.S. borders at and between ports of entry by preventing inadmissible people and illicit goods from entering the U.S., among other responsibilities. Within CBP, the primary offices and components involved in border security are OFO at ports of entry, Border Patrol between ports of entry, and AMO for air and marine security. The Coast Guard and

²¹These recommendations related to developing and implementing a process to systematically review the reliability of metric data and identify and communicate limitations of the metrics. [GAO-19-305](#).

²²We selected this time period to update the information in our March 2019 and November 2021 reports, which identified relevant metrics we and the DHS Office of Inspector General recommended in reports issued from August 2009 through September 2021. [GAO-19-305](#) and [GAO-22-104651](#). For the purpose of this report, we reviewed 28 reports from our prior work and 73 DHS Office of Inspector General reports.

CBP's AMO share responsibility for security of the nation's maritime borders.

Border Security Metrics

DHS's Office of Immigration Statistics (OIS), within the Office of Strategy, Policy, and Plans, is responsible for developing DHS's annual report on the 43 metrics as required by the 2017 NDAA.²³ To prepare the report, OIS officials stated that they obtained data and information related to each NDAA metric from the administrative records of the DHS components with primary responsibilities for border security in the four domains. Table 1 shows examples of border security metrics by domain and the DHS components that collect the associated data.

Table 1: Examples of Border Security Metrics by Domain and Department of Homeland Security (DHS) Component

Domain	Relevant DHS component	Example of a metric
Between ports of entry	U.S. Customs and Border Protection (CBP) and U.S. Border Patrol	The number of apprehensions in each Border Patrol sector ^a
At ports of entry	CBP Office of Field Operations	A secondary examination rate that measures the frequency of secondary examinations at each land port of entry ^b
Maritime border	U.S. Coast Guard and CBP Air and Marine Operations (AMO)	The rate at which illicit drugs are removed by DHS maritime security components
Air environment ^c	CBP AMO	The number of missions cancelled by AMO due to weather compared with the total planned missions

Source: GAO analysis of DHS 2021 *Border Security Metrics Report*. | GAO-24-106277

^aBorder Patrol divides responsibility for border security operations geographically among 20 sectors, each with its own sector headquarters. Each sector is further divided into varying numbers of stations, each with its own area of responsibility. There are nine sectors along the southwest border, eight along the northern border, and three in the Gulf Coast and Caribbean regions.

^bA secondary examination is when a CBP officer at a port of entry refers a traveler to a separate area, outside the primary inspection area, to complete the inspection or examination process without causing delays for other travelers. Reasons why a traveler may be referred for a secondary examination include, for example, when the CBP officer cannot verify a traveler's information or a traveler does not have all the required documentation.

^cThe National Defense Authorization Act for Fiscal Year 2017 refers to this domain as "Air and Marine security metrics in the land domain," which it defines as aviation assets and operations of AMO. 6 U.S.C. § 223(e).

The 2017 NDAA defined the required border security metrics, which include a mix of counts, rates, estimates, or a combination of these types

²³In 2022, DHS established the Office of Homeland Security Statistics, which will subsume the Office of Immigration Statistics. According to DHS, this new office will expand over time to conduct independent reporting and analysis on all DHS statistical data. DHS officials stated that, as of July 2023, DHS plans to finish standing up the Office of Homeland Security Statistics in late September 2023.

of metrics, spanning each of the four border domains.²⁴ For example, the NDAA defined one metric, a count, as the number of apprehensions in each Border Patrol sector.²⁵ For some metrics, the NDAA defined them as rates compared to the last 5 years, such as rates at which illicit drugs were seized compared to the average over the last 5 years at ports of entry and between ports of entry.²⁶ The NDAA also requires an estimate of the number of undetected unlawful entries, as well as several metrics the law defined as a combination of observed data and estimates. For example, one of these combination metrics is the cocaine seizure effectiveness rate at ports of entry. This combination metric divides the amount of cocaine seizures at ports of entry—a known quantity—by an estimate of total cocaine flow through ports of entry, which cannot be directly measured.²⁷

The 2017 NDAA did not specifically define three of the 43 metrics. For example, while the NDAA called for an examination of each consequence under the Consequence Delivery System, it did not specify how the examination is to be carried out or what it should include.²⁸ We provide descriptions for all of the metrics in appendix II. Figure 1 shows the number of metrics required by the 2017 NDAA that DHS did and did not include in its 2021 *Border Security Metrics Report* by type of metric.

²⁴See 6 U.S.C. § 223. Rate metrics compare one value or number against another. Estimates measure activities that are largely undetected and, therefore, cannot be measured directly. We refer to metrics that are comprised of a count or a rate and use an estimate as part of their computation as “combination metrics.”

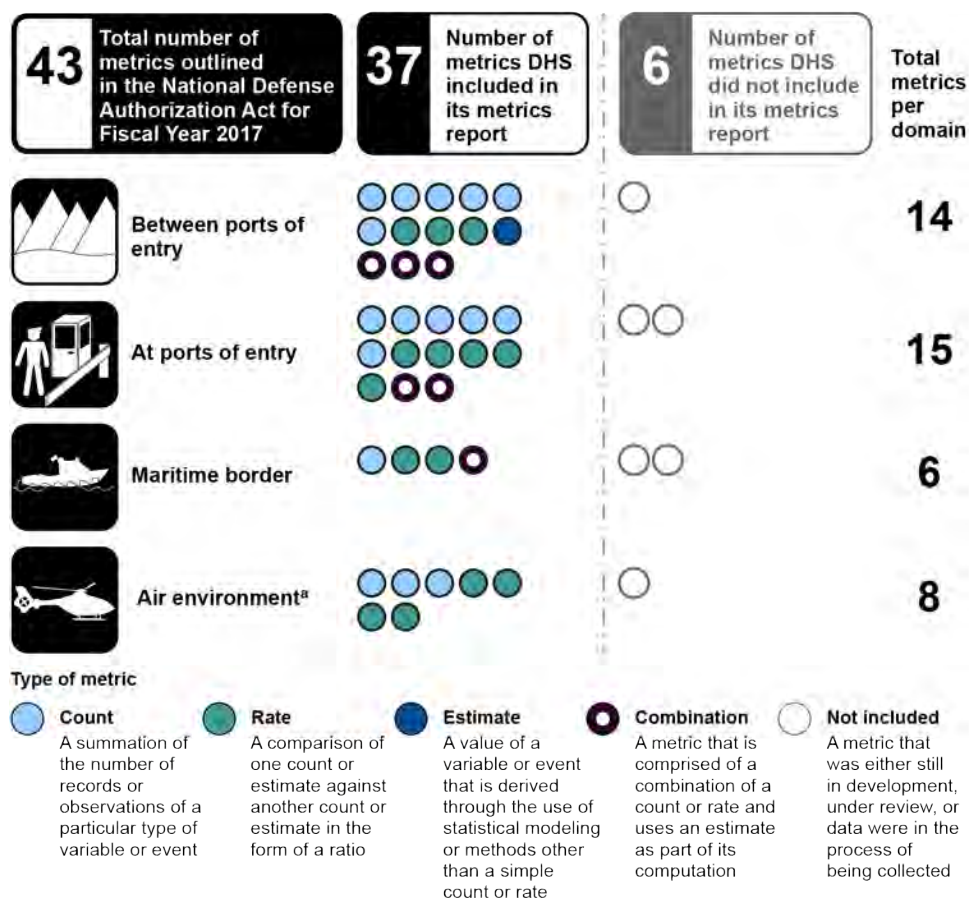
²⁵6 U.S.C. § 223(b)(1)(E).

²⁶6 U.S.C. § 223(b)(1)(H), (c)(1)(C).

²⁷6 U.S.C. § 223(c)(1)(E). Another combination metric is the unlawful border crossing effectiveness rate—the percentage that results from dividing the number of apprehensions and turn backs by the sum of the number of apprehensions, estimated undetected unlawful entries, turn backs, and got aways—in each U.S. Border Patrol sector. *Id.* at § 223(b)(1)(C).

²⁸6 U.S.C. § 223(b)(1)(J). The Consequence Delivery System refers to the series of consequences applied by Border Patrol in collaboration with other federal agencies to persons unlawfully entering the U.S. in order to prevent unlawful border-crossing recidivism. *Id.* at § 223(a)(2).

Figure 1: Number and Type of Metrics Included in the Department of Homeland Security's (DHS) 2021 *Border Security Metrics Report*



Source: GAO analysis of DHS's 2021 *Border Security Metrics Report*, GAO icons. | GAO-24-106277

^aThe National Defense Authorization Act for Fiscal Year 2017 refers to this domain as "Air and Marine security metrics in the land domain," which it defines as aviation assets and operations of AMO. 6 U.S.C. § 223(e).

OIS calculates or estimates many of the metrics required by the 2017 NDAA using data provided by the components, but certain metrics require advanced statistical methods and technical expertise. For example, DHS uses a statistical model to estimate undetected unlawful entries. In the model, DHS focuses on individuals who unlawfully cross the border, are apprehended by Border Patrol, and then removed from the country across the U.S.-Mexico border, and attempt to cross the border again. In our March 2019 assessment of DHS's first *Border Security Metrics Report*, we reported that DHS did not validate all of the assumptions it

used to develop the model.²⁹ We recommended that DHS conduct an analysis of how changing the assumptions might affect the accuracy of the model—a process known as sensitivity analysis. To address this recommendation, DHS conducted a sensitivity analysis and published the results in the 2019 *Border Security Metrics Report*. This sensitivity analysis will allow Congress, policymakers, and the public to better understand potential limitations of DHS’s statistical model and more fully evaluate the validity of the border security metrics derived from the model.

DHS’s Use of Border Security Metrics

In addition to reporting metrics in response to 2017 NDAA requirements, DHS officials use some of the metrics reported in the *Border Security Metrics Report*, or conceptually similar measures, as DHS GPRA Modernization Act of 2010 performance measures.³⁰ For example, *DHS’s Annual Performance Report for Fiscal Years 2021–2023* includes a measure of migrant interdiction effectiveness in the maritime environment—a measure that DHS also reported in the 2021 *Border Security Metrics Report*.

Additionally, CBP officials told us they use the metrics in the *Border Security Metrics Report* to inform component decision-making and operational understanding. For example, Border Patrol officials stated that certain metrics, such as the number of apprehensions, “got aways”, and “turn backs”, collectively provide a picture of the current state of the northern and southwest border.³¹ These officials told us they look at the metrics to understand the success of Border Patrol’s tactical approach and shift resources as needed. AMO officials told us that the metric on the AMO readiness rate helps officials to understand when issues other

²⁹[GAO-19-305](#).

³⁰The Government Performance and Results Act of 1993 (GPRA), as updated and expanded by the GPRA Modernization Act of 2010 (GPRAMA), requires agencies to establish annual performance goals with target levels of performance to measure progress toward those goals. See Pub. L. No. 111-352, 124 Stat. 3866 (2011) (updating Pub. L. No. 103-62, 107 Stat. 285 (1993)).

³¹The 2017 NDAA defines “got aways” as individuals who are directly or indirectly observed entering unlawfully, are not apprehended, and are not turn backs. See 6 U.S.C. § 223(a)(3). The 2017 NDAA defines “turn backs” as individuals who, after making an unlawful entry into the U.S., respond to U.S. enforcement efforts by returning promptly to the country from which they entered. *Id.* at § 223(a)(9).

than weather, such as personnel issues, may have contributed to a cancelled aviation mission.³²

DHS Made Limited Progress Reporting Required Metrics and Did Not Fully Engage Components or Congress

DHS Reported Three More Metrics That Correspond with Their NDAA Definitions Since Its 2019 Report

DHS made limited progress toward reporting all of the metrics required by the 2017 NDAA since the 2019 *Border Security Metrics Report*. In the 2021 *Border Security Metrics Report*, DHS reported 37 of the 43 metrics required by the NDAA. The set of metrics included in the 2021 report did not change since the 2019 report and DHS's reporting on some metrics improved.³³ Specifically, DHS reported three of the metrics in the 2021 report such that they corresponded with their definitions in the NDAA; in the 2019 report, these metrics did not correspond with those definitions.³⁴ In addition, two metrics DHS reported in the 2021 report more closely corresponded with their NDAA definitions than in the 2019 report, but

³²As defined by the 2017 NDAA, the AMO readiness rate compares the number of aviation missions flown by AMO to the number of aviation missions cancelled by AMO due to maintenance, operations, or other causes. 6 U.S.C. § 223(e)(1)(C).

³³In November 2021, we reported on the number of metrics DHS included in its 2019 *Border Security Metrics Report*. [GAO-22-104651](#).

³⁴For the purposes of this report, we use the word "correspond" to describe how the metrics DHS included in its 2021 *Border Security Metrics Report* were similar to, or different from, their definitions in the 2017 NDAA.

these metrics still differed from their NDAA definitions.³⁵ As a result, 21 of the 37 reported metrics generally corresponded with their NDAA definitions in the 2021 report, compared to 18 of the 37 metrics in the 2019 *Border Security Metrics Report*, as shown in table 2.

Table 2: Metrics in the 2021 and 2019 *Border Security Metrics Reports* (BSMR) and Their Correspondence with the Fiscal Year (FY) 2017 NDAA

Correspondence of reported metrics with definitions in FY 2017 NDAA	2021 BSMR	2019 BSMR
Metric generally corresponds with definition in the NDAA	21	18
Metric differs from definition in NDAA because:		
• it uses a different scope or calculation	15 ^a	18
• Department of Homeland Security provided an alternative measure to what is defined in the NDAA	1	1

Source: GAO analysis of Department of Homeland Security 2021 *Border Security Metrics Report*. | GAO-24-106277

Note: FY 2017 NDAA = The National Defense Authorization Act for Fiscal Year 2017.

^aTwo of these metrics, related to apprehensions and nationality of family units and unaccompanied children, more closely corresponded with their definitions in the NDAA, but still differed.

The 21 metrics that generally corresponded with their definitions spanned each of the four border domains. For example, in the between ports of entry domain, DHS reported the number of apprehensions of individuals attempting to unlawfully cross the border for each border sector, as required by the law.³⁶ Also within this domain, in prior *Border Security Metrics Reports* DHS presented three metrics related to unlawful entries—(1) detected unlawful entries, (2) turn backs, and (3) got

³⁵For the two metrics that more closely corresponded to the NDAA definition, apprehensions of family units and apprehensions of unaccompanied children, DHS provided data on the southern, northern, and coastal borders in the 2021 report but did not report the northern and coastal borders by border sector as specified in the 2017 NDAA. For the apprehension of unaccompanied children metric, the statute uses the term “unaccompanied alien child”. See 6 U.S.C. §§ 223(b)(1)(F), 279(g)(2). DHS also provided data on the number of family units and unaccompanied children expelled under Title 42, along with the apprehensions in each border patrol sector metric. In March 2020, CBP began to assist the Centers for Disease Control and Prevention in the enforcement of a series of public health orders issued under Title 42 of the U.S. code, and thus processed and expelled certain noncitizens under this public health authority, rather than processing them under Title 8 immigration enforcement and removal authority. Title 8 refers to the title of the U.S. Code that pertains to immigration and nationality. Title 42 refers to the title of the U.S. Code pertaining to public health and welfare. The expiration of the public health emergency at the end of May 11, 2023 caused the then-operative Title 42 order to end.

³⁶6 U.S.C. § 223(b)(1)(E).

aways—only for the southwest border.³⁷ Consistent with the NDAA requirement for reporting standardized data across all Border Patrol sectors for metrics within the between ports of entry domain, DHS included data for the northern and coastal borders in its 2021 report for these three metrics.³⁸ Table 3 lists the metrics that generally corresponded with their definitions in the NDAA by domain.

Table 3: Border Security Metrics in the 2021 *Border Security Metrics Report* That Generally Corresponded with Their Definitions in the National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA)

Domain	Metric ^a
Between ports of entry	Apprehensions in each U.S. Border Patrol sector
	Between ports of entry illicit drug seizure rate
	Detected unlawful entries ^b
	Estimates of the impact of the Consequence Delivery System on recidivism
	Examination of each consequence under the Consequence Delivery System
	Got aways ^{b,c}
	Turn backs ^{b,d}
At ports of entry	Illicit drugs seized at ports of entry
	Port of entry illicit drug seizure rate
	Average wait times and traffic volume
	Infrastructure capacity utilization rate
	Number of potentially “high-risk” cargo containers
Maritime border	Known maritime migrant flow rate
	Cocaine removal effectiveness rate
Air environment	Flight hour effectiveness rate
	Funded flight hour effectiveness rate
	Air and Marine Operations (AMO) readiness rate
	AMO weather-related cancellation rate
	AMO individuals detected
	AMO apprehensions assisted
	Illicit drug seizures assisted by AMO

Source: GAO analysis of Department of Homeland Security 2021 *Border Security Metrics Report*. | GAO-24-106277

³⁷As noted in the 2021 *Border Security Metrics Report*, previous versions of the table containing data on turn backs misreported total turn backs as being only turn backs at the southern border in some years.

³⁸6 U.S.C. § 223(b)(3). Data for between ports of entry shall be collected and reported in a consistent and standardized manner across all U.S. Border Patrol sectors, informed by situational awareness. The three other domains also have this requirement for the manner of collection. See 6 U.S.C. § 223(c)(3), (d)(3), (e)(3).

^aWe refer to the 43 metrics enumerated in the 2017 NDAA by the titles provided by DHS in the 2021 *Border Security Metrics Report*. See app. II for definitions and legal citations of all of the mandated metrics.

^bMetric newly corresponded with its NDAA definition since our previous review of the 2019 *Border Security Metrics Report*.

^cThe NDAA defines “got aways” as individuals who are directly or indirectly observed entering unlawfully, are not apprehended, and are not turn backs. See 6 U.S.C. § 223(a)(3).

^dThe NDAA defines “turn backs” as individuals who, after making an unlawful entry into the U.S., respond to U.S. enforcement efforts by returning promptly to the country from which they entered. 6 U.S.C. § 223(a)(9).

Sixteen of the metrics in the 2021 *Border Security Metrics Report* continued to differ from their definitions in the 2017 NDAA. A variety of factors contributed to these differences, such as DHS’s statistical model not calculating estimates with the needed granularity, DHS’s systems not maintaining data in the units of measurement required by the NDAA, and DHS not fully reporting available data, as shown in table 4. For example, although DHS included some information about apprehensions of family units and apprehensions of unaccompanied children at northern and coastal borders, it did not report those data for every border sector as required by the NDAA.³⁹ OIS officials told us they have this information, but the numbers for northern and coastal border sectors are very small, such that the tables for border sectors would mostly contain values of zero. In July 2023, OIS officials told us that they would consider summarizing the available data for the northern and coastal border sectors in the narrative section of future reports.

Another gap in the reported data relates to the secondary examination rate metric.⁴⁰ At a port of entry, a secondary examination takes place when a CBP officer refers individuals or vehicles for additional inspection, such as to verify documents or ask further questions. The 2021 *Border Security Metrics Report* included data for secondary examinations of passengers, but not data OFO maintains on cargo or commercial traffic. We further discuss this gap later in this report.

³⁹6 U.S.C. §§ 223(b)(1)(F), (G); 279(g)(2).

⁴⁰6 U.S.C. § 223(c)(1)(F)(iii).

Table 4: Factors Contributing to Differences between Metrics in the 2021 *Border Security Metrics Report* and Their Definitions in the National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA)

Factor	Metric that differed ^a
DHS bases metric in whole or in part on a statistical model that does not calculate estimates for the northern and coastal borders, which are to be included consistent with the 2017 NDAA.	Attempted unlawful border crosser apprehension rate
	Estimated undetected unlawful entries
	Probability of detection rate
	Unlawful border crossing effectiveness rate
DHS components collect data needed for metric, but DHS does not fully report available data.	Major infractions at ports of entry
	Secondary examination rate
	Apprehensions of unaccompanied children
	Apprehensions of family units
DHS's systems do not maintain data in the units of measurement required by the 2017 NDAA.	Potentially high-risk cargo containers scanned before arrival at a U.S. port of entry
	Potentially high-risk cargo containers scanned upon arrival at a U.S. port of entry
	Ratio of potentially high-risk cargo containers scanned relative to high-risk containers entering in previous fiscal year
DHS has not developed a means to estimate unknown inadmissible individuals who seek admission at U.S. ports of entry reliably, which is information department officials said it needs to report these metrics.	Refusal and interdiction rates at ports of entry
	Total inadmissible travelers at ports of entry
DHS relies on other federal agencies for cocaine flow estimates and there is not an estimate available for the share of the total cocaine flow through land ports of entry as required by the 2017 NDAA.	Cocaine seizure effectiveness rate
DHS reports data for drug removals by the Coast Guard only, because it has not yet validated data from other maritime security components, which the 2017 NDAA requires.	Illicit drugs removal rate
DHS provided an alternative measure.	Situational awareness achieved in the maritime environment

Source: GAO analysis of Department of Homeland Security (DHS) 2021 *Border Security Metrics Report* and interviews with DHS officials. | GAO-24-106277

^aWe refer to the 43 metrics enumerated in the 2017 NDAA by the titles provided by DHS in the 2021 *Border Security Metrics Report*.

In its 2021 *Border Security Metrics Report*, DHS continued not to report information on six required metrics that it has omitted from all of its prior reports. These six metrics spanned all four domains as shown in table 5 below.

According to the 2021 *Border Security Metrics Report* and agency officials, DHS has plans to include all six omitted metrics in future reports. In its 2022 *Border Security Metrics Report*, issued in July 2023, DHS reported on two of these metrics—the DHS known maritime threat response rate and a related metric, the intergovernmental actionable

maritime threat response rate.⁴¹ OIS officials stated that they focused on engaging with the Coast Guard to include information for these two metrics. According to Border Patrol and AMO officials, they are working towards reporting the two metrics in the between ports of entry and the air environment domains, respectively.

The remaining two metrics—the unlawful entries at ports of entry and the secondary examinations effectiveness rate—relate to the at ports of entry domain. DHS's 2021 and 2022 reports stated that DHS does not characterize secondary examinations as either effective or ineffective and thus cannot report on the secondary examinations effectiveness rate metric. OIS officials told us in July 2023 that, despite this challenge, OFO had provided OIS with information for both of the metrics in the at ports of entry domain, and OIS plans to report on them in the 2023 report. Table 5 describes DHS's rationale for omitting each of the six metrics and the reporting year DHS plans to include the metric or reported on the metric.

⁴¹As defined by the 2017 NDAA, the DHS known maritime threat response rate is a response rate that compares the ability of DHS maritime security components to respond to and resolve known maritime threats, whether inside or outside a transit zone, by placing assets on-scene, with the total number of events with respect to which the department has known threat information. 6 U.S.C § 223(d)(1)(E). The intergovernmental actionable maritime threat response rate is a response rate that compares the ability of the maritime security components of DHS or other U.S. government entities to respond to and resolve actionable maritime threats, whether inside or outside a transit zone, with the number of such threats detected. 6 U.S.C. § 223(a)(8), (d)(1)(F). The 2017 NDAA included a provision for us to review DHS's first *Border Security Metrics Report*, and biennially for the following 10 years with respect to every other DHS report, to review and report our findings to Congress. We will analyze the 2022 *Border Security Metrics Report* as part of a future review.

Table 5: Six Metrics the Department of Homeland Security (DHS) Omitted from its 2021 *Border Security Metrics Report* (report)

Domain	Metric omitted	DHS reported rationale for omitting metric	Reporting year DHS plans to include metric or reported on metric
Between ports of entry	A measurement of situational awareness achieved in each U.S. Border Patrol sector	The 2021 report states that Border Patrol is refining measures for this metric as part of a larger effort to measure performance and success in securing the border between ports of entry. Border Patrol officials told us they planned to complete these efforts by fiscal year 2024, and DHS tentatively plans to report on the metric in the 2024 report.	2024
At ports of entry	Unlawful entries at ports of entry	The 2021 report states that the Compliance Examination program is unable to reliably estimate successful unlawful entries due to the nature of the survey, including insufficient sample size. ^a According to the report, it is highly unlikely that DHS will ever be able to provide data for successful unlawful entries. Although DHS's 2022 report also noted this challenge, DHS officials told us they plan to provide information on this metric in the 2023 report.	2023
	Secondary examinations effectiveness rate	The 2021 report states that the U.S. Customs and Border Protection (CBP) does not categorize a given secondary examination as 'effective' or 'ineffective' and therefore, does not report on this metric. DHS officials told us they will continue to consider approaches to developing a secondary examination effectiveness rate. DHS officials told us they plan to provide information on this metric in the 2023 report.	2023
Maritime border	DHS maritime threat response rate	The 2021 report states that DHS has data on cocaine-response activities but not all maritime threats, and that DHS cannot separate DHS activities from intergovernmental data. DHS reported on this metric in the 2022 report, which it issued in July 2023. We will analyze the information DHS reported for this metric as part of a future review.	2022
	Intergovernmental maritime threat response rate	The 2021 report states that DHS has data on cocaine-response activities but not all maritime threats, and that DHS cannot separate DHS activities from intergovernmental data. DHS reported on this metric in the 2022 report, which it issued in July 2023. We will analyze the information DHS reported for this metric as part of a future review.	2022
Air environment ^b	Air and Marine Operations (AMO) actionable intelligence	AMO officials told us they are working to define this metric and quantify it in their system of record. The 2021 report states that AMO is in the process of creating a dashboard of historic data on sensor surveillance to help inform the development of this metric. AMO officials said the dashboard contains data on remotely piloted assets and information on how AMO used intelligence to inform targeting.	2024

Source: GAO analysis of DHS 2021 and 2022 *Border Security Metrics Reports* and interviews with DHS officials. | GAO-24-106277

Note: We refer to the 43 metrics listed in the National Defense Authorization Act for Fiscal Year 2017 by the titles provided by DHS in the 2021 *Border Security Metrics Report*.

^aThis program is a statistical survey in which vehicles cleared for entry into the U.S. by CBP are selected for a comprehensive audit through a computer-generated random sample. CBP is to conduct an audit of the selected vehicles by doing a secondary inspection, using a standardized system of checks to identify any violations that were missed during the routine inspection.

^bThe National Defense Authorization Act for Fiscal Year 2017 refers to this domain as "Air and Marine security metrics in the land domain," which it defines as aviation assets and operations of AMO. 6 U.S.C. § 223(e).

DHS's Policy Office
Obtains Data from
Components but Has Not
Engaged with Them to
More Fully Report Metrics
as Outlined in the NDAA

OIS—within DHS's Office of Strategy, Policy, and Plans—has engaged with components to obtain data for developing the *Border Security Metrics Report* and to encourage the future reporting of metrics it has previously omitted. In particular, OIS engaged with components by emailing them to obtain the latest data for the 2021 *Border Security Metrics Report*. However, for those metrics that do not fully correspond with their NDAA definition, OIS has not engaged with components to determine whether data and information are available that would help them improve their reporting on those metrics.

OIS's most recent strategic plan identifies OIS as the leader of DHS's effort to develop rigorous metrics of border security, including producing the *Border Security Metrics Report*.⁴² As part of this effort, the strategic plan states that OIS will engage with internal stakeholders, including DHS components, such as CBP and the Coast Guard. Although OIS is responsible for producing the *Border Security Metrics Report*, DHS components are responsible for collecting the data that underlie the metrics within the report. As such, engaging with DHS components is necessary for OIS to report on the 43 required metrics as outlined in the 2017 NDAA.

When preparing the annual *Border Security Metrics Report*, OIS engages components to request and receive updated data for metrics it has previously included in the report. We reviewed OIS's outreach to CBP for the 2021 *Border Security Metrics Report*, which included its outreach to Border Patrol, OFO, and AMO. To conduct this outreach, OIS emailed CBP its request for data, and asked that the components enter data from the most recent fiscal year in a template containing data tables OIS had included in the prior report.

While this outreach to components allowed OIS to obtain data on previously reported metrics, it was not thorough or comprehensive enough to ensure that OIS was aware of all available data or component

⁴²U.S. Department of Homeland Security, Office of Policy, Office of Immigration Statistics, *Strategic Plan Fiscal Years 2016-2020* (Sep. 2016). The strategic plan was operational in fiscal year 2020, which is the latest data included in the 2021 *Border Security Metrics Report*. In April 2023, OIS officials told us that the office drafted a new strategic plan, but paused its implementation as OIS transitions to the new Office of Homeland Security Statistics. According to a memo establishing this office, OIS leads official immigration reporting and has had the long-standing mission to disseminate high-quality information that is relevant and timely to inform policymakers, Congress, and the public about the effects of immigration in the U.S. OIS is also responsible for overseeing the analysis and reporting of all DHS statistical data. U.S. Department of Homeland Security, *Establishing an Office of Homeland Security Statistics* (July 25, 2022).

efforts to improve metric reporting. For example, OIS officials told the components that the office was repeating last year's report format and did not plan substantive updates beyond updating the report with the most recent year's data. Further, OIS did not ask any questions related to improving the reporting of metrics that continue to differ from, or did not correspond to, their definitions in the NDAA—as described above in table 4.

We found two specific instances where OIS missed an opportunity to engage with components to help previously reported metrics better correspond to their NDAA definitions. These instances consisted of opportunities where OIS could have engaged components to understand or provide input regarding: (1) available data for a reported metric, and (2) CBP's efforts to develop a statistical model.

- **Available data for a reported metric.** OIS did not actively engage with OFO to understand all available data to report on the secondary examination rate metric as defined in the 2017 NDAA.⁴³ In the 2021 *Border Security Metrics Report*, DHS's reporting on the secondary examination rate metric did not generally correspond with its definition in the 2017 NDAA. Specifically, the metric differed in scope. DHS reported data on the percentage of passengers subject to secondary inspection at each land port of entry, but did not report data on cargo or commercial traffic. However, according to OFO officials and documentation, OFO maintains data on secondary examinations of cargo and commercial traffic. OFO officials told us they had not provided these data to OIS for inclusion in the *Border Security Metrics Report* because officials were waiting for OIS's leadership to define what relevant data were needed to report information on the metric, such as cargo and commercial traffic. By not asking OFO officials about the availability of data on secondary examinations of cargo and commercial traffic, OIS is missing an opportunity to report the secondary examination rate metric as defined in the 2017 NDAA.
- **CBP's efforts to develop a statistical model.** DHS's current statistical model calculates estimates of unlawful entries for the entire southwest border. The model cannot provide estimates for each Border Patrol sector because DHS has not yet produced and validated such estimates. As a result, DHS's reporting of four metrics related to unlawful entries does not fully correspond with the metrics'

⁴³6 U.S.C. § 223(c)(1)(F)(iii).

definitions in the 2017 NDAA.⁴⁴ The NDAA calls for one of these metrics to include estimates for each Border Patrol sector and for all four metrics to include estimates for the southwest, northern, and coastal borders. Thus, these metrics differed in scope from their definitions in the NDAA. To improve the reporting of these and other border security metrics, CBP has been developing a different statistical model, called the Operational Performance Simulator, since 2017.⁴⁵ However, OIS has not actively engaged CBP to understand or provide input into its efforts to develop a statistical model that could improve the reporting of the four metrics related to unlawful entries.

OIS officials told us they have not taken an active role in the Operational Performance Simulator's development because they view it as CBP's responsibility. While CBP requested feedback from OIS on the model during a February 2023 briefing, OIS officials told us it is too early to know whether the model can be used to report sector-level estimates. Currently, the model can only report station-level estimates for the northern and southwestern borders. OIS officials said they expect CBP to reach out further for feedback as needed, but do not consider the model's development a priority for OIS. OIS's latest strategic plan specifically notes that OIS is to lead DHS's effort to develop estimates of unlawful entries. By not actively engaging with CBP on the model's development, OIS is missing opportunities to provide input that could improve the reporting of the four unlawful entry metrics.

OIS's prior efforts to elicit support from and engage with components in developing *Border Security Metrics Reports* yielded positive results. In particular, with support from a DHS component, OIS was able to report on previously omitted metrics, and thus strengthened the department's

⁴⁴These four metrics include: (1) the attempted unlawful border crosser apprehension rate, (2) the number of estimated undetected unlawful entries, (3) the probability of detection rate, and (4) the unlawful border crossing effectiveness rate. As defined by the NDAA, each of these metrics is an estimate or a combination metric that includes an estimate. In its 2021 report, DHS used its statistical model to report the first three metrics and observational data to report the fourth metric.

⁴⁵We have previously reported that DHS's current statistical model may not accurately reflect conditions at the southwest border because the model does not fully account for the changing population of unlawful border crossers. For example, the model excludes all individuals who are not Mexican nationals from the count of unlawful border crossers. [GAO-22-104651](#). DHS has previously referred to the Operational Performance Simulator as a model developed by the Johns Hopkins Applied Physics Laboratory. This model uses a combination of statistical modeling and data from sensors along the border to estimate the total number of unlawful border entries between land ports of entry, including entries both detected by Border Patrol and those not detected by Border Patrol.

reporting. For example, OIS and Coast Guard officials told us that engagement between them had been notable during the development of the 2022 report. According to Coast Guard officials, OIS reached out to them in September 2022 to request a proposal to develop these previously omitted metrics, which they submitted. As a result of such efforts, the most recently issued report includes two metrics that DHS had previously omitted.

OIS officials told us they have not undertaken similar engagement to more fully report the metrics that DHS already reports according to their 2017 NDAA definitions because components are ultimately responsible for determining what data and information to provide for the report. Component officials are also responsible for making decisions around developing alternative reporting methods, according to OIS officials. However, according to OIS's strategic plan, it is to lead the department's efforts to develop rigorous border security metrics, including through engagement with DHS components. By engaging with components, OIS could obtain information needed and guide relevant efforts to more fully report DHS border security metrics according to their 2017 NDAA definitions. Such engagement could include, for example, requesting relevant component data and providing input on component efforts to develop a statistical model.

DHS Has Not Periodically Engaged with Congress to Improve the Usefulness of Its Reports

DHS has documented that it will engage with Congress to refine its border security metrics reporting and ensure that the information it includes in its reports is useful to Congress. The 2021 *Border Security Metrics Report* states that, in addition to issuing the report, DHS will update Congress on its progress toward refining the metrics through periodic briefings. The report also states that DHS will continue to refine the metrics through external engagement and collaboration, including with Congress. Additionally, DHS Directive 139-02 on Information Quality requires DHS to ensure and maximize the utility of the information it disseminates to the public.⁴⁶ Guidance on implementing that directive states that DHS should consider the usefulness of the information to its intended users, which includes Congress.⁴⁷ One aspect of the usefulness of information in the report is its timeliness, and internal control standards

⁴⁶Department of Homeland Security, *Information Quality*, Directive 139-02 (Washington, D.C.: Nov. 21, 2019).

⁴⁷Department of Homeland Security, *Information Quality Implementation*, Instruction 139-02-001 (Washington, D.C.: Nov. 27, 2019).

note that quality information is to be timely.⁴⁸ However, OIS has not periodically engaged with Congress to improve its *Border Security Metrics Reports*.

During the course of our audit work, we identified instances where engaging with Congress could help DHS identify next steps and address challenges it has faced in fully reporting border security metrics as defined by the 2017 NDAA. For example, DHS did not include six metrics required by the NDAA in its first five iterations of the *Border Security Metrics Report*.⁴⁹ One of those metrics, which DHS plans to include in future reports, is the Air and Marine Operations actionable intelligence metric.⁵⁰ OIS officials told us that defining the scope of information they should report for this metric has been a challenge. In November 2021, we reported that AMO officials told us that the component does not use the term “actionable intelligence” and thus does not have a way to measure it.⁵¹ In February 2023, AMO officials told us they are in the process of developing a dashboard to report this metric. Given DHS’s challenges with defining this metric, engaging with Congress on its informational needs for the metric could help inform AMO’s efforts to develop the dashboard and ensure its usefulness.

Likewise, for the two metrics DHS plans to report in the 2023 *Border Security Metrics Report*—unlawful entries at ports of entry and the secondary examinations effectiveness rate—engaging with Congress could help DHS identify steps it could take toward reporting information for the metrics that would be most useful to Congress. According to the 2021 *Border Security Metrics Report*, it is “highly unlikely” for DHS to report on the unlawful entries at ports of entry metric.⁵² DHS uses the Compliance Examination, or COMPEX, program to measure the

⁴⁸[GAO-14-704G](#).

⁴⁹DHS reported on two of these metrics in its 2022 *Border Security Metrics Report* and officials told us the department plans to include the remaining four metrics in future reports.

⁵⁰6 U.S.C. § 223(e)(1)(H).

⁵¹[GAO-22-104651](#).

⁵²6 U.S.C. § 223(a)(11), (c)(1)(A)(iii).

effectiveness of CBP's inspections at ports of entry.⁵³ However, according to the report, COMPEX does not have a sufficient sample size to generate an estimate of unlawful entries at ports of entry, as required by the NDAA. In addition, OFO officials told us that they suspended COMPEX at land ports of entry in March 2020 and at airports in January 2021, and they are analyzing possible enhancements to the program's methodology. As DHS considers possible enhancements, engaging with Congress could help the department understand congressional needs for the metric and inform the department's next steps.

DHS could also benefit from engaging with Congress regarding the 16 metrics it included in its 2021 report but that continued to differ from their NDAA definitions. For example, for three of these metrics, DHS's systems and processes do not track information in a way that positions the department to report them according to 2017 NDAA requirements. In particular, CBP's data system does not distinguish between containers and shipments, or between its three methods of cargo inspection: (1) reviewing, (2) scanning, and (3) assessing.⁵⁴ As a result, three metrics related to high-risk cargo containers scanned by CBP differed from their definitions in the 2017 NDAA. Engaging Congress could help DHS identify any refinements the department could make to these metrics to best meet Congress's needs.

DHS could also benefit from further engaging with Congress on the usefulness of the *Border Security Metrics Report* with respect to its timeliness, and to resolve related concerns. OIS officials told us that congressional staff have raised concerns about the timeliness of the report. Specifically, OIS officials told us congressional staff raised concerns about the time frame in which DHS issues the report each year. OIS officials told us that DHS responded to this concern by stating that DHS was meeting its obligation under the law to issue the report annually.

⁵³The COMPEX program is a statistical survey in which vehicles cleared for entry into the U.S. by CBP are randomly selected for a comprehensive audit through a computer-generated sample. CBP is to conduct an audit of the selected vehicles by doing a secondary inspection, using a standardized system of checks to identify any violations that were missed during the routine inspection.

⁵⁴Comparison of potentially high-risk cargo containers scanned by OFO at sea ports of entry during a fiscal year to total high-risk containers entering at such sea ports in the previous fiscal year. 6 U.S.C. § 223(c)(1)(G)(ii); Potentially high-risk cargo containers scanned upon arrival at a U.S. sea port of entry. Id. at § 223(c)(1)(G)(iii); Potentially high-risk cargo containers scanned before arrival at a U.S. sea port of entry. Id. at § 223(c)(1)(G)(iv).

While DHS has issued the report annually as required by the 2017 NDAA, the time frame in which it has issued the report has varied.

For example, DHS has issued each of its first six *Border Security Metrics Reports* 4 to 11 months after the end of the fiscal year for which the report was issued. Further, the latest data included in each report was generally 2 years old by the time the report was published. For example, to meet the annual reporting requirement for fiscal year 2021, DHS issued its *Border Security Metrics Report* in April 2022, and the most recent data the report included was for fiscal year 2020. Table 6 shows the timing of the *Border Security Metrics Reports* issued as of July 2023. By periodically engaging with Congress, DHS could better understand, and work toward addressing, concerns with the reports' timeliness.

Table 6: Timing of *Border Security Metrics Reports* Issued Pursuant to the National Defense Authorization Act for Fiscal Year (FY) 2017, as of July 2023

Reporting year	Date of issuance	Latest data included
Fiscal year (FY) 2017	May 1, 2018	FY 2016
FY 2018	February 26, 2019	FY 2017
FY 2019	August 5, 2020	FY 2018
FY 2020	September 16, 2021	FY 2019
FY 2021	April 27, 2022	FY 2020
FY 2022	July 3, 2023	FY 2021

Source: GAO analysis of Department of Homeland Security *Border Security Metrics Reports*. | GAO-24-106277

While the *Border Security Metrics Report* states DHS will update Congress on its progress refining the metrics through periodic briefings in addition to issuing the report, OIS officials told us that DHS has not conducted such briefings. Further, OIS officials told us they have not generally engaged with Congress to help refine the information the department includes in the report to improve its usefulness to Congress. The officials explained that they consider producing the reports for Congress as a form of engagement. However, transmitting the report is a separate activity from the briefings that DHS's report says it will provide, and does not allow for dialogue. For example, during a briefing, congressional staff could ask questions and DHS could obtain information to better understand congressional needs and inform its report development. By periodically engaging with Congress, OIS may be able to identify potential opportunities to refine the metrics and ensure the information in its report is useful to Congress.

DHS Improved the Quality of Some Information in Its 2021 Report but Has Not Fully Assessed Its Deterrence Model or Identified Limitations for Reported Metrics

DHS Has Improved Information Quality by Conveying Statistical Uncertainty for Model-Based Metrics

DHS improved the quality of information of several metrics it reported in the 2021 *Border Security Metrics Report* compared to its 2019 report. In particular, DHS improved the quality of three unlawful entry metrics: (1) the attempted unlawful border crosser apprehension rate (model-based apprehension rate), (2) the estimated number of undetected unlawful entries, and (3) the probability of detection rate.⁵⁵ These metrics contain information on estimates derived from a statistical model. One of the inputs into this model is an estimated deterrence rate.

DHS uses this model to estimate the three unlawful entry metrics. This model is focused on individuals who unlawfully crossed the border between ports of entry, who Border Patrol apprehended and removed from the country across the U.S.-Mexico border. These individuals also

⁵⁵In general, the attempted unlawful border crosser apprehension rate is the rate of apprehension of attempted unlawful border crossers (6 U.S.C. § 223(b)(1)(A)(i)). In the *Border Security Metrics Reports*, DHS presents both observed and modeled apprehension rates. For the purposes of this discussion, we focus on the modeled rates and refer to the metric as the "model-based apprehension rate." Undetected unlawful entries are an estimate of the number of undetected unlawful border crossers who enter the U.S. and are not apprehended by a DHS border security component (6 U.S.C. § 223(a)(11), (b)(1)(A)(iii)). The probability of detection rate compares the estimated total unlawful border crossing attempts not detected by Border Patrol with the unlawful border crossing effectiveness rate (i.e., the percentage resulting from dividing the number of apprehensions and turn backs by the sum of the number of apprehensions, estimated undetected unlawful entries, turn backs, and got aways). 6 U.S.C. § 223(a)(10), (b)(1)(C), (D)).

made subsequent reentry attempts.⁵⁶ Within the model's framework, when an individual's first attempt at unlawfully crossing the border is successful, the individual enters the U.S., and no apprehension is made. However, if Border Patrol apprehends an individual, the agency records it in a DHS data system.⁵⁷ Within the model's framework, the individual is then returned across the U.S.-Mexico border.⁵⁸ A Mexican research center subsequently surveys certain individuals about their intentions to attempt to enter the U.S. again.⁵⁹ DHS uses the results from this survey to estimate the rate at which individuals are deterred from crossing again—the estimated deterrence rate.⁶⁰ Should the individuals make a second attempt to cross the border unlawfully, they may succeed in entering the U.S. unlawfully or be apprehended by Border Patrol. Figure 2 provides information on the process DHS uses to calculate unlawful entry metrics, including the estimated deterrence rate.

⁵⁶This type of statistical model is known as a "repeated trials model" because, in this case, it extrapolates from a subset of individuals who unlawfully crossed the border and attempted to cross again. This subset consists of Mexican adults who were removed from the country across the U.S.-Mexico border (not to the Mexican interior or other locations) and who have not ever requested asylum, among other characteristics. We discuss this model in more detail later in this report.

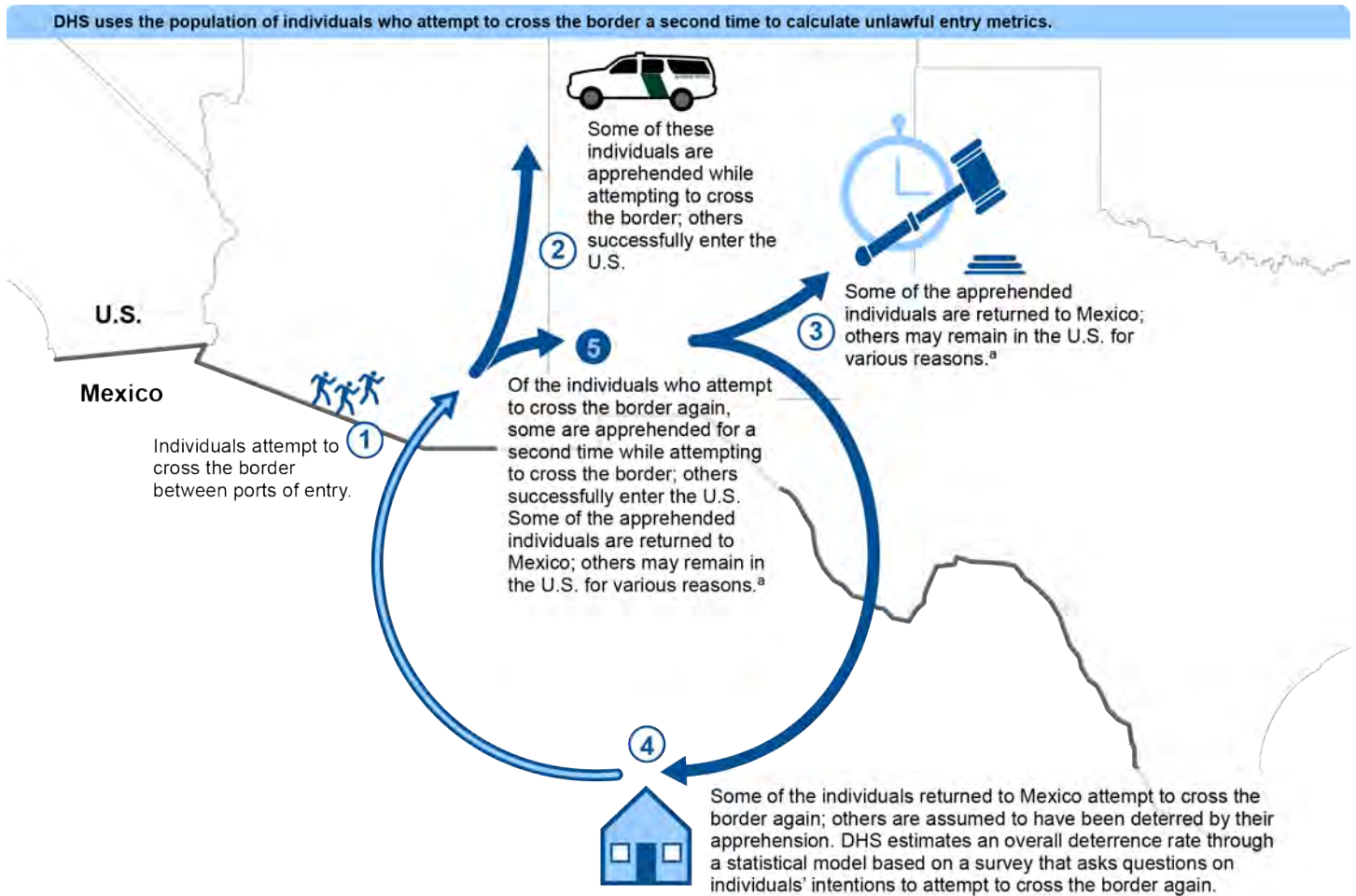
⁵⁷The apprehended individual is potentially subject to consequences for entering unlawfully, such as administrative enforcement and removal, criminal prosecution, or being barred from legally entering the U.S. in the future.

⁵⁸While some apprehended individuals are returned to Mexico, others may remain in the U.S. for various reasons such as awaiting removal to their home country, resolution of immigration proceedings, resolution of criminal proceedings, or serving terms of imprisonment.

⁵⁹The survey Encuesta sobre Migración en la Frontera Norte de México is conducted by a Mexican research and educational institution, El Colegio de la Frontera Norte. The survey website can be accessed at <http://www.colef.mx/emif/>.

⁶⁰If an individual does not make another attempt to unlawfully cross the border, the statistical model makes no further assumption about the individual's actions.

Figure 2: Framework for the Department of Homeland Security's (DHS) Statistical Model for Unlawful Entry Metrics



Source: GAO analysis of DHS's model-based apprehension rate, GAO icons. | GAO-24-106277

Note: Some individuals who cross the border unlawfully respond to U.S. enforcement efforts by choosing to return promptly to the country from which they entered (called a turn back).

^aThese reasons include awaiting removal to their home country, resolution of immigration proceedings, resolution of criminal proceedings, or serving terms of imprisonment.

In March 2019, we reported that DHS did not provide information on the level of uncertainty related to this statistical model in the 2017 *Border Security Metrics Report*. For example, DHS provided a single model-based apprehension rate that did not fully convey the uncertainty of estimating these metrics. We reported that, like all statistical models, DHS based its estimate on a limited sample of data that may have been affected by random variation, among other things. That is, the estimates derived from the model included some level of uncertainty. We

recommended that DHS include measures of statistical uncertainty for all metrics based on estimates derived from statistical models in its annual *Border Security Metrics Report*.⁶¹

In its 2019 *Border Security Metrics Report*, DHS took steps toward implementing this recommendation by conveying the statistical uncertainty of the model-based apprehension rate and of the total number of unlawful entries in a report appendix.⁶² Specifically, OIS officials told us they allowed key assumptions to vary by as much as twice the confidence interval for the estimated apprehension rate for a particular subset of border crossers—a key input into the statistical model.⁶³ According to OIS officials, this uncertainty reflected sampling and prediction error in estimating the probability of deterrence.

In its 2021 *Border Security Metrics Report*, DHS fully addressed our recommendation by conveying statistical uncertainty for all three relevant unlawful entry metrics.⁶⁴ Specifically, DHS noted the confidence interval it used—95 percent—and displayed the range (i.e., lower and upper bounds) for each of these estimates. For example, DHS estimated that 66 percent of individuals were apprehended in fiscal year 2020, and the remaining 34 percent entered the U.S. To display the range of that estimate, DHS used the confidence interval to determine that the true

⁶¹[GAO-19-305](#).

⁶²Within the between ports of entry domain, the 2017 NDAA mandates that DHS report separately on detected unlawful entries and estimated undetected unlawful entries. In the 2019 *Border Security Metrics Report*, DHS conveyed statistical uncertainty for the total number of unlawful entries, which is the sum of detected and undetected unlawful entries.

⁶³DHS, using a survey of Mexican individuals who were apprehended and returned to the border region of Mexico by U.S. immigration authorities, calculated the estimated apprehension rate—as well as a 95 percent confidence interval—for this particular subset of border crossers. A margin of error (or confidence interval) provides the range around a statistical estimate where the true value is likely to exist. If an estimate's margin of error is small, the estimate has a lower amount of random error and is therefore more precise and known with greater certainty.

⁶⁴DHS did not convey statistical uncertainty for a fourth metric, the unlawful border crossing effectiveness rate, because it did not report on the metric using its statistical model. Instead, DHS reported on an alternative metric (the interdiction effectiveness rate) using known data that did not require estimation, and therefore, did not involve statistical uncertainty. The model-based apprehension rate is also known as the attempted unlawful border crosser apprehension rate. The probability of detection rate is the ratio of detected unlawful entries to estimated total unlawful entries.

value of the percentage of individuals apprehended was likely to exist within the range of 60 percent to 74 percent.

By conveying statistical uncertainty in the 2021 *Border Security Metrics Report*, DHS met the intent of our recommendation. The Office of Management and Budget's statistical standards for federal agencies state that the possible variation of estimates should be noted, such as by reporting the range of each estimate.⁶⁵ Measures of statistical uncertainty, such as confidence intervals, help to convey the amount by which estimates might vary due to randomness in the data and allow consumers of the estimates to evaluate their accuracy. These actions should allow Congress, policymakers, and the public to more fully evaluate the extent to which the metrics are valid.

DHS Has Not Assessed or Updated Its Deterrence Model to Reflect Current Conditions

As previously noted, DHS's statistical model for estimating the three unlawful entry metrics requires an estimated deterrence rate—the share of individuals who decide not to attempt to reenter the U.S. after being apprehended. As an input to this model, DHS uses a separate statistical model to estimate deterrence, referred to as the deterrence model. However, DHS has not assessed or updated the deterrence model since its development in 2016, raising questions about the extent to which the model reflects current southwest border conditions.

DHS developed the deterrence model by contracting with the Institute for Defense Analyses (IDA) in 2016.⁶⁶ IDA developed this deterrence model using an academic survey of individuals returning to Mexico and DHS administrative data.

- **Survey.** A research center linked to a Mexican university has regularly surveyed Mexican individuals who have been apprehended and returned across the U.S.-Mexico border about their intentions to stay close to the border and reenter the U.S.⁶⁷ Specifically, this survey has asked individuals about their intention to attempt to reenter after certain intervals of time, such as 7 days and 90 days. Using these

⁶⁵Office of Management and Budget, *Standards and Guidelines for Statistical Surveys* (Washington, D.C.: September 2006).

⁶⁶IDA is a non-profit corporation that operates three federally-funded research and development centers to provide analyses of national security issues, particularly those requiring scientific and technical expertise.

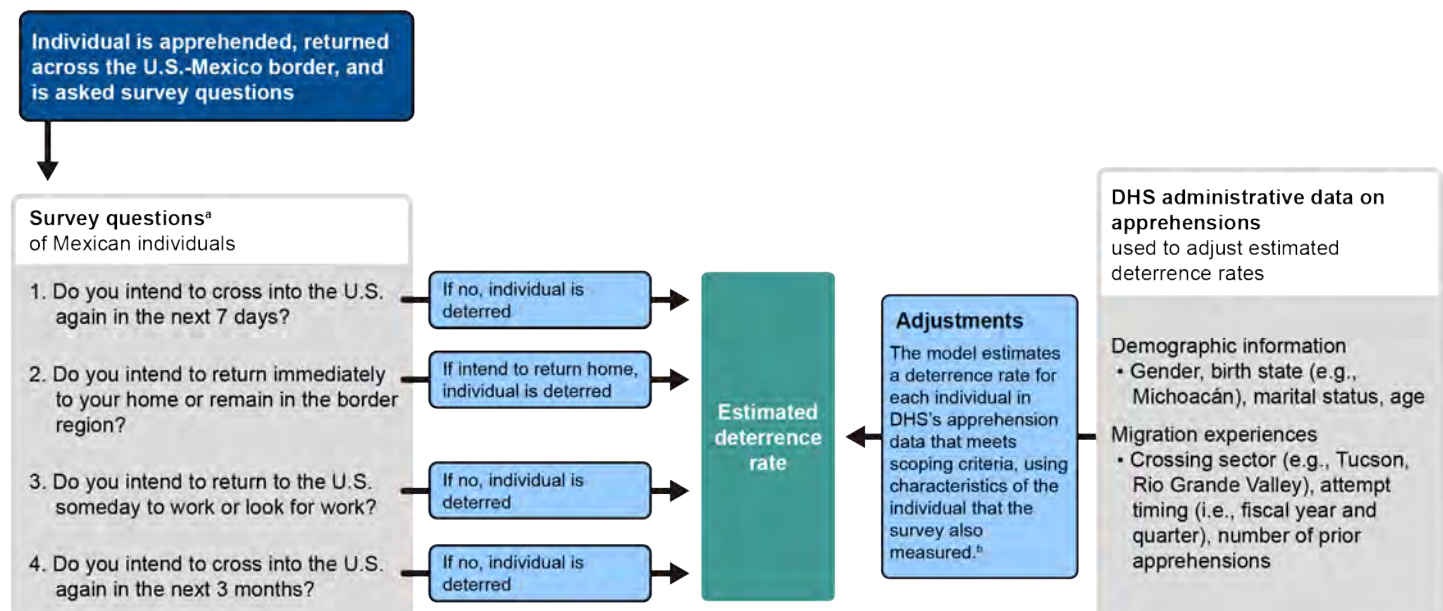
⁶⁷The survey Encuesta sobre Migración en la Frontera Norte de México is conducted by a Mexican research and educational institution, El Colegio de la Frontera Norte. The survey website can be accessed at <http://www.colef.mx/emif/>.

responses, IDA developed estimated deterrence rates for individuals who took the survey, based on how various individual characteristics and experiences, such as gender, birth state, and age, predicted the probability of deterrence.

- **Administrative data.** IDA used these estimated deterrence rates, developed based on the survey, to estimate deterrence for the broader population of Mexican individuals in its administrative data, using individual characteristics and experiences that each data source measured. IDA estimated deterrence for all apprehended individuals from Mexico in DHS's administrative data that met scoping criteria, not only individuals who took the survey, and adjusted for characteristics and experiences that may affect reentry attempts.⁶⁸ In its 2021 *Border Security Metrics Report*, DHS estimated that 71 percent of individuals who were apprehended in 2020 were deterred from attempting to enter the U.S. again.

Figure 3 shows the model DHS adapted from IDA to estimate a deterrence rate.

Figure 3: Model the Department of Homeland Security (DHS) Uses to Estimate a Deterrence Rate



Source: GAO analysis of DHS and Institute for Defense Analyses documentation. | GAO-24-106277

⁶⁸IDA applied the same scoping criteria used to estimate the unlawful entry metrics that included a subset of individuals. For example, IDA excluded non-Mexican nationals.

^aThe survey Encuesta sobre Migración en la Frontera Norte de México is conducted by a Mexican research and educational institution, El Colegio de la Frontera Norte. When developing the model, the Institute for Defense Analyses made additional assumptions regarding the responses to the survey questions if an individual answered “yes” to one question, but “no” to a different question.

^bFor example, the scoping criteria excluded non-Mexican nationals and apprehended individuals who had missing data on the factors used to predict deterrence.

When developing the deterrence model for each *Border Security Metrics Report*, DHS has mainly used the same deterrence model that IDA developed in 2016. Based on the border conditions and available data in 2015, IDA developed the deterrence model, a predictive statistical model. Specifically, IDA developed the model based on survey responses from 2002 through 2015, the latest data available at the time of development. IDA also chose administrative data, such as gender, that predicted deterrence at the time.

DHS has made some refinements to the model over time and uses updated data in the model to re-estimate the deterrence rate for each *Border Security Metrics Report*. For example, in its 2021 *Border Security Metrics Report*, DHS refined the deterrence model by adjusting its methods for calculating sampling uncertainty.⁶⁹ After making these refinements, the model’s estimated deterrence rate decreased by 1 to 3 percentage points and the estimated model-based apprehension rate decreased by up to 7 percentage points. OIS officials stated that they made these refinements to avoid using the survey data improperly and to better reflect the underlying assumptions of the survey sample design. Moreover, for each report, OIS typically re-estimates the deterrence rate by inputting both updated survey data and DHS administrative data into the deterrence model. For example, in the 2021 report, DHS used survey data from fiscal years 2012 through 2020 in its deterrence model. OIS officials told us that subject matter experts examined the deterrence model to consider the current year’s estimated deterrence rate against those from prior years. OIS officials also told us they did so as a way to examine the accuracy of the estimated deterrence rate.

OIS has also identified issues with the deterrence model and its inputs. Consequently, the office is considering ways to address them. For example, the academic survey of returning Mexican individuals used in

⁶⁹Specifically, DHS refined the deterrence model by incorporating two statistical techniques: (1) survey weights and (2) robust standard errors. Survey weights are values used to make data more representative of the population. Robust standard errors are a mathematical tool used to calculate how accurately a set of data represents the actual population.

the model was discontinued from April to June 2020 and all of 2021, due to the COVID-19 pandemic.⁷⁰ More broadly, southwest border conditions have changed substantially from 2015 to 2021, with DHS experiencing a significant increase in the number of individuals encountered at, or apprehended between, U.S. ports of entry along the southwest border, along with a significant increase in the number of non-Mexican individuals unlawfully crossing the border. This has implications for the deterrence model because its inputs are the survey of returning Mexican individuals and DHS administrative data on apprehended individuals from Mexico. According to DHS data, the agency encountered or apprehended about 331,000 individuals in fiscal year 2015 and about 1.7 million individuals in fiscal year 2021.⁷¹

DHS noted the implications of these changing conditions on its reporting of metrics in the 2021 *Border Security Metrics Report*, stating that the characteristics of those crossing the border unlawfully between ports of entry has changed. In particular, the report noted that the statistical model used for estimating unlawful entry metrics has used only about 20 percent of southwest border apprehensions in recent years because it excludes all individuals who are not Mexican nationals from the count of unlawful border crossers, among other reasons. The report also noted that the number of individuals apprehended from Central American countries has been increasing. For example, according to DHS data, the agency apprehended about 33,000 individuals from Honduras in fiscal year 2015 and about 142,000 individuals from Honduras in fiscal year 2021.

OIS officials told us they are considering some steps to address these issues, but have not yet made decisions on those steps, and related time frames are uncertain. For example, officials said they do not currently know how they will update or replace the deterrence model without updated survey data on intended reentry attempts. They are, however, considering using historical survey data in future years. OIS is also

⁷⁰In its 2022 report, OIS did not provide data from fiscal year 2021 for metrics based on estimates derived from a statistical model. It did not do so because the Mexican research center did not conduct surveys in 2021, which made estimating the deterrence rate for that fiscal year unfeasible, according to the report.

⁷¹Department of Homeland Security, *Border Security Metrics Report: 2022* (Washington, D.C.: July 3, 2023). Beginning in March 2020, CBP data includes individuals who CBP processed under both Title 8 immigration enforcement and Title 42 public health authorities. On May 11, 2023, CBP's authority to expel certain recent border crossers for public health reasons under Title 42 expired. According to the 2022 *Border Security Metrics Report*, CBP processed approximately 63 percent of the 1.7 million individuals under Title 42 and approximately 37 percent under Title 8.

considering leveraging information from the Operational Performance Simulator model that CBP is developing. The Operational Performance Simulator calculates a simulation-based estimate. We reported in November 2021 that OIS officials stated a simulation-based estimate would rely on fewer assumptions about the types of individuals who unlawfully cross the border as compared with the current deterrence model.⁷² OIS officials told us they do not plan to incorporate data from the Operational Performance Simulator in the 2023 *Border Security Metrics Report*, but are considering incorporating these data in future versions of the report.

Given that OIS does not plan to use the Operational Performance Simulator model for the 2023 *Border Security Metrics Report*, it would be beneficial for OIS to assess and update other inputs to its deterrence model to better ensure that the model reflects border conditions. As previously mentioned, for each *Border Security Metrics Report*, OIS typically re-estimates the deterrence rate by inputting both updated survey data and DHS administrative data into the deterrence model. However, DHS has not substantially updated the model or reassessed its predictive accuracy since the model was developed in 2016. Two examples illustrate how OIS could more immediately assess and update its deterrence model in the near term, as appropriate:

- **DHS administrative data.** When developing the deterrence model in 2016, DHS incorporated administrative data on specific characteristics to help predict whether an individual was deterred from attempting to reenter the U.S. after apprehension. For example, DHS incorporated the location an individual crossed into the U.S. into its model. While DHS is considering how to address issues identified with the survey of returning Mexican individuals, DHS could take more immediate steps. For example, it could assess whether the specific DHS administrative data characteristics it currently uses are reflective of existing border conditions and help to predict deterrence. DHS could also assess whether other administrative data characteristics could be useful. DHS could use the results of its assessment to update the model, as appropriate.
- **Type of statistical model.** DHS chose to use a particular type of statistical model, known as logistic regression. This type of model estimates the probability of an event occurring based on a set of characteristics. DHS could assess whether this type of model remains

⁷²[GAO-22-104651](#).

the most appropriate to predict deterrence, compared to alternative types of predictive modeling methods.

OIS officials agreed that it would be beneficial for the office to assess and update the deterrence model. However, OIS has not yet considered doing so beyond how it could address issues with the survey and with DHS administrative data accounting only for Mexican individuals. Our key practices for continuous monitoring of performance call for artificial intelligence systems—such as predictive statistical models, including the deterrence model used by DHS—to be routinely re-evaluated to ensure the system produces desired results.⁷³ The key practice related to drift (i.e., a reduction in the model's predictive power) calls for agencies to establish the range of data and model drift that is acceptable to ensure the model produces desired results, such as a predicted rate of deterrence.

In addition, statistical principles and standards for internal control support the need for DHS to assess and update its deterrence model, considering changes to the southwest border's conditions. Statistical principles call for predictive models, such as the deterrence model, to be developed and validated using data sampled from the populations where they will be used.⁷⁴ Models developed for one population may not predict as well when applied to different populations, such as when a population changes over time. As a result, predictive models should be updated regularly as their target populations change. *Standards for Internal Control in the Federal Government* states that management should identify information requirements in an iterative and ongoing process.⁷⁵ As changes in the entity occur, management should change information requirements as needed to meet these modified objectives and address these modified risks. Further, *Standards for Internal Control in the Federal Government* states that documentation is a necessary part of an effective internal control system.⁷⁶

⁷³GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, [GAO-21-519SP](#) (Washington, D.C.: June 30, 2021).

⁷⁴Gareth James, et al., *An Introduction to Statistical Learning: with Applications in R*, 2nd ed. (New York: Springer, 2021), 29-37.

⁷⁵GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

⁷⁶[GAO-14-704G](#).

DHS could better ensure that the deterrence model reflects current southwest border conditions by assessing the extent to which its choice of input administrative data and statistical model type remains sufficiently predictive, and by documenting the results. This assessment is particularly important if OIS uses historical survey data. Further, by using the results of its assessment to update or inform its efforts to replace its statistical model of deterrence, as appropriate, DHS could have better assurance the model reflects current southwest border conditions.

DHS Does Not Yet Have a Systematic Process for Reviewing the Reliability of Data to Identify Limitations

In March 2019, we reported that DHS did not have a process to systematically review the reliability of data used in its *Border Security Metrics Report* and identify limitations with the data and methodologies that underlie the metrics.⁷⁷ DHS officials told us at that time that they largely relied on the DHS components from which they collected the data to assess the data's reliability and communicate identified limitations. The specific processes DHS components used to ensure data reliability varied from metric to metric. For example, we reported that Border Patrol officials issued guidance and monitored the implementation of it, while AMO officials conducted supervisory reviews of data entries to ensure data reliability.

We concluded in our March 2019 report that having a process to systematically review the reliability of the data would help improve the quality of the information available to Congress. We recommended that the Secretary of Homeland Security develop and implement a process to systematically review the reliability of the data used in its *Border Security Metrics Report* and comprehensively identify any limitations with the data and methodologies that underlie its metrics. DHS concurred with our recommendation. In July 2022, DHS officials stated that they did not yet have sufficient resources to implement this recommendation. In July 2023, OIS officials stated that they have ongoing conversations to examine their processes and determine how they can systematically review the reliability of the operational data.

We also recommended in March 2019 that DHS communicate the limitations of the metrics that the department identifies through its systematic review of information in the *Border Security Metrics Report*. DHS concurred with this recommendation. In December 2022, OIS

⁷⁷[GAO-19-305](#). According to *Standards for Internal Control in the Federal Government*, data are considered reliable when they are reasonably free from error and bias. Quality information is derived from relevant and reliable data and is considered to be complete, accurate, and timely. [GAO-14-704G](#).

officials told us they would address this recommendation after developing a process to systematically review the reliability of the data and identify data limitations.

DHS took steps to improve the quality of information reported in its 2021 *Border Security Metrics Report*. As discussed above, DHS conveyed statistical uncertainty for relevant metrics. In addition, DHS clarified the source of the data used in all tables of the report by adding source lines to them. For example, a table showing the number of enforcement flight hours and apprehensions assisted by aircraft identified the source of the data as AMO.⁷⁸

However, our review of DHS's 2021 *Border Security Metrics Report* also identified issues with the quality of information in the report. Some of these issues relate to the persistence of data reliability issues that we identified in our previous reports. Our review of DHS's 2017 *Border Security Metrics Report* identified 21 metrics that had limitations that DHS did not disclose in that report. Our review of the 2021 *Border Security Metrics Report* found that 17 of these 21 metrics still had limitations, which DHS did not disclose in its report. The number of limitations DHS did not disclose remained the same from our last review. For example, we reported in March 2019 that commercial vehicle wait time data—part of the average wait times and traffic volume metric—were unreliable for fiscal years 2012 through 2016.⁷⁹ The 2019 and 2021 *Border Security Metrics Reports* did not disclose that some of the commercial vehicle wait time data presented in the report were not reliable.

Other quality issues related to newly-identified instances of inaccurate information in the 2021 *Border Security Metrics Report*. For example, prior to 2021, the *Border Security Metrics Reports* inaccurately labeled nationwide turn back and got away data as southwest-border only. DHS acknowledged this error in a table note in the 2021 *Border Security Metrics Report*. According to OIS officials, they discovered the errors after being prompted during our review of the 2019 *Border Security Metrics Report*. We previously reported that these metrics did not correspond with

⁷⁸As defined by the 2017 NDAA, the number of apprehensions assisted by AMO are those apprehensions assisted through the use of unmanned aerial systems and manned aircraft. 6 U.S.C. § 223(e)(1)(F).

⁷⁹[GAO-19-305](#).

their NDAA definitions because DHS labeled these metrics as pertaining to the southwest border.

Another example is OIS's labeling of actions CBP officials take when encountering noncitizens. Specifically, OIS labeled expulsions of noncitizens for public health reasons under Title 42 of the U.S. Code as "apprehensions" in certain tables in the 2021 *Border Security Metrics Report*. Border Patrol officials told us that using the term "apprehension" is inaccurate. Rather, using the terms "encounter" or "expulsion" would have been accurate. OIS officials acknowledged that they were aware CBP does not use the term "apprehension" to describe individuals expelled from the U.S. under Title 42, but did not correct or update the term in the titles of these tables in the 2021 *Border Security Metrics Report*.

According to DHS Directive 139-02 on Information Quality, DHS is to ensure and maximize the quality, objectivity, utility, and integrity of the information that it disseminates to the public.⁸⁰ Guidance implementing that directive states that DHS should have a process for reviewing the quality of information before it is disseminated.⁸¹ The guidance also states that the quality of information involves a focus on ensuring accurate information. Additionally, *Standards for Internal Control in the Federal Government* state that management officials should evaluate data sources for reliability and communicate quality information, including relevant data from reliable sources, to achieve an agency's objectives.⁸² The quality information can then be used by agency management and external stakeholders, such as policymakers, to make informed decisions and evaluate performance.

By implementing our prior recommendation to develop and implement a process to systematically review the reliability of data, DHS would be better positioned to comprehensively identify and fully disclose metrics' limitations and to maximize the quality of the data. Thereafter, by communicating the data or methodological limitations with the metrics, it would facilitate a better understanding and appropriate interpretation of the data in the context of the *Border Security Metrics Report*.

⁸⁰Department of Homeland Security, *Information Quality*, Directive 139-02.

⁸¹Department of Homeland Security, *Information Quality Implementation*, Instruction 139-02-001.

⁸²[GAO-14-704G](#).

Conclusions

Since 2018, DHS has issued an annual *Border Security Metrics Report* containing metrics related to border security efforts, a key part of DHS's mission. This report makes an important contribution to understanding these efforts by providing data and information to policymakers and the public spanning multiple border domains and years.

OIS coordinated with multiple DHS components to provide updated data for the metrics it included in its 2021 *Border Security Metrics Report*, but DHS made limited progress in aligning certain metrics it already reports with their 2017 NDAA definitions. By better engaging with components, OIS could help obtain additional information needed and guide relevant DHS component efforts to more fully report the metrics according to their 2017 NDAA definitions. DHS also could benefit from engaging with Congress about metrics that have been challenging to report and that it has previously omitted. By periodically engaging with Congress, OIS could identify potential opportunities to refine the metrics and ensure the information is useful to Congress.

DHS improved the quality of information related to some metrics in its 2021 report. However, it has not fully assessed its deterrence model or identified limitations related to its methods, or the reliability of data it uses to report metrics. DHS uses a statistical model that estimates a deterrence rate to report on three metrics, but DHS has not assessed or updated the model since 2016. By conducting and documenting an assessment, and then updating or informing its efforts to replace the deterrence model, as appropriate, DHS can better ensure its choice of input administrative data and model type remains sufficiently predictive, and reflective of current southwest border conditions. In addition, we have continued to find that DHS has not addressed data limitations we have previously identified. We continue to believe that it would be beneficial to develop and implement a process to systematically review the reliability of data, and then communicate relevant limitations, consistent with our 2019 recommendations. Taking these actions would better position DHS to comprehensively identify and fully disclose metrics' limitations, and to maximize the quality of the data in the *Border Security Metrics Report*.

Recommendations for Executive Action

We are making the following four recommendations to DHS:

The Under Secretary for the Office of Strategy, Policy, and Plans should take steps to engage with components to more fully report the metrics as defined by the 2017 NDAA in its *Border Security Metrics Report*. (Recommendation 1)

The Under Secretary for the Office of Strategy, Policy, and Plans should periodically engage with Congress to improve the usefulness of information in its *Border Security Metrics Report*. (Recommendation 2)

The Under Secretary for the Office of Strategy, Policy, and Plans should assess the extent to which its choice of input administrative data and model type for its statistical model of deterrence remains sufficiently predictive, and document the results. (Recommendation 3)

The Under Secretary for the Office of Strategy, Policy, and Plans should use the results of its assessment to update or inform its efforts to replace its statistical model of deterrence, as appropriate. (Recommendation 4)

Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. DHS provided written comments, which are reproduced in appendix III. DHS also provided technical comments, which we incorporated as appropriate. DHS concurred with all four of our recommendations and described actions planned or underway that, if implemented fully, should address the intent of three of the recommendations. For the remaining recommendation, in addition to engaging with components to newly report metrics, DHS should ensure that it also engages with components to more fully report metrics already included in its *Border Security Metrics Report* according to their 2017 NDAA definitions.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Rebecca Gambler at 202-512-8777 or gablerr@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.



Rebecca Gambler
Director, Homeland Security and Justice

Appendix I: Other Metrics for Measuring the Effectiveness of Border Security

In prior GAO reports, we have identified other metrics the Department of Homeland Security (DHS) could use to help measure the effectiveness of border security, in addition to the National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA) metrics. These metrics spanned the four domains in the 2017 NDAA—between ports of entry, at ports of entry, the maritime border, and the air environment, respectively.¹ In our March 2019 and November 2021 reports, we identified 14 recommendations from 11 prior GAO reports.² We noted that implementing these recommendations would provide DHS with additional indicators and metrics that could provide important insights into the state of border security.

The following tables provide updates on the recommendations included in our March 2019 and November 2021 reports.³ Of the 14 recommendations, seven have been implemented, four have been closed and not implemented, and three remain open as of September 2023. Implementing the open recommendations would provide DHS with additional indicators and metrics that could provide important insights into

¹Pub. L. No. 114-328, div. A, title X, subtitle G, § 1092, 130 Stat. 2000, 2429-36 (2016) (classified at 6 U.S.C. § 223). The statute refers to the final domain as “Air and Marine security metrics in the land domain,” which it defines as aviation assets and operations of U.S. Customs and Border Protection’s (CBP) Air and Marine Operations. 6 U.S.C. § 223(e). In our 2019 report, we referred to this as “air and marine security in the land domain.”

²In our March 2019 report, we identified 11 recommendations from nine reports issued from August 2009 through January 2019 related to measures for assessing border security. In our November 2021 report, we identified three recommendations from two reports issued from January 2019 through September 2021. GAO, *Border Security: DHS Should Improve the Quality of Unlawful Border Entry Information and Other Metric Reporting*, [GAO-19-305](#) (Washington, D.C.: Mar. 21, 2019); and *Border Security Metrics: Progress Made, but DHS Should Take Additional Steps to Improve Information Quality*, [GAO-22-104651](#) (Washington, D.C.: Nov. 16, 2021). For the purpose of this report, we also reviewed 28 reports from our prior work and 73 DHS Office of Inspector General reports issued from October 2021 through September 2023. Through this review, we identified one relevant recommendation in a September 2023 DHS Office of Inspector General report addressing CBP efforts to inspect international mail. The DHS Office of Inspector General recommended that CBP update its August 2001 *International Mail Operations and Enforcement Handbook* to include, among other things, key performance metrics and targeting goals to assess the effectiveness of mail operations. CBP did not concur with the recommendation. The DHS Office of Inspector General considers this recommendation open and unresolved. DHS OIG, *CBP Did Not Effectively Conduct International Mail Screening or Implement the STOP Act*, OIG-23-56 (Washington, D.C.: Sept. 25, 2023).

³[GAO-19-305](#). In our November 2021 report, we found that three of the 14 recommendations had been implemented and four had been closed and not implemented. [GAO-22-104651](#).

the state of border security. Tables 7–10 chronologically list the three open recommendations and four recommendations that have been implemented since our November 2021 report by domain. The tables also provide the status of DHS’s implementation of those recommendations as of September 2023.

Table 7: Other Metrics the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security Between Ports of Entry

GAO product title and number	Summary and finding	Recommended metric	Status of recommendation implementation as of September 2023
<i>Northern Border Security: CBP Identified Resource Challenges but Needs Performance Measures to Assess Security Between Ports of Entry</i> ^a (GAO-19-470)	In June 2019, we reported on northern border security efforts. We found that the U.S. Border Patrol, a component of U.S. Customs and Border Protection (CBP), had performance measures that assessed specific border security operations or programs that included data from the northern border. However, these measures generally combined data with other border regions and, collectively, the measures did not assess effectiveness at securing the northern border between ports of entry. We concluded that without northern border performance measures, Border Patrol cannot assess its effectiveness at securing the northern border between ports of entry.	Border Patrol should develop and implement performance measures to assess its effectiveness at securing the northern border between ports of entry.	Open Border Patrol agreed with this recommendation and in April 2020 stated that it was developing new northern border security metrics. In a July 2023 update, Border Patrol stated that it had developed a catalog of metrics that are relevant to the northern border operational environment to better measure performance. Border Patrol stated that it is in the process of testing the catalog and estimated it will be fully functional in late 2023.

**Appendix I: Other Metrics for Measuring the
Effectiveness of Border Security**

GAO product title and number	Summary and finding	Recommended metric	Status of recommendation implementation as of September 2023
<i>Southwest Border Security: Additional Actions Needed to Better Assess Fencing's Contributions to Operations and Provide Guidance for Identifying Capability Gaps</i> (GAO-17-331)	In February 2017, we reported on the use of border fencing along the southwest border. We found that Border Patrol collected data that could be useful to assess the contributions of border fencing to border security operations but had not conducted such an assessment.	Border Patrol should develop metrics to assess the contributions of pedestrian and vehicle fencing to border security along the southwest border, using the data Border Patrol already collects, and apply this information, as appropriate, when making investment and resource allocation decisions.	Closed – implemented (priority recommendation)^b DHS agreed with the recommendation. In January 2022, Border Patrol officials provided us with a demonstration of its model that uses quantitative analysis and qualitative field insight. According to these officials, Border Patrol is using the model to depict the overall balance of constraints and enablers that affect a station's current potential to perform its mission-essential tasks within its area of responsibility. Officials added that this model is helping Border Patrol determine what resources, including fencing, would benefit Border Patrol's operations. As Border Patrol is demonstrating that it is using available data to assess the effectiveness of and inform its investment decisions for assets such as pedestrian and vehicle fencing, we closed this recommendation as implemented.

**Appendix I: Other Metrics for Measuring the
Effectiveness of Border Security**

GAO product title and number	Summary and finding	Recommended metric	Status of recommendation implementation as of September 2023
<i>Arizona Border Surveillance Technology Plan: Additional Actions Needed to Strengthen Management and Assess Effectiveness</i> (GAO-14-368)	In March 2014, we reported on the status of DHS's Arizona Border Surveillance Plan—a plan for security technology deployment across the Arizona border that includes a mix of radars, sensors, and cameras to help provide security for the Arizona border. We found that while CBP defined mission benefits for the technology programs under the plan, the agency did not develop key attributes for performance metrics for all surveillance technologies to be deployed as part of the plan.	CBP should analyze available data on apprehensions and seizures and technological assists, in combination with other relevant performance metrics or indicators, as appropriate, to determine the contribution of surveillance technologies to CBP's border security efforts.	Closed - implemented (priority recommendation) DHS agreed with this recommendation. As of March 2019, Border Patrol was able to generate a performance report, using data collected from multiple systems, on how surveillance technologies have assisted agents during operations, including Border Patrol apprehensions. In January 2022, Border Patrol officials provided us with a demonstration of its model that uses quantitative analysis and qualitative field insight. According to these officials, Border Patrol is using the model to depict the overall balance of constraints and enablers that affect a station's current potential to perform mission essential tasks within its area of responsibility. Officials added that this model is helping Border Patrol determine what resources, including technology, would benefit Border Patrol's operations. As Border Patrol is demonstrating that it is using available data to assess the effectiveness of and inform its investment decisions for assets such as surveillance technologies, we closed this recommendation as implemented.

Source: GAO analysis of prior GAO reports related to border security effectiveness metrics. | GAO-24-106277

^aWe issued this report, which identified an additional metric that DHS could use to measure border security effectiveness, in June 2019 and therefore, the metric was not listed in our March 2019 report. This report also appears in table 9 because it also includes a recommendation related to the air environment.

^bA priority open recommendation is one that may significantly improve government operations in the following ways: (1) realizing large dollar savings; (2) aiding in congressional decision-making on major issues; (3) substantially improving major government programs; (4) eliminating mismanagement, fraud, and abuse; (5) ensuring that programs comply with laws and that funds are legally spent; and (6) making progress toward addressing a high-risk or duplication, overlap, and fragmentation issue.

**Appendix I: Other Metrics for Measuring the
Effectiveness of Border Security**

Table 8: Other Metrics the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security at Ports of Entry

GAO product title and number	Summary and finding	Recommended metric	Status of recommendation implementation as of September 2023
<i>Land Ports of Entry: CBP Should Update Policies and Enhance Analysis of Inspections^a</i> (GAO-19-658)	In August 2019, we reported on U.S. Customs and Border Protection (CBP) processes for inspections at land ports of entry. We found that CBP uses various sets of performance measures to assess its efforts to detect illegal activity at land ports. We also found that these measures generally reflected key attributes of effective measures; however, CBP had not set an ambitious and realistic target for one measure. Specifically, CBP's target for the land border interception rate—the estimated percentage of major violations in privately owned vehicles that CBP intercepts out of the projected total number of major violations—was lower than the actual reported rate for fiscal years 2015 through 2018.	CBP should develop a new target for the land border interception rate for passengers in privately owned vehicles with major violations that sets an ambitious and realistic goal on the basis of past performance.	Open CBP agreed with this recommendation. In May 2022, CBP officials stated that the COVID-19 pandemic and associated drop in inbound vehicle traffic at land ports of entry has impacted its ability to analyze the land border interception rate. In January 2023, CBP officials estimated that CBP would establish an updated target by the beginning of 2025. We will continue to monitor CBP's ongoing efforts to address this recommendation.

**Appendix I: Other Metrics for Measuring the
Effectiveness of Border Security**

GAO product title and number	Summary and finding	Recommended metric	Status of recommendation implementation as of September 2023
<i>Supply Chain Security: CBP Needs to Enforce Compliance and Assess the Effectiveness of the Importer Security Filing and Additional Carrier Requirements</i> (GAO-17-650)	In July 2017, we reported on CBP's implementation of its Importer Security Filing (ISF) program related to compliance, enforcement, and performance. We found that the ISF rule data have improved CBP's ability to identify high-risk cargo shipments, but CBP could collect additional performance information to better evaluate program effectiveness.	CBP should identify and collect additional performance information on the impact of the ISF rule data, such as the identification of shipments containing contraband, to better evaluate the effectiveness of the ISF program.	Closed – implemented CBP agreed with this recommendation. In March 2022, CBP officials provided documentary evidence to us that CBP had (1) implemented capabilities to identify and capture unmanifested containers, (2) identified the number of times an ISF entity is also a Customs Trade Partnership Against Terrorism (CTPAT) entity, and (3) developed system capabilities to actively display an indicator of a CTPAT entity in targeting systems for targeting personnel to recognize the lower risk of those entities. These actions should allow CBP to better evaluate whether the ISF program is meeting its intended goal of improving the identification of high-risk cargo shipments. Based on these actions, we closed this recommendation as implemented.

Source: GAO analysis of prior GAO reports related to border security effectiveness metrics. | GAO-24-106277

^aThis August 2019 report identified improvements to another metric outside of those mandated by the National Defense Authorization Act and listed in our March 2019 report.

Appendix I: Other Metrics for Measuring the Effectiveness of Border Security

Table 9: Other Metric the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security at the Maritime Border

GAO product title and number	Summary and finding	Recommended metric	Status of recommendation implementation as of September 2023
<i>Coast Guard: Actions Needed to Enhance Performance Information Transparency and Monitoring</i> (GAO-18-13)	In October 2017, we reported on the U.S. Coast Guard's performance goals. We found that although the Coast Guard's performance goals were generally aligned with its statutory missions, the Coast Guard did not explain why certain aspects of mission performance were measured while others were not. We concluded that, in the absence of documentation explaining how existing performance goals address each mission, the extent to which the Coast Guard's performance goals encompass all of its mission activities is unclear.	The Coast Guard should either develop new performance goals to address mission activity gaps or explain in the Coast Guard's Annual Performance Report (APR) why certain aspects of mission performance are measured while others are not.	Closed – implemented The Coast Guard agreed with the recommendation and stated that it would add new measures in future APRs and explain what is measured and what is not, as appropriate. In January 2023, the Coast Guard released its fiscal year 2022 APR. Related to its drug interdiction mission, the fiscal year 2022 APR explains that the Coast Guard tracks multiple illicit drugs in the maritime environment. However, cocaine remains the predominate illicit drug moved via non-commercial maritime conveyances. The APR further states that data collected on other illicit drug interdictions compares trends in removal rates from year to year without annual targets. The description in its APR on how existing data sufficiently assess the performance of each mission provides more meaningful information on progress in achieving the Coast Guard's missions to executive branch decision-makers, Congress, and the public.

Source: GAO analysis of prior GAO reports related to border security effectiveness metrics. | GAO-24-106277

**Appendix I: Other Metrics for Measuring the
Effectiveness of Border Security**

Table 10: Other Metric the Department of Homeland Security (DHS) Could Use to Measure the Effectiveness of Border Security in the Air Environment

GAO product title and number	Summary and finding	Recommended metric	Status of recommendation implementation as of September 2023
<i>Northern Border Security: CBP Identified Resource Challenges but Needs Performance Measures to Assess Security Between Ports of Entry^a</i> (GAO-19-470)	In June 2019, we reported on northern border security efforts. We found that while U.S. Border Patrol and Air and Marine Operations (AMO) have performance measures that assess specific border security operations or programs that include data from the northern border, these measures generally combine data with other border regions and, collectively, the measures do not assess effectiveness at securing the northern border between ports of entry. We concluded that without northern border performance measures, AMO cannot assess its effectiveness at securing the northern border between ports of entry.	AMO should implement performance measures to assess its effectiveness at securing the northern border between ports of entry in the air and maritime environments.	Open AMO agreed with this recommendation and in a May 2023 update, AMO stated that in order to ensure the data collection mechanism is reliable, AMO is collecting a full fiscal year's worth of data from 2023. AMO estimated that the performance measures will be implemented by early December 2023. We will continue to monitor AMO's ongoing efforts.

Source: GAO analysis of prior GAO reports related to border security effectiveness metrics. | GAO-24-106277

Note: The National Defense Authorization Act for Fiscal Year 2017 refers to this domain as "Air and Marine security metrics in the land domain," which it defines as aviation assets and operations of AMO. 6 U.S.C. § 223(e).

^aWe issued this report, which identified an additional metric that DHS could use to measure border security effectiveness, in June 2019 and therefore, was not listed in our March 2019 report. This report also appears in table 7 because it also includes a recommendation related to the between ports of entry domain.

Appendix II: Border Security Metrics as Defined in the National Defense Authorization Act for Fiscal Year 2017

This appendix provides the border security metrics the Department of Homeland Security (DHS) is required to report on as defined in the National Defense Authorization Act for Fiscal Year 2017 (2017 NDAA).¹ This appendix organizes the metrics by each of the four domains listed in the NDAA: (1) metrics for securing the border between ports of entry, (2) metrics for securing the border at ports of entry, (3) metrics for securing the maritime border, and (4) Air and Marine security metrics in the land domain.²

Between Ports of Entry

Estimates—using alternative methodologies where appropriate, including recidivism data, survey data, known-flow data, and technologically measured data—of the five following metrics:

Attempted unlawful border crosser apprehension rate. The rate of apprehension of attempted unlawful border crossers.³

Detected unlawful entries. The number of detected unlawful border crossers who enter the U.S. and are not apprehended by a border security component of DHS.⁴

Estimated undetected unlawful entries. The number of estimated undetected unlawful border crossers who enter the U.S. and are not apprehended by a border security component of DHS.⁵

Turn backs. The number of unlawful border crossers who, after making unlawful entries into the U.S., respond to U.S. enforcement efforts by returning promptly to the country from which they entered.⁶

¹Pub. L. No. 114-328, div. A, title X, subtitle G, § 1092, 130 Stat. 2000, 2429-36 (2016) (classified at 6 U.S.C. § 223).

²Previously in this report, we refer to the fourth domain as “air environment” because the 2017 NDAA defines it as aviation assets and operations of Customs and Border Protection’s Air and Marine Operations (AMO). 6 U.S.C. § 223(e)(1).

³6 U.S.C. § 223(b)(1)(A)(i).

⁴Id. at § 223(a)(11), (b)(1)(A)(ii).

⁵Id. at § 223(a)(11), (b)(1)(A)(iii).

⁶Id. at § 223(a)(9), (b)(1)(A)(iv).

Got aways. The number of unlawful border crossers who—(A) are directly or indirectly observed making unlawful entries into the U.S., (B) are not apprehended, and (C) are not turn backs.⁷

Measurement of situational awareness achieved in each U.S. Border Patrol sector. Measurement of the knowledge and understanding of current unlawful cross-border activity, for each U.S. Border Patrol sector, including the following: (A) threats and trends concerning illicit trafficking and unlawful crossings, (B) the ability to forecast future shifts in such threats and trends, (C) the ability to evaluate such threats and trends at a level sufficient to create actionable plans, and (D) the operational capability to conduct persistent and integrated surveillance of the international borders of the U.S.⁸

Unlawful border crossing effectiveness rate in each U.S. Border Patrol sector. For each U.S. Border Patrol sector, the percentage that results from dividing the number of apprehensions and turn backs by the sum of the number of apprehensions, estimated undetected unlawful entries, turn backs, and got aways.⁹

Probability of detection rate. Rate that compares the estimated total unlawful border crossing attempts not detected by U.S. Border Patrol to the unlawful border crossing effectiveness rate, as informed by the attempted unlawful border crosser apprehension rate; the number of detected unlawful entries, turn backs, and got aways; and the number of estimated undetected unlawful entries.¹⁰

Apprehensions in each U.S. Border Patrol sector. The number of apprehensions in each U.S. Border Patrol sector.¹¹

⁷Id. at § 223(a)(3), (b)(1)(A)(v).

⁸Id. at § 223(a)(7), 223(b)(1)(B).

⁹Id. at § 223(a)(10), (b)(1)(C).

¹⁰Id. at § 223(a)(3), (9), (11), (b)(1)(D).

¹¹Id. at § 223(b)(1)(E).

Apprehensions of unaccompanied alien children. The number of apprehensions, and nationality of such unaccompanied children, in each U.S. Border Patrol sector.¹²

Apprehensions of family units. The number of apprehensions of family units, and the nationality of such family units, in each U.S. Border Patrol sector.¹³

Between the ports illicit drug seizure rate. Rate for illicit drugs seized by U.S. Border Patrol between ports of entry, which compares the ratio of the amount and type of illicit drugs seized between ports of entry in any fiscal year to the average of the amount and type of illicit drugs seized between ports of entry in the immediately preceding 5 fiscal years.¹⁴

Estimates of the impact of the Consequence Delivery System on recidivism. Estimates of the impact on the rate of recidivism of unlawful border crossers over multiple fiscal years of the Consequence Delivery System, which is the series of consequences applied by U.S. Border Patrol in collaboration with other federal agencies to persons unlawfully entering the U.S. in order to prevent unlawful border crossing recidivism.¹⁵

Examination of each consequence under the Consequence Delivery System. An examination of each of the following consequences under the Consequence Delivery System: (i) voluntary return, (ii) warrant of arrest or notice to appear, (iii) expedited removal, (iv) reinstatement of removal, (v) alien transfer exit program, (vi) criminal consequence program, (vii) standard prosecution, and (viii) Operation Against Smugglers Initiative on Safety and Security.¹⁶

At Ports of Entry

¹²Id. at §§ 223(b)(1)(F), 279(g)(2).

¹³Id. at § 223(b)(1)(G).

¹⁴Id. at § 223(b)(1)(H).

¹⁵Id. at § 223(a)(2), (11), (b)(1)(I).

¹⁶Id. at § 223(b)(1)(J). For more information on the Consequence Delivery System, see GAO, *Border Patrol: Actions Needed to Improve Oversight of Post-Apprehension Consequences*, [GAO-17-66](#) (Washington, D.C.: Jan. 12, 2017).

Estimates—using alternative methodologies where appropriate, including recidivism data, survey data, and randomized secondary screening data—of the three following metrics:

Total inadmissible travelers at ports of entry. The total inadmissible travelers who attempt to, or successfully, enter the U.S. at a port of entry.¹⁷

Refusal and interdiction rate at ports of entry. The rate of refusals and interdictions for travelers who attempt to, or successfully, enter the U.S. at a port of entry.¹⁸

Unlawful entries at ports of entry. The number of unlawful entries at a port of entry.¹⁹

Illicit drugs seized at ports of entry. The amount and type of illicit drugs seized by the U.S. Customs and Border Protection's (CBP) Office of Field Operations (OFO) at ports of entry during the previous fiscal year.²⁰

Port of entry illicit drugs seizure rate. Illicit drugs seizure rate for drugs seized by OFO, which compares the ratio of the amount and type of illicit drugs seized OFO in any fiscal year to the average of the amount and type of illicit drugs seized by OFO in the immediately preceding 5 fiscal years.²¹

Major infractions at ports of entry. The number of infractions related to travelers and cargo committed by major violators who are interdicted by OFO at ports of entry, and the estimated number of such infractions committed by major violators who are not so interdicted. Major violators are persons or entities that have engaged in serious criminal activities at any land, air, or sea port of entry, including the following: (A) possession of illicit drugs, (B) smuggling of prohibited products, (C) human smuggling, (D) possession of illegal weapons, (E) use of fraudulent

¹⁷6 U.S.C. § 223(c)(1)(A)(i); 8 U.S.C. § 1182(a).

¹⁸6 U.S.C. § 223(c)(1)(A)(ii).

¹⁹Id. at § 223(a)(11), (c)(1)(A)(iii).

²⁰Id. at § 223(c)(1)(B).

²¹Id. at § 223(c)(1)(C).

documents, and (F) any other offense that is serious enough to result in an arrest.²²

Cocaine seizures effectiveness rate. In consultation with the heads of the Office of National Drug Control Policy and the U.S. Southern Command, a cocaine seizure effectiveness rate, which is the percentage resulting from dividing the amount of cocaine seized by OFO by the total estimated cocaine flow rate at ports of entry along the U.S. land border with Mexico and Canada.²³

A measurement of how border security operations affect crossing times, including the four following metrics:

Ratio of average wait times and traffic volume. A wait time ratio that compares the average wait times to total commercial and private vehicular traffic volumes at each land port of entry.²⁴

Infrastructure capacity utilization rate. An infrastructure capacity utilization rate that measures traffic volume against the physical and staffing capacity at each land port of entry.²⁵

Secondary examination rate. Rate that measures the frequency of secondary examinations at each land port of entry.²⁶

Secondary examinations effectiveness rate. Enforcement rate that measures the effectiveness of such secondary examinations at detecting major violators.²⁷

A seaport scanning rate that includes the four following metrics:

Number of potentially “high-risk” cargo containers. The number of all cargo containers that are considered potentially

²²Id. at § 223(a)(5), (c)(1)(D).

²³Id. at § 223(c)(1)(E).

²⁴Id. at § 223(c)(1)(F)(i).

²⁵Id. at § 223(c)(1)(F)(ii).

²⁶Id. at § 223(c)(1)(F)(iii).

²⁷Id. at § 223(c)(1)(F)(iv).

“high-risk”, as determined by the Executive Assistant
Commissioner of OFO.²⁸

Ratio of potentially high-risk cargo containers scanned relative to high-risk containers entering in previous fiscal year. A comparison of the number of potentially high-risk cargo containers scanned by OFO at each sea port of entry during a fiscal year to the total number of high-risk cargo containers entering the U.S. at each such sea port of entry during the previous fiscal year.²⁹

Potentially high-risk cargo containers scanned upon U.S. arrival by sea. The number of potentially high-risk cargo containers scanned upon arrival at a U.S. sea port of entry.³⁰

Potentially high-risk cargo containers scanned before U.S. arrival by sea. The number of potentially high-risk cargo containers scanned before arrival at a U.S. sea port of entry.³¹

Maritime Border

Situational awareness achieved in the maritime environment.

Knowledge and understanding of current unlawful cross-border activity in the maritime environment, including the following: (A) threats and trends concerning illicit trafficking and unlawful crossings, (B) the ability to forecast future shifts in such threats and trends, (C) the ability to evaluate such threats and trends at a level sufficient to create actionable plans, and (D) the operational capability to conduct persistent and integrated surveillance of the international borders of the U.S.³²

Known maritime migrant flow rate. An unspecified rate of known maritime migrant flow, which flow is the sum of the number of undocumented migrants—(A) interdicted in the waters over which the U.S. has jurisdiction; (B) identified at sea either directly or indirectly, but not interdicted; (C) if not described in (A) or (B), who were otherwise

²⁸Id. at § 223(c)(1)(G)(i).

²⁹Id. at § 223(c)(1)(G)(ii).

³⁰Id. at § 223(c)(1)(G)(iii).

³¹Id. at § 223(c)(1)(G)(iv).

³²Id. at § 223(a)(7), (d)(1)(A).

reported, with a significant degree of certainty, as having entered, or attempted to enter, the U.S. through the maritime border.³³

Illicit drugs removal rate. Rate for drugs removed inside and outside of a transit zone, which compares the amount and type of illicit drugs removed, including drugs abandoned at sea, by DHS maritime security components in any fiscal year to the average of the amount and type of illicit drugs removed by such maritime components for the immediately preceding 5 fiscal years. The term “transit zone” means the sea corridors of the western Atlantic Ocean, the Gulf of Mexico, the Caribbean Sea, and the eastern Pacific Ocean through which undocumented migrants and illicit drugs transit, either directly or indirectly, to the U.S.³⁴

Cocaine removal effectiveness rate. In consultation with the heads of the Office of National Drug Policy and the U. S. Southern Command, a rate for cocaine removed inside a transit zone and outside a transit zone that compares the amount of cocaine removed by DHS maritime security components with the total documented cocaine flow rate, as contained in federal drug databases.³⁵

DHS known maritime threat response rate. Rate that compares the ability of the maritime security components of DHS to respond to and resolve known maritime threats, whether inside or outside a transit zone, by placing assets on-scene, with the total number of events with respect to which DHS has known threat information.³⁶

Intergovernmental actionable maritime threat response rate. Rate that compares the ability of the maritime security components of DHS or other U. S. government entities to respond to and resolve actionable maritime threats, whether inside or outside a transit zone, with the number of such threats detected.³⁷

Air and Marine Security in the Land Domain

³³Id. at § 223(a)(4), (d)(1)(B).

³⁴Id. at § 223(a)(8), (d)(1)(C).

³⁵Id. at § 223(a)(8), (d)(1)(D).

³⁶Id. at § 223(d)(1)(E).

³⁷Id. at § 223(a)(8), (d)(1)(F).

Flight hour effectiveness rate. Rate that compares CBP Air and Marine Operations (AMO) flight hours requirements the number of flight hours flown by AMO.³⁸

Funded flight hour effectiveness rate. Rate that compares the number of funded flight hours appropriated to AMO to the number of actual flight hours flown by AMO.³⁹

AMO readiness rate. Rate that compares the number of aviation missions flown by AMO to the number of aviation missions cancelled by AMO due to maintenance, operations, or other causes.⁴⁰

AMO weather-related cancellation rate. The number of missions AMO cancelled due to weather compared to the total number of planned missions.⁴¹

Individuals detected by AMO. The number of individuals detected by AMO through the use of unmanned aerial systems and manned aircraft.⁴²

Apprehensions assisted by AMO. The number of apprehensions assisted by AMO through the use of unmanned aerial systems and manned aircraft.⁴³

Illicit drug seizures assisted by AMO. The number and quantity of illicit drug seizures assisted by AMO through the use of unmanned aerial systems and manned aircraft.⁴⁴

³⁸Id. at § 223(e)(1)(A).

³⁹Id. at § 223(e)(1)(B).

⁴⁰Id. at § 223(e)(1)(C).

⁴¹Id. at § 223(e)(1)(D).

⁴²Id. at § 223(e)(1)(E).

⁴³Id. at § 223(e)(1)(F).

⁴⁴Id. at § 223(e)(1)(G).

AMO actionable intelligence. The number of times that actionable intelligence related to border security was obtained through the use of unmanned aerial systems and manned aircraft.⁴⁵

⁴⁵Id. at § 223(e)(1)(H).

Appendix III: Comments from the Department of Homeland Security

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



**Homeland
Security**

October 31, 2023

Rebecca Gambler
Director, Homeland Security & Justice Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548-0001

Re: Management Response to Draft Report GAO-24-106277, "Reporting of Border Security Metrics Could Be Improved"

Dear Ms. Gambler:

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

DHS leadership is pleased to note GAO's recognition that DHS's fiscal year (FY) 2021 Border Security Metrics Report (BSMR) made improvements on previous reports, such as implementing a prior GAO recommendation to include measures of statistical uncertainty for all metrics that rely on its statistical model. Securing the U.S. borders is a complex undertaking for which DHS has made significant investments over the years. Accordingly, DHS continues to make important contributions in providing data and information on the changing state of border security for stakeholders to understand the effectiveness of these investments.

The DHS Office of Strategy, Policy, and Plans (PLCY) acknowledges the issues, challenges, and limitations GAO found in the FY 2021 BSMR, which were addressed to a notable degree in the development of the FY 2022 and 2023 BSMR. PLCY discussed its efforts to address the FY 2021 BSMR issues with GAO during this audit, including informing the audit team of engagements with Components to interpret metric requirements from Congress to source data, and to report on the last metrics (planned to be complete in 2024 report). PLCY also continued meeting with Congressional staff to

Appendix III: Comments from the Department
of Homeland Security

inform Congress of the new Office of Homeland Security Statistics (OHSS),¹ as well as update committees on DHS's creation of the Migration Analysis Center (MAC),² which both provide modeling capabilities that include focus on border activities and challenges. DHS continues to build rapport for future discussions to get clarity on topics related to border security, highlight OHSS reporting, and solicit requirements for new reporting and to reduce outdated reporting.

The draft report contained four recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

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

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2023.10.31 14:37:17 -0400

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Enclosure

¹ On September 29, 2023, Secretary of Homeland Security Alejandro N. Mayorkas signed a memorandum formally establishing OHSS. OHSS creates objective, credible, accurate, relevant, timely, and authoritative statistical homeland security data products to increase transparency for the interagency, Congress, and the public and to support internal evidence-based policymaking and leadership decisions.

² The Joint Explanatory Statement accompanying the FY 2022 DHS Appropriations Bill directed the establishment of the MAC and provided funding above President's request to establish the MAC. The MAC works with other parts of DHS, the interagency, and private sector partners to support evidence-based policymaking by leading enterprise-wide research on the causes and consequences of U.S. immigration and the impacts of migration-related policies and programs.

**Enclosure: Management Response to Recommendations
Contained in GAO-24-106277**

GAO recommended the Under Secretary for PLCY:

Recommendation 1: Take steps to engage with components to more fully report the metrics as defined by the 2017 NDAA [National Defense Authorization Act for Fiscal Year 2017] in its Border Security Metrics Report.

Response: Concur. PLCY met with U.S. Coast Guard's (USCG) and U.S. Customs and Border Protection's (CBP) operational sub-components in three meetings in June 2023 to discuss: (1) scoping, sourcing data, and reporting on two additional metrics for the FY 2022 BSMR associated primarily with USCG maritime activities; (2) scoping, sourcing, and reporting on two more metrics for the FY 2023 BSMR associated with CBP activities; (3) scoping, sourcing, and reporting on two metrics for the FY 2024 BSMR associated with CBP activities. In addition, PLCY communicated with the RAND Corporation and CBP regarding a projected model update to address challenges of the interruption to participation in the Mexican survey due to restrictions of social engagement during the Coronavirus Disease 2019 pandemic. PLCY expects the FY 2023 BSMR to be released in November 2023 and the FY 2024 BSMR to be released in late summer of 2024. Estimated Completion Date (ECD): October 31, 2024.

Recommendation 2: Periodically engage with Congress to improve the usefulness of information in its Border Security Metrics Report.

Response: Concur. In FY 2023, PLCY informed, and met with, congressional staff on establishment of the OHSS and updated the U.S House of Representatives Judiciary Committee, House Committee on Appropriations, and U.S. Senate Committee on Appropriations on establishment of the MAC. During these engagements, PLCY highlighted its increasing modeling capabilities to report on border activities as well as challenges in reporting. As OHSS transitions to full capabilities and attains Office of Management and Budget's endorsement as an independent Recognized Statistical Agency or Unit, PLCY expects more direct engagement with congressional staff to share data (such as via a standing weekly provision of data), clarify reporting details, and identify data requirements. ECD: October 31, 2024.

Recommendation 3: Assess the extent to which its choice of input administrative data and model type for its statistical model of deterrence remains sufficiently predictive, and document the results.

Response: Concur. PLCY is exploring alternative methods to produce defensible estimates of unauthorized entries due to challenges with the current model. This may involve assessments of the current statistical model of deterrence, its predictiveness, and use of alternative sources of administrative data. Further discussion of the new methodology and its results will be provided in the future report, once a methodology is finalized. ECD: October 31, 2024.

Recommendation 4: Use the results of its assessment to update or inform its efforts to replace its statistical model of deterrence, as appropriate.

Response: Concur. Any results of assessments of the current model of deterrence are, and will continue to be, used to inform research into alternative methods of producing estimates of unauthorized entries. In August 2023, OHSS worked with the RAND Corporation, the Homeland Security Operational Analysis Center, and Federally Funded Research and Development Centers to deliver an assessment and recommendations for alternative modeling to the CBP Planning, Analysis, and Requirements Evaluation team regarding its Operational Performance Simulator (OPS), which is being considered as the source of FY 2022 estimates of unauthorized entries in the FY 2023 Border Security Metrics Report. Future reports may rely on OPS or may use an alternative methodology. ECD: October 31, 2024.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Rebecca Gambler, at (202) 512-8777 or gambler@gao.gov

Staff Acknowledgements

In addition to the contact named above, Taylor Matheson (Assistant Director), Emily Hutz (Analyst-in-Charge), Benjamin Crossley, Dominick Dale, Michele Fejfar, Sasan J. “Jon” Najmi, Cristina Norland, Christine Stenglein, and Jeff Tessin made key contributions to this report.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548





U.S. DEPARTMENT OF HOMELAND SECURITY **OFFICE OF INSPECTOR GENERAL**

OIG-24-10

January 9, 2024

FINAL REPORT

Summary of Previously Issued Recommendations and Other Insights to Improve Operational Conditions at the Southwest Border





OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

January 9, 2024

MEMORANDUM FOR:

Troy A. Miller
Senior Official Performing the Duties of the
Commissioner
U.S. Customs and Border Protection

Patrick J. Lechleitner
Senior Official Performing the Duties of the
Director
U.S. Immigration and Customs Enforcement

The Honorable Ur M. Jaddou
Director
U.S. Citizenship and Immigration Services

FROM:

Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V
CUFFARI

Digitally signed by
JOSEPH V CUFFARI
Date: 2024.01.09
16:50:48 -07'00'

SUBJECT:

*Summary of Previously Issued Recommendations and Other Insights
to Improve Operational Conditions at the Southwest Border*

Attached for your action is our final report, *Summary of Previously Issued Recommendations and Other Insights to Improve Operational Conditions at the Southwest Border*. We incorporated the formal comments provided by your office. The report contains no recommendations.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies our report to congressional committees with oversight and appropriations responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

Summary of Previously Issued Recommendations and Other Insights to Improve Operational Conditions at the Southwest Border

January 9, 2024

Why We Did This Review

The number of migrant encounters along the Southwest border dramatically increased during FYs 2018 through 2022, growing from more than 500,000 in FY 2018 to more than 2.3 million in FY 2022.

We conducted this review to summarize our prior work on the Southwest border and identify related common issues.

What We Recommend

The report does not contain recommendations.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

During fiscal years 2018 through 2022, we issued 61 reports and 178 recommendations for improving conditions at the Southwest border. As of August 17, 2023, 144 recommendations were closed, 31 recommendations were resolved and open, and 3 recommendations remained unresolved.

Based on our recommendation analysis, we identified 10 program management deficiency categories associated with the 178 recommendations, with the top five categories accounting for 143 (80 percent) of the recommendations as follows:

- Compliance with Requirements 52 recommendations
- Program Guidance 44 recommendations
- Strategic Planning 20 recommendations
- Evaluation of Resources 15 recommendations
- Collaboration 12 recommendations

The results of our recommendation analysis may be indicative of similar program management deficiencies affecting other Southwest border programs and operations due to the number of times the recommendations were associated with the same program deficiency from our 61 prior reports.

Additionally, we interviewed Department of Homeland Security component officials to obtain their perspectives on current Southwest border operations. Officials described difficulties in staffing and resources, workloads, system capabilities and integration, and policies and procedures, which correspond to categories we identified from our prior work. DHS should learn from these common deficiencies identified in our analysis and from other insights in this summary report to better address conditions at the Southwest border.

DHS Response

Even though this report contains no recommendations, DHS provided a management response, which is included in its entirety in Appendix B.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table of Contents

Background	1
Results of Review	3
Analysis of Prior Recommendations Highlights Program Management Deficiencies	4
Issues Affecting Current Southwest Border Operations.....	12
Conclusion	16
Management Comments and OIG Analysis.....	16
Appendix A: Objective, Scope, and Methodology	19
DHS OIG's Access to DHS Information.....	20
Appendix B: DHS Comments on the Draft Report.....	21
Appendix C: List of Reports Included in This Review.....	26
Appendix D: Report Distribution	32

Abbreviations

Border Patrol	U.S. Border Patrol
CBP	U.S. Customs and Border Protection
ICE	U.S. Immigration and Customs Enforcement
NFR	Notice of Findings and Recommendations
OFO	Office of Field Operations
OMB	Office of Management and Budget
PBNDS	ICE Performance-Based National Detention Standards
SBCC	Southwest Border Coordination Center
TEDS	CBP National Standards on Transport, Escort, Detention, and Search
USCIS	U.S. Citizenship and Immigration Services



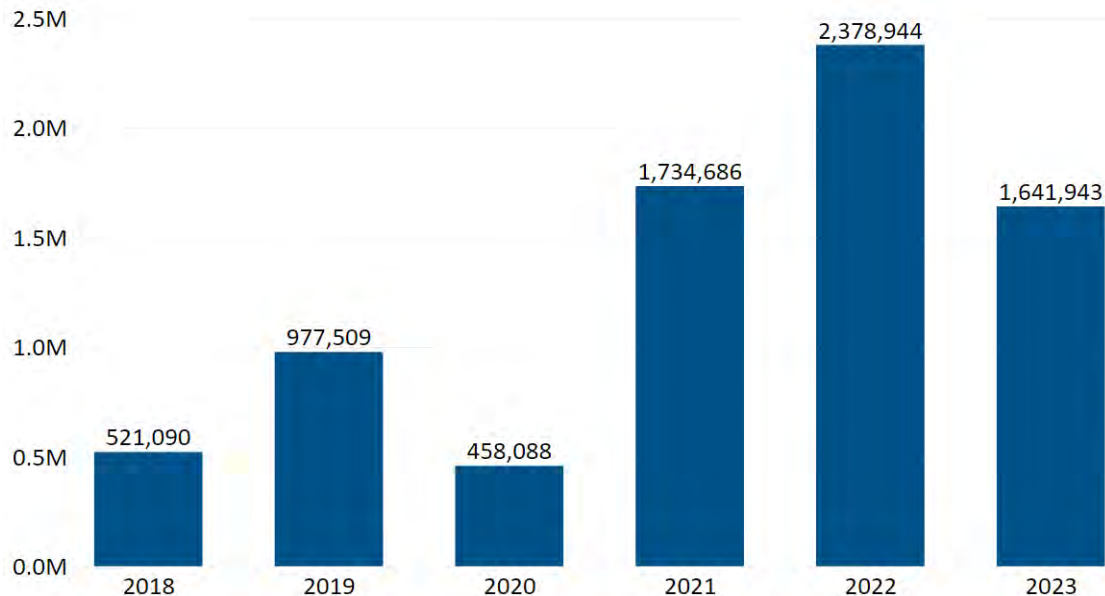
OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Background

The Department of Homeland Security is responsible for securing and managing air, land, and maritime borders; securing the Nation against potential threats; and enforcing and administering U.S. immigration laws. In previous years, hundreds of thousands of migrants attempted to enter the United States, legally and illegally, through the border with Mexico (Southwest border). The number of migrant encounters along the Southwest border dramatically increased between fiscal years 2018 and 2022, growing from more than 500,000 to more than 2.3 million.¹ See Figure 1 for U.S. Customs and Border Protection (CBP) encounters at the Southwest border. During this same time, the Federal Government invested approximately \$67 billion² in support of DHS' mission at the Southwest border.

Figure 1. FYs 2018 – 2023 Year-to-Date CBP Encounters at the Southwest Border³



Source: Prepared by DHS Office of Inspector General using CBP encounter data from CBP website

¹ Encounters are tracked by the number of “apprehensions” and “inadmissibles.” Apprehensions refers to physical control or temporary detainment of a person not lawfully in the United States by U.S. Border Patrol (Border Patrol), which may or may not result in an arrest. Inadmissibles refers to individuals who are encountered by Office of Field Operations (OFO) at ports of entry seeking lawful admission into the United States but are determined to be inadmissible; individuals presenting themselves to seek humanitarian protection under our laws; and individuals who withdraw an application for admission and return to their countries of origin within a short timeframe.

² *Department of Homeland Security U.S. Customs and Border Protection, Budget Overview, Congressional Justification* and *Department of Homeland Security U.S. Immigration and Customs Enforcement, Budget Overview, Congressional Justification* for FYs 2020 through 2024.

³ FY 2023 data is year to date as of June 7, 2023.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Within DHS, CBP and U.S. Immigration and Customs Enforcement (ICE) are the primary components responsible for enforcing immigration laws and securing U.S. borders. The Southwest border accounts for about one-third of the country's approximately 6,000 miles of border. U.S. Citizenship and Immigration Services (USCIS) supports the border mission by interviewing migrants who claim asylum based on credible fear. Table 1 shows DHS component roles and responsibilities at the Southwest border.

Table 1. DHS Component Roles and Responsibilities at the Southwest Border⁴

Component	Subcomponent	Responsibilities at the Border
CBP	Border Patrol	Agents apprehend individuals illegally crossing the border between ports of entry.
	OFO	Officers inspect and examine people and goods entering and leaving the country at ports of entry.
ICE	Enforcement and Removal Operations	Deportation officers manage long-term custody of noncitizens in detention facilities nationwide, and they deport individuals who are illegally in the country.
	Homeland Security Investigations	Agents investigate, disrupt, and dismantle terrorist, transnational, and other criminal organizations exploiting the customs and immigration laws of the United States.
USCIS	Refugee, Asylum, and International Operations	Asylum officers conduct credible fear screenings of noncitizens referred to USCIS and make determinations.

Source: DHS OIG analysis of DHS component roles and responsibilities at the Southwest border

During FYs 2018 through 2022, we issued 61 reports, which included 18 audits, 23 inspections and reviews, and 20 unannounced inspections related to the Southwest border, with 178 recommendations to DHS, CBP, and ICE. The 61 reports included in our review focus on specific Southwest border programs and operations and unannounced inspections of CBP and ICE detention facilities at the Southwest border. DHS OIG is congressionally mandated to conduct unannounced inspections of CBP and ICE detention facilities to evaluate compliance with

⁴ Table 1 does not include all CBP, ICE, and USCIS subcomponents' roles and responsibilities.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

applicable detention standards. CBP's holding facilities are required to comply with National Standards on Transport, Escort, Detention, and Search (TEDS), which specify how detainees should be treated in CBP custody. Each ICE detention facility must comply with one of several national detention standards, such as the Performance-Based National Detention Standards (PBNDS). The recommendations in the 61 reports aim to address deficiencies identified during our audits and inspections.

We conducted this review to summarize the results of our prior work on the Southwest border and identify related common issues.

Results of Review

During FYs 2018 through 2022, we issued 61 reports and 178 recommendations for improving conditions at the Southwest border. As of August 17, 2023, 144 recommendations were closed, 31 recommendations were resolved and open, and 3 recommendations remained unresolved.⁵

Based on our recommendation analysis, we identified 10 program management deficiency categories associated with the 178 recommendations, with the top five categories accounting for 143 (80 percent) of the recommendations as follows:

• Compliance with Requirements	52 recommendations
• Program Guidance	44 recommendations
• Strategic Planning	20 recommendations
• Evaluation of Resources	15 recommendations
• Collaboration	12 recommendations

The results of our recommendation analysis may be indicative of similar program management deficiencies affecting other Southwest border programs and operations due to the number of times the recommendations were associated with the same program deficiency from our 61 prior reports.

⁵ According to DHS OIG Directive Number OIG-PTS-2, July 1, 2010, titled *Determining a Recommendation's Status*, a recommendation is considered Open when agreed-upon corrective action has not been implemented. Open recommendations may be unresolved or resolved. A recommendation is considered Unresolved and Open when a management decision has not been received by OIG, or, if received, OIG has determined that the action does not meet the recommendation requirements. A recommendation is considered Resolved and Open when a management decision has been received and OIG determines that the action meets the recommendation requirements. A recommendation is Closed if (1) a resolved management decision has been implemented; (2) the Resolution Official makes the decision not to implement the recommendation; or (3) OIG closes the recommendation at its own discretion.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Additionally, we interviewed DHS component officials to obtain their perspectives on current Southwest border operations. Officials described difficulties in staffing and resources, workloads, system capabilities and integration, and policies and procedures, which correspond to the categories we identified from our prior work.

DHS should learn from these common deficiencies identified in our analysis and from other insights in this summary report to better address conditions at the Southwest border.

Analysis of Prior Recommendations Highlights Program Management Deficiencies

During FYs 2018 through 2022, we issued 61 reports related to the Southwest border, with 178 recommendations to DHS, CBP, and ICE. See Appendix C for the complete list of DHS OIG reports. As of August 17, 2023, 144 of the 178 recommendations are closed (81 percent), 31 recommendations are resolved and open (17 percent), and 3 recommendations are unresolved and open (2 percent).

We conducted an analysis of these 178 recommendations and determined they could be grouped into 10 program management deficiency categories. We ranked the categories based on the total number of recommendations assigned to each. The results of our analysis are presented in Table 2.

Table 2. Recommendations Grouped into 10 Program Management Deficiency Categories

Rank	Program Management Deficiency	No. of Recs	Percent of Total
1	Compliance with Requirements	52	29%
2	Program Guidance	44	25%
3	Strategic Planning	20	11%
4	Evaluation of Resources	15	8%
5	Collaboration	12	7%
6	Program Monitoring	9	5%
7	Training	8	5%
8	Data Collection	7	4%
9	System Interoperability	6	3%
10	Maintenance of Records	5	3%
Grand Total		178	100%

Source: DHS OIG results of analysis from prior recommendations



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Top Five Categories Account for 80 percent of Total Recommendations

Compliance with Requirements

During FYs 2018 through 2022, we issued 19 reports containing 52 recommendations pertaining to this category. Compliance with requirements ensures that DHS and its components are consistently conducting program activities according to program objectives and within the governing laws, regulations, and standards to achieve the Department's mission at the Southwest border.

Our recommendations were intended to ensure DHS and its components complied with Federal and DHS requirements. For example:

- In OIG 22-57, *El Paso Sector Border Patrol Struggled with Prolonged Detention and Consistent Compliance with TEDS Standards*, we reported CBP did not meet TEDS standards; specifically, we identified inconsistency with implementation of standards related to segregating juveniles from unrelated adults or legal guardians and the provision of interpretation services to detained individuals. We recommended CBP develop and implement quality assurance and quality control tools to ensure the provision of interpretation services, particularly during the medical screening process. CBP's actions were sufficient to close this recommendation on July 24, 2023.
- In OIG 21-18, *CBP Needs Additional Oversight to Manage Storage of Illicit Drugs (REDACTED)*, we reported that CBP approved waivers without ensuring that ICE denied requests to store drug amounts exceeding established thresholds or that requests included an Assistant Attorney General appeal as required in CBP's *Seized Asset Management and Enforcement Procedures Handbook*. We recommend CBP ensure that requests to store drug amounts exceeding established thresholds are automatically denied. CBP's actions were sufficient to close this recommendation on July 1, 2021.
- In OIG 21-12, *ICE Needs to Address Prolonged Administrative Segregation and Other Violations at the Imperial Regional Detention Facility*, we reported that administrative segregation was being used as a long-term solution for detainees in protective custody and overly restricted detainees by not offering privileges similar to those offered to detainees in general housing units. We recommended ICE direct the San Diego Enforcement and Removal Operations Office responsible for the facility to ensure that detainees in administrative segregation are provided outdoor recreation and access to privileges similar to those offered to detainees in the general population in compliance with 2011 PBNDS requirements. ICE's actions were sufficient to close this recommendation on May 4, 2021.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- In *OIG 21-12, ICE Needs to Address Prolonged Administrative Segregation and Other Violations at the Imperial Regional Detention Facility*, we reported the living conditions at the facility not only violated ICE detention standards, but in some instances, could pose health and safety risks to detainees. We recommended ICE direct the San Diego Enforcement and Removal Operations Office responsible for the facility to review the facility's conditions we identified as deficient to ensure corrective action in compliance with 2011 PBNDS requirements. ICE's actions were sufficient to close this recommendation on May 4, 2021.
- In *OIG 21-02, CBP Has Taken Steps to Limit Processing of Undocumented Aliens at Ports of Entry*, we reported that, without prior public notice, CBP stopped processing most undocumented aliens,⁶ including asylum seekers, at seven Class A ports of entry and redirected them to other port locations.⁷ We recommended CBP resume processing undocumented aliens at these ports of entry or formally redesignate the ports to exclude undocumented aliens. At report issuance, CBP did not concur with this recommendation. However, in August 2022, CBP provided an updated corrective action plan, which was accepted by DHS OIG. This recommendation was resolved and open as of August 17, 2023.⁸

CBP and ICE implemented corrective actions that enabled us to close 44 of the 52 recommendations. Additionally, seven recommendations were resolved and open, and one recommendation was unresolved and open as of August 17, 2023.⁹

⁶ CBP refers to individuals who are not in possession of documents allowing them entry into the United States — e.g., a travel visa — as undocumented aliens.

⁷ These ports are classified as Class A ports under Title 8, Section 100.4 of the Code of Federal Regulations. Class A ports are designated for all aliens. CBP has authority to change a port's classification. When changing a port's classification in the past, CBP has published a final rule in the *Federal Register*.

⁸ CBP did not concur with the recommendation when the report was issued on October 27, 2020. However, CBP provided an update on August 9, 2022, indicating it was gathering and analyzing data to determine what action should be taken considering potential regulatory changes to Title 42. DHS OIG approved CBP's action plan and changed the recommendation's status to resolved and open on October 26, 2022. The target completion date for corrective action was May 31, 2023. Title 42 COVID-19 authority expired on May 11, 2023.

⁹ In addition to the unresolved recommendation discussed in footnote 8 above, ICE did not concur with the recommendation in *OIG-22-31, Management Alert – Immediate Removal of All Detainees from the Torrance County Detention Facility*, for ICE to remove all detainees from the facility until it ensured adequate staffing and appropriate living conditions. ICE responded that it complied with staffing level requirements and that it had made all necessary repairs. However, DHS OIG did not receive any documentation to support the statements made in ICE's response. The status of this recommendation remains unresolved and open.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Program Guidance

During FYs 2018 through 2022, we issued 24 reports containing 44 recommendations pertaining to this category. Program guidance ensures that DHS conducts its critical functions consistently and reliably in order to execute its Southwest border mission effectively and efficiently.

Our recommendations were intended to help DHS develop, revise, or update guidance, policies, and procedures. For example:

- In OIG 22-80, *Del Rio Area Struggled with Prolonged Detention, Consistent Compliance with CBP's TEDS Standards, and Data Integrity*, we reported during an inspection of a CBP Border Patrol facility that we observed the use of a bar-coded wristband system to track the handling, retention, retrieval, and return of detainee personal property along with the use of supplemental procedures to clarify the handling and secure storage of personal property. We considered this to be a best practice and recommended CBP assess whether the Eagle Pass soft-sided facility's supplemental guidance on the management of detainee property could be developed and implemented sector-wide, and to implement where operationally feasible. This recommendation was resolved and open as of August 17, 2023.
- In OIG 22-71, *U.S. Border Patrol Screened Migrants at the Southwest Border but Could Strengthen Processes*, we reported that CBP did not issue a formal policy detailing how to expedite the processing of migrants as apprehension numbers continued to rise. We recommended CBP develop and implement a comprehensive policy to use different pathways for expedited processing during times of increased apprehension activity. CBP's actions were sufficient to close this recommendation on February 17, 2023.
- In OIG 22-57, *El Paso Sector Border Patrol Struggled with Prolonged Detention and Consistent Compliance with TEDS Standards*, we reported that Border Patrol agents utilized the Ysleta OFO ports of entry for expelling migrants subject to immediate Title 42 authorities. Even though this practice created operational efficiencies, formal documentation or guidance could have defined roles and responsibilities, as well as aided in the coordination and documentation of migrants. We recommended CBP clarify and document existing procedures to formalize Border Patrol's use of OFO facilities. CBP's actions were sufficient to close this recommendation on February 21, 2023.
- In OIG 19-67, *Limitations of CBP OFO's Screening Device Used to Identify Fentanyl and Other Narcotics*, we reported that CBP had not issued guidance on standard use of small-scale chemical screening devices to detect illicit narcotics. We recommended CBP develop a formal strategy to deploy and use small-scale chemical screening devices and



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

keep them updated. CBP's actions were sufficient to close this recommendation on September 13, 2022.

- In OIG 18-76, *Assaults on CBP and ICE Law Enforcement Officers*, we reported that CBP and ICE did not have specific guidance on reporting acts of resistance or attempted assaults on law enforcement officers. We issued two recommendations that CBP and ICE clarify guidance on the types of assaults that must be officially reported, as well as the steps in the reporting process. CBP and ICE's actions were sufficient to close these recommendations on July 19, 2019, and September 4, 2018, respectively.

CBP and ICE implemented corrective actions that enabled us to close 37 of the 44 recommendations. The remaining seven recommendations were resolved and open as of August 17, 2023.

Strategic Planning

During FYs 2018 through 2022, we issued 13 reports containing 20 recommendations to strengthen strategic planning for Southwest border operations. Effective strategic planning positions DHS to better consider risks, resources, and alternative options for mission success.

Our recommendations were intended to help DHS develop strategies, plans, and objectives to achieve various goals and missions. For example:

- In OIG 22-68, *U.S. Border Patrol Faces Challenges Administering Post-Apprehension Outcomes Consistently Across Sectors*, we reported that CBP appeared unprepared to meet increased processing burdens when a Centers for Disease Control and Prevention order was terminated.¹⁰ A CBP official stated that there were no contingency plans for when the Centers for Disease Control and Prevention order expired. We recommended CBP develop and implement contingency plans for increased apprehensions and processing. CBP's actions were sufficient to close this recommendation on October 13, 2022.
- In OIG 19-67, *Limitations of CBP OFO's Screening Device Used to Identify Fentanyl and Other Narcotics*, we reported that CBP did not have a policy for ensuring the chemical screening devices at U.S. ports of entry had the most up-to-date spectral database library and operating system. We recommended CBP develop and implement a plan for the

¹⁰ On March 20, 2020, under Title 42 authority and in response to the COVID-19 pandemic, the Centers for Disease Control and Prevention issued an order temporarily prohibiting the introduction of certain persons from foreign countries traveling from Canada or Mexico, regardless of their country of origin. On August 2, 2021, a subsequent Centers for Disease Control and Prevention order extended the prohibition of entry under Title 42. Title 42 COVID-19 authority expired on May 11, 2023.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

long-term development of a centralized spectral database for the chemical screening devices. CBP's actions were sufficient to close this recommendation on February 23, 2021.

- In *OIG-18-77, Lack of Planning Hinders Effective Oversight and Management of ICE's Expanding 287(g) Program*,¹¹ we reported that according to ICE field program managers, ICE's 287(g) program reporting structure was confusing and made management and oversight of participating law enforcement agencies more difficult. We recommended ICE develop a reporting structure for the 287(g) program that clearly defined the reporting structure for field program managers. ICE's actions were sufficient to close this recommendation on April 1, 2020.

CBP and ICE implemented corrective actions that enabled us to close 18 of the 20 recommendations. Additionally, one recommendation was resolved and open, and one recommendation was unresolved and open as of August 17, 2023.¹²

Evaluation of Resources

During FYs 2018 through 2022, we issued 14 reports containing 15 recommendations pertaining to this category. Evaluating its resources will ensure that DHS and its components make appropriate and necessary adjustments to achieve the Department's mission at the Southwest border.

Our recommendations were intended to ensure DHS and its components evaluated resources, such as staffing, equipment, and facilities, as environments and priorities changed. For example:

- In *OIG 21-02, CBP Has Taken Steps to Limit Processing of Undocumented Aliens at Ports of Entry*, we reported that two ports of entry had stopped using available detention space, even though undocumented aliens were waiting in queue management lines. We recommended CBP evaluate whether it could more efficiently use available holding spaces to process undocumented aliens, including asylum seekers. CBP's actions were sufficient to close this recommendation on October 26, 2022.
- In *OIG 19-67, Limitations of CBP OFO's Screening Device Used to Identify Fentanyl and Other Narcotics*, we reported that CBP purchased small-scale chemical screenings

¹¹ Section 287(g) of the *Immigration and Naturalization Act* authorizes ICE to enter into agreements with state and local law enforcement entities, permitting designated officers to perform immigration law enforcement functions.

¹² DHS did not concur with Recommendation 1 in *OIG-20-52* and explained that the CBP Wall Acquisition Program appropriately conducted an Alternatives Analysis in accordance with DHS Acquisition Management Directive 102-01 and other related guidance. According to DHS, this program will be dispositioned. DHS will provide documentation to support this action when completed.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

devices that could not identify fentanyl at purity levels of 10 percent or less. We recommended CBP conduct a comprehensive analysis on the ability of any chemical screening device to identify the presence of fentanyl and other narcotics at lower purity levels in field environments, perform reproducibility test runs, and obtain a third-party verification of the results. CBP's actions were sufficient to close this recommendation on September 22, 2020.

- In OIG 19-23, *Border Patrol Needs a Staffing Model to Better Plan for Hiring More Agents*, we reported that neither CBP nor Border Patrol had completed or submitted a workforce staffing model, as required by Congress. We recommended DHS ensure CBP and Border Patrol expedite development and implementation of a workforce staffing model for Border Patrol to better inform staffing and resource deployment decisions. This recommendation was unresolved and open as of August 17, 2023, as CBP has revised the estimated completion date eight times during the last 4 years.¹³

CBP and ICE Implemented corrective actions that enabled us to close 11 of the 15 recommendations. Additionally, three recommendations were resolved and open, and one recommendation was unresolved and open as of August 17, 2023.

Collaboration

During FYs 2018 through 2022, we issued 8 reports containing 12 recommendations pertaining to this category. Collaboration allows DHS components and other government agencies to freely and transparently share information, ideas, and skills that support decisions and activities to achieve the Department's mission at the Southwest border.

Our recommendations were intended to facilitate coordination and collaboration between DHS and its components as well as with external agencies. For example:

- In OIG 22-66, *DHS Technology Systems Do Not Effectively Support Migrant Tracking at the Southwest Border*, we reported that DHS and external agencies often relied on relationship-based communication and past practices. Not all agents and officers at the Southwest border locations were aware of existing memorandums of agreement, which require meetings and coordination between components and agencies. We issued two recommendations for CBP and ICE to evaluate adherence to current immigration policies and memorandums of agreement for internal and external collaboration and working groups and to update them as needed. Both recommendations were resolved and open as of August 17, 2023.

¹³ On May 6, 2022, CBP Border Patrol Submitted to Office of Management and Budget (OMB) the Patrol Border Group sub-model of the CBP Border Patrol Staffing Model. Before it can be submitted to Congress, it has to be cleared by OMB. CBP is waiting for feedback from OMB.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- In OIG 20-06, *DHS Lacked Technology Needed to Successfully Account for Separated Migrant Families*, we reported that before DHS implemented a Zero Tolerance policy, it did not establish a plan for how CBP, ICE, and the Department of Health and Human Services would successfully reunify separated family members. We recommended DHS coordinate with the Department of Health and Human Services to outline roles and responsibilities and create and distribute standard operating procedures for migrant family reunification. This recommendation was resolved and open as of August 17, 2023.
- In OIG 19-57, *A Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations*, DHS OIG and the Department of Justice OIG reported cooperation failures that negatively affected investigations and operations. We issued five recommendations to improve cooperation between the Federal Bureau of Investigation and Homeland Security Investigations along the Southwest border. ICE's actions, in coordination with the Federal Bureau of Investigation, were sufficient to close all five recommendations between June 23, 2020, and January 17, 2023.

CBP and ICE implemented corrective actions that enabled us to close 9 of the 12 recommendations. The remaining three recommendations were resolved and open as of August 17, 2023.

Remaining Five Categories Account for 20 Percent of Recommendations

The remaining 20 percent of recommendations fall into the bottom five categories and have less than 10 recommendations associated with each program management deficiency, as shown in Table 2. Table 3 depicts these bottom five program deficiency categories and the related impact to DHS and its components.



Table 3. Remaining Five Program Management Deficiency Categories

Program Deficiency Category	DHS and Components' Impacted Activity
Program Monitoring	Conduct program reviews to identify areas for improvement.
Training	Provide, improve, and increase frequency of trainings.
Data Collection	Identify and address system errors to improve data collection.
System Interoperability	Improve systems integration for systems to connect to each other and share information.
Maintenance of Records	Maintain complete and accurate documentation.

Source: DHS OIG analysis of recommendations from prior reports

A total of 35 recommendations were assigned to these five categories. As of August 17, 2023, 25 recommendations were closed and 10 were open and resolved.

In summary, our recommendation analysis may be indicative of similar program management deficiencies affecting other Southwest border programs and operations due to the number of times the recommendations were associated with the same program deficiency from our 61 prior reports. Although we do not make a recommendation in this report, DHS should continue to monitor the program deficiencies to ensure Southwest border programs and operations support successful mission execution.

Issues Affecting Current Southwest Border Operations

We met with Southwest border officials and personnel from CBP, ICE, and USCIS to obtain their perspectives on current Southwest border operations. As of February 2023, the components experienced four primary issues — staffing and resources, workloads, system capabilities and integration, and policies and procedures. Table 4 shows a summary of the issues each component faces.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table 4. Current Southwest Border Issues by Component

<i>Component</i>	<i>Staffing and Resources</i>	<i>Workloads</i>	<i>System Capabilities and Integration</i>	<i>Policies and Procedures</i>
<i>CBP</i>	✓	✓	✓	✓
<i>ICE</i>	✓	✓	-	✓
<i>USCIS</i>	✓	✓	✓	-

- No data

Source: DHS OIG analysis based on interviews with CBP, ICE, and USCIS officials

Staffing and Resources

According to CBP, ICE, and USCIS officials, staffing continues to be an issue for current Southwest border operations. To combat this issue, components are using contractors and other partners and agencies, and they are reallocating resources from their primary missions to details along the Southwest border.

Components attributed staffing shortages to unfilled positions. One official stated his component “could not hire fast enough.” The number of Border Patrol encounters¹⁴ along the Southwest border dramatically increased during the 5-year period of our review, growing from almost 400,000 in FY 2018 to almost 1.7 million in FY 2021, and to more than 2.2 million in FY 2022. Based on year-to-date data as of June 7, 2023, encounters are on track to increase for a third consecutive year with significant migrant crossings. During this period of unprecedented growth, the number of Border Patrol agents assigned to the Southwest border remained consistent, as shown in Figure 2.

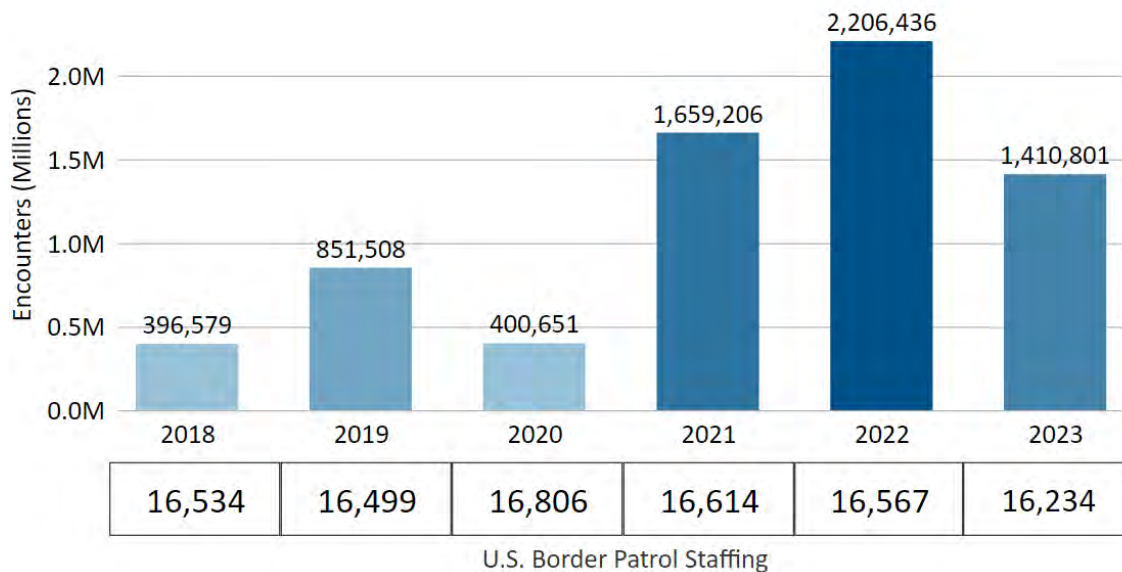
¹⁴ Since March 2020, CBP has separately reported both apprehensions under Title 8 and expulsions under Title 42, referring to them jointly as encounters. DHS further clarified that actions taken under the Centers for Disease Control and Prevention’s Title 42 public health order, which ended on May 11, 2023, are considered encounters and expulsions. Title 8 actions are considered apprehensions under immigration authorities set forth in Title 8 of the United States Code.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Figure 2. U.S. Border Patrol Encounters and Staffing¹⁵



Source: Prepared by DHS OIG using CBP data for Southwest border encounters and staffing

Workloads

CBP, ICE, and USCIS officials identified workloads as an issue. Workloads are closely aligned with staffing and are influenced by migrant volume. According to USCIS officials, their workload challenges are primarily volume driven. They explained that the credible fear asylum screening caseload was unpredictable because they were unable to control the referrals. Further, these officials stated that USCIS does not have resources fully dedicated to conducting credible fear screenings; when USCIS receives a credible fear referral, it must draw resources from other primary missions.

System Capabilities and Integration

CBP and USCIS officials indicated that system capabilities and integration were an issue. According to a CBP official, the component's technology was outdated and could not handle current needs. They also stated that technology in remote locations near the Southwest border did not have normal infrastructure available, such as internet access.

Further, USCIS officials stated that during detainees' credible fear screenings, they experienced logistical challenges, such as lack of phones, software, computer access, and other technology

¹⁵ Border Patrol encounters are recorded by FY, and staffing is based on CBP information for pay period 3 for each calendar year.



connectivity issues. Lack of phones posed a serious issue due to a majority of credible fear screenings being conducted over the phone.

According to USCIS officials, USCIS coordinates with CBP and ICE by using their systems to help obtain information for processing. All three components use different systems. Challenges exist when trying to access all parts of CBP and ICE's systems. A USCIS official stated that the integration of these systems is mostly being done at ICE facilities near the Southwest border, but it would be beneficial if they expanded it to all ICE facilities to help process cases more efficiently.

Policies and Procedures

CBP officials stated that communicating current and revised policies and procedures to the field was an ongoing issue. CBP OFO created the Southwest Border Operation Cell to help communicate policies to OFO personnel in the field. An ICE official mentioned similar challenges, noting that lawful pathways, alternatives to detention, and pandemic response requirements are guidance that was frequently changed.

DHS established the Southwest Border Coordination Center (SBCC) in February 2022 to coordinate planning, operations, engagement, and interagency support for the Southwest border. According to CBP and ICE officials we interviewed, SBCC has no authority to direct change, and it depends on component management to implement changes. An ICE official questioned SBCC's effectiveness, partly due to this perceived lack of authority. The ICE official further stated that adding SBCC to the existing Southwest border structure may have created confusion about partners' roles and responsibilities.

In summary, DHS officials we interviewed cited current issues at the Southwest border that are similar to common deficiencies featured in our analysis of recommendations. We consider all four of the primary issues DHS component officials identified as high-risk due to their potential consequences, such as:

- negative effects on other DHS mission areas resulting from moving resources to the Southwest border;
- additional burdens on staff and increases in workloads resulting from inadequate technology solutions, reliance on obsolete systems, and use of systems that do not adequately support the mission needs; and
- inefficiencies and ineffectiveness due to program deficiencies that impact staffing, workloads, and DHS' ability to meet its primary missions.



Conclusion

Our analysis of DHS OIG reports issued during FYs 2018 through 2022 related to the Southwest border identified 10 program management deficiencies, with the top five categories accounting for 80 percent of the recommendations. This may be indicative of similar program management deficiencies affecting other Southwest border programs and operations due to the number of times the recommendations were associated with the same program deficiency. Additionally, DHS officials we interviewed cited current issues at the Southwest border that are similar to the issues featured in our analysis of recommendations. Although we do not make a recommendation in this report, DHS should learn from these common deficiencies identified from our prior work and from other insights in this summary report to better address conditions at the Southwest border.

Management Comments and OIG Analysis

DHS provided management comments on a draft of this report. We included the comments in their entirety in Appendix B. We also received technical comments from DHS on the draft report, and we revised the report as appropriate. A summary of the DHS response and our analysis follows.

DHS Response: DHS expressed concerns that the report does not fully recognize the extent of initiatives DHS has recently implemented to address common deficiencies in Southwest border program management. For example:

- DHS claimed SBCC created more efficient processes, particularly regarding balancing where resources are located versus where they are needed. Based on SBCC's results, agency leadership recommended integrating SBCC functions and coordinating processes into a more permanent effort.
- DHS stated it has taken measures since May 2021 to address and prevent the prolonged detention of individuals at the Southwest border through:
 - integration of digital processing;
 - use of electronic A-files;
 - coordination with partner agencies and governments; and
 - leveraging virtual processing to improve processing operations and reduce time in custody.
- DHS stated CBP bases staffing level requests on internal models. Like all Government agencies, CBP and ICE request staffing through the Federal budget process, and staffing levels are based on funding for positions through appropriations and/or user fees.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- DHS stated USCIS added four language interpreter services contracts on May 1, 2023, and another contract on July 8, 2023, for a total of five language interpreter services contracts to further support credible fear screenings related to the Southwest border workload.

Finally, DHS noted differences between the draft report and information discussed during the Notice of Findings and Recommendations (NFR) meeting held on July 18, 2023. DHS found the information discussed to be more useful than a traditional capping report of previously published work. It also noted that the number of reports and recommendations increased substantially from the NFR meeting to the draft report and indicated that DHS OIG did not communicate this change before delivering the draft report. DHS encouraged frequent and open communication between program officials and audit and inspection teams, including discussions on revisions in findings and messaging.

OIG Analysis: In our November 2022 entrance conference, we explained that our scope included a review of prior DHS OIG reports relevant to the Southwest border issued from FYs 2018 through 2022. Further, we explained that our objective was to summarize those prior reports and recommendations on DHS' Southwest border operations and programs and identify similar issues and trends. As such, we believe the recommendation analysis identifies useful information that may aid DHS' efforts to ensure efficient and effective operations at the Southwest border. The report provides information regarding issues and trends categorized by 10 common program management deficiencies across DHS' programs. This includes complying with requirements, sufficient guidance, planning, and evaluating results and resource efficiencies. If these elements are not operating as intended, DHS programs will not achieve optimal results.

We acknowledge that the contents of the September 2023 draft report differed from information discussed at the July 2023 NFR meeting. We explained during the NFR meeting that the results presented were preliminary and subject to change before the issuance of the report. Subsequent to the NFR meeting, we decided to include unannounced inspection reports issued by our Office of Inspections and Evaluations. We re-examined the recommendations associated with the unannounced inspections and concluded that they appropriately aligned with the categories used in the recommendation analysis and should therefore be included.

In its response, DHS stated it had implemented numerous recent initiatives to address the findings and recommendations included in the original reports. We cannot verify DHS' assertions because these efforts were not included in the original scope of work summarized. However, we acknowledge in the report all recommendations that have been closed.

We share DHS' desire for frequent and open communication between program officials and audit and inspection teams. We received DHS' technical comments on October 27, 2023 and held an exit conference on November 1, 2023. The discussion in the exit conference focused on the



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

technical comments. Although DHS did note the differences between the information discussed in the NFR meeting and the draft report, it did not share any of the initiatives it highlighted in its management response.



Appendix A:

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107–296) by amendment to the *Inspector General Act of 1978*.

The objective of this review was to summarize our prior work on the Southwest border and identify related common issues. Our scope was DHS OIG reports issued during FYs 2018 through 2022 that were related to the Southwest border.

To answer our objective, we manually reviewed all DHS OIG reports issued during this period to identify those related to the Southwest border. We selected audits, reviews, and inspections based on an initial review of report titles and highlights pages to identify an association with Southwest or southern border. We reviewed the reports' objectives and scopes to determine whether the reports were related to Southwest border operations or programs. We further reviewed the Objective, Scope, and Methodology section of each report to confirm if site visits included locations at the Southwest border. We identified 61 reports, which included 18 audits, 23 inspections and reviews, and 20 unannounced inspections related to the Southwest border, with 178 recommendations to DHS, CBP, and ICE.

We gathered recommendation data for each report we reviewed from the Project Tracking System — the DHS OIG system of record for all projects and reports. We included recommendations resolved and open, unresolved and open, and implemented and closed. We did not include recommendations administratively closed and closed-not implemented because they would not have had any impact on the conditions at the Southwest border. These recommendations were not implemented due to a variety of reasons, such as being overcome by events. For example, the relevant executive order was rescinded, the pertinent contract was terminated, or the applicable program was eliminated.

We organized recommendations into categories by manually reviewing each recommendation to identify the underlying program deficiency that the recommendation aimed to correct. We identified 10 program deficiency categories and ranked the categories based on the number of recommendations assigned to each category.

We conducted interviews to discuss current challenges along the Southwest border with officials and personnel from:

- CBP Border Patrol and OFO — Admissibility and Passenger Program, Operations, Planning, Program Analysis, and Evaluation, and Mission Support;
- ICE Enforcement and Removal Operations and Homeland Security Investigations;



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

- USCIS — Refugee, Asylum, and International Operations Directorate and Office of Policy and Strategy; and
- DHS' Office of Strategy, Policy, and Plans to understand the challenges DHS faces along the Southwest border.

We also interviewed officials and personnel from SBCC to gain an understanding of SBCC and its role and responsibilities along the Southwest border.

We reviewed Government Accountability Office (GAO) and Congressional Research Service reports related to the Southwest border. To assess the reliability of Project Tracking System-generated data, we traced a sample of recommendations in the reports we reviewed back to the relevant report language to determine if information was entered into the system correctly.

We conducted this review between November 2022 and August 2023 under the authority of the *Inspector General Act of 1978*, 5 U.S.C. §§ 401-424, and according to *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

During this review, DHS provided timely responses to our requests for information and did not delay or deny access to information we requested.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix B: DHS Comments on the Draft Report

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



Homeland
Security

December 11, 2023

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

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

Digitally signed by JIM H
CRUMPACKER
Date: 2023.12.11 08:57:13
-05'00'

SUBJECT: Management Response to Draft Report: "Summary of
Previously Issued Recommendations and Other Insights to
Improve Operational Conditions at the Southwest Border"
(Project No. 23-006-AUD-CBP, ICE, USCIS)

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

DHS leadership is pleased to note the OIG's recognition that the Department has closed 80 percent (143 of 178) of Southwest Border (SWB)-related recommendations issued by the OIG in 61 reports from fiscal years (FY) 2018 through 2022, as of August 17, 2023. Leadership, however, is concerned that this draft report includes stale information and does not fully recognize the extent of initiatives DHS has implemented to address what the OIG characterizes as "common deficiencies" in SWB program management. Current and complete information is needed to provide "cold readers" of the report a clearer understanding of the present state of DHS operations at the SWB.

For example, DHS has developed a more unified and robust approach to respond to migrant surges, starting with the formation of the Southwest Border Coordination Center (SBCC) in February 2022. The SBCC, which was staffed and managed by several DHS Components, including U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), and U.S. Immigration and Customs Enforcement (ICE) personnel, was established to coordinate the whole of DHS resources along the SWB. Accordingly, the SBCC created more efficient processes, particularly with regard to balancing where resources are located versus where they are needed and moving those resources to address gaps and reduce pressure on local staffing. In recognition that this coordination must continue long beyond a singular incident, event, or planning effort, the



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

SBCC and agency leadership recommended taking the lessons learned by the SBCC and integrating its functions and coordinating processes into a more permanent effort, the Southwest Border Executive Council. Going forward, DHS will continue to support cross-Component working groups with field and headquarters representatives, consistent with DHS's overall border strategy and future DHS migration resource and response plans, which build on the lessons learned from the SBCC and provides resources and proven approaches, including the cross-Component working group structure described above, to ensure a whole-of-government response to managing the SWB. DHS remains committed to maintaining employee morale and resiliency, as well as the safety and well-being of our workforce and those individuals in our custody.

DHS has also taken numerous steps to address issues previously identified by CBP, ICE, and USCIS personnel as challenges in the SWB environment that the OIG considers to be "high risk" due to their potential consequences. For example, with regard to system capabilities and integration, as well as collaboration, DHS has taken measures since May 2021 to address and prevent the prolonged detention of individuals at the SWB who are in its custody, through:

- (1) integration of digital processing;
- (2) use of electronic A-files;
- (3) coordination with partner agencies and governments, such as through the DHS Movement Coordination Cell; and
- (4) leveraging virtual processing to improve processing operations and reduce time in custody.

Using electronic A-files significantly decreases processing and in-custody times for individual noncitizens and family units by reducing the number of paper A-files and forms. Specifically, using electronic A-numbers and A-files speeds the transfer of information and coordination within DHS and its Components, while increasing case acceptance and processing of asylum, credible fear, and immigration court cases. Use of electronic A-files also allows DHS employees with a need to know to retrieve entire casefiles on demand while eliminating hours of delays waiting for hard copy casefiles to be delivered via traditional mail and courier services. This results in quicker completion and adjudication of a higher volume of cases while providing relief to strained budgets, and therefore provides a time savings to the Department. Accordingly, this enhances efficiencies in numerous processes from apprehension to final adjudication.

Further, the Department has bolstered coordination with partner agencies through the creation and implementation of multi-Component initiatives such as Enhanced Expedited Removal, which allows CBP, ICE Enforcement and Removal Operations and USCIS to perform all agency functions and responsibilities while the noncitizen is still in custody. This streamlines required DHS processes from several weeks to a matter of days and results in a greater number of individuals whose cases are adjudicated in shorter timeframes.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Previously, United States Border Patrol (USBP) sectors utilized Virtual Processing on a limited basis to assist with processing during sporadic surges in irregular migration. Since FY 2021, however, CBP components have employed virtual processing nationwide, as a force multiplier that augments live processing along the SWB. For instance, CBP law enforcement personnel, along with DHS Volunteer Force and contractor personnel, are able to process casework remotely for in-custody family units and single adults. This manner of virtual processing increases case throughput, while decreasing time in custody. Further, Virtual Processing has enabled CBP to simultaneously process additional non-citizens on top of the casework prepared and completed by USBP Agents and CBP Office of Field Operations (OFO) Officers at stations and ports of entry (POE) along the SWB.

With regard to staffing, resources, and workload, CBP uses internal models on which staffing level requests are based. Specifically, USBP's staffing model is comprised of four separate sub-models, while CBP OFO currently uses a model as a first step in determining workload level at each of its POEs, to include sudden or unplanned needs, as appropriate. Like all government agencies, CBP and ICE request staffing through the federal budget process, and staffing levels are based on funding for positions through appropriations and/or user fees.

Specifically, USBP's staffing model is comprised of four workforce sub-models that delineate personnel requirements for USBP. In developing the four sub-models, USBP incorporated statistically sound methodologies to ensure that the results were demonstrable and repeatable. As USBP regions can vary greatly due to the operational environment, types of threats, and levels of available resources, the USBP model accounts for the operational realities and uniqueness of the different USBP regions. USBP also continuously reviews the model to ensure that all significant variables that affect staffing requirements are considered, to include ever-changing threat levels and investments in other mission capabilities that augment personnel requirements. Currently, the USBP's staffing model considers 37 key essential mission functions that are performed by USBP personnel.

Similarly, CBP OFO's workload staffing model (WSM) serves as a decision support tool for OFO leadership and is the initial data-driven step in the process of quantifying workload at the POEs. OFO executive leadership uses the model results, along with other factors such as emerging threats and newly opening facilities, to determine the allocation of staffing across our ports of entry. This model is completely reviewed and updated each year with data from the previous FY. The activities covered in the model (currently approximately 100) are reviewed and evaluated each year to:

- (1) remove any activities that are no longer performed;
- (2) update processes to reflect current operating conditions; and
- (3) add new activities in response to changing conditions and emerging threats.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Further, the WSM is independently assessed, and the model routinely audited and reviewed by outside stakeholders such as DHS and the Office of Management and Budget. Accordingly, it is updated each year to reflect the changing activities and emerging threats in all environments, to include air, sea, and land. Throughout the year, CBP OFO uses the WSM to inform other modeling efforts that estimate the impact to throughput and enforcement of various scenarios to determine the best way to respond to sudden and unplanned needs. Currently, the WSM models approximately 100 activities that cover the entirety of a CBP OFO Officer's duties from pre-primary, primary, and secondary, to seizure processing.

In addition, USCIS added four language interpreter services contracts on May 1, 2023, and one interpreter services contract on July 8, 2023, for a total of five language interpreter services contracts to further support credible fear screenings related to the SWB workload. USCIS also continues to divert staff from other primary missions and to diligently hire and onboard staff to support credible fear screenings and other related humanitarian workloads. As part of this effort, USCIS prioritizes the expeditious screening of noncitizens for protection claims at the SWB, as these individuals are subject to immigration detention.

Lastly, DHS notes that the OIG's draft report departs in several respects from the Notice of Findings and Recommendations (NFR), dated July 14, 2023, and discussed with Component and Headquarters officials on July 18, 2023. Specifically, the NFR:

- Anchored OIG's analysis and identification of "common deficiencies" in SWB program management to U.S. Government Accountability Office (GAO) "Standards for Internal Control in the Federal Government" (i.e., the "Green Book") (GAO-14-704G, dated September 10, 2014),¹ which DHS program officials, subject matter experts, and others thought was an appropriate source of authoritative criteria for the analysis. This included:
 - (1) An Appendix B summarizing and associating the applicable 17 GAO internal control principles (Principles) with each program deficiency category OIG identified, and
 - (2) Extensive narrative throughout the NFR discussing the Principles and how they related to each of the deficiencies OIG identified.

However, the draft report does not mention of the Green Book work accomplished in the report's "Objective, Scope, and Methodology" appendix, nor any explanation of the apparent professional judgment used to conduct OIG's revised analysis. DHS believes the Principles-based analysis would have been more

¹<https://www.gao.gov/greenbook>



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

valuable compared to a traditional capping report of previously published work received.

- Discussed 45 reports with 130 recommendations related to the SWB and issued from FY 2018 through FY 2022; however, the draft report provided for DHS' formal management response included 61 reports and 178 recommendations; an increase of 36 and 37 percent in reports and recommendations reviewed, respectively. DHS realizes that the NFR represented the preliminary results of OIG's work and was subject to further review and revision, but nevertheless notes that this significant scope change appeared in the draft report without any communication from the OIG. DHS officials might have chosen to allocate resources to review and engage with the NFR differently had they known the NFR was not fully representative of draft report on which they would later be asked to comment.

DHS encourages frequent and open communication between program officials and audit and inspection teams, including about shifts in findings and messaging, in accordance with the spirit and intent of Council of the Inspectors General on Integrity and Efficiency "Blue Book" guidance.² We hope that moving forward our two organizations can work more closely together in this regard.

The draft report did not contain any recommendations. DHS previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions.

² <https://www.ignet.gov/sites/default/files/files/QualityStandardsforInspectionandEvaluation-2020.pdf>



Appendix C:

List of Reports Included in This Review

We compiled and analyzed the recommendations from the following DHS OIG reports, which identified challenges at the Southwest border during the past 5 FYs.

Audits

1. *DHS Needs a More Unified Approach to Immigration Enforcement and Administration*, OIG-18-07, October 2017 https://www.oig.dhs.gov/sites/default/files/assets/2017-11/OIG-18-07-Nov17_test.pdf.
2. *Immigration and Customs Enforcement Did Not Follow Federal Procurement Guidelines When Contracting for Detention Services*, OIG-18-53, February 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-02/OIG-18-53-Feb18.pdf>.
3. *CBP Has Not Ensured Safeguards for Data Collected Using Unmanned Aircraft Systems*, OIG-18-79, September 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-79-Sep18.pdf>.
4. *DHS Training Needs for Hiring 15,000 Border Patrol Agents and Immigration Officers*, OIG-19-07, November 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-11/OIG-19-07-Nov18.pdf>.
5. *Border Patrol Needs a Staffing Model to Better Plan for Hiring More Agents*, OIG-19-23, February 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-23-Feb19.pdf>.
6. *Management Alert – CBP Did Not Adequately Protect Employees from Possible Fentanyl Exposure*, OIG-19-53, July 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-07/OIG-19-53-Jul19.pdf>.
7. *Limitations of CBP OFO's Screening Device Used to Identify Fentanyl and Other Narcotics*, OIG-19-67, September 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-10/OIG-19-67-Sep19.pdf>.
8. *DHS Lacked Technology Needed to Successfully Account for Separated Migrant Families*, OIG-20-06, November 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-11/OIG-20-06-Nov19.pdf>.
9. *CBP Has Not Demonstrated Acquisition Capabilities Needed to Secure the Southern Border*, OIG-20-52, July 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-07/OIG-20-52-Jul20.pdf>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

10. *DHS Cannot Determine the Total Cost, Effectiveness, and Value of Its Joint Task Forces*, OIG-20-80, September 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-10/OIG-20-80-Sep20.pdf>.
11. *CBP Needs Additional Oversight to Manage Storage of Illicit Drugs*, OIG-21-18, March 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-04/OIG-21-18-Mar21-Redacted.pdf>.
12. *CBP Has Improved Southwest Border Technology, but Significant Challenges Remain*, OIG-21-21, February 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-02/OIG-21-21-Feb21.pdf>.
13. *CBP Generally Provided Accurate Notices to Appear to Migrant Protection Protocols Enrollees, but Could Improve Procedures to Reduce Future Errors*, OIG-21-45, July 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-07/OIG-21-45-Jul21.pdf>.
14. *CBP Needs to Strengthen Its Oversight and Policy to Better Care for Migrants Needing Medical Attention*, OIG-21-48, July 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-07/OIG-21-48-Jul21.pdf>.
15. *CBP's FAST Program Exposes Borders to Security Risks*, OIG-21-70, September 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-10/OIG-21-70-Sep21-Redacted.pdf>.
16. *CBP Officials Implemented Rapid DNA Testing to Verify Claimed Parent-Child Relationships*, OIG-22-27, February 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-02/OIG-22-27-Feb22.pdf>.
17. *DHS Technology Systems Do Not Effectively Support Migrant Tracking at the Southwest Border*, OIG-22-66, September 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-66-Sep22.pdf>.
18. *U.S. Border Patrol Screened Migrants at the Southwest Border but Could Strengthen Processes*, OIG-22-71, September 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-71-Sep22.pdf>.

Inspections and Reviews

1. *ICE's Inspections and Monitoring of Detention Facilities Do Not Lead to Sustained Compliance or Systemic Improvements*, OIG-18-67, June 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-06/OIG-18-67-Jun18.pdf>.
2. *Assaults on CBP and ICE Law Enforcement Officers*, OIG-18-76, September 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-76-Sep18.pdf>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

3. *Lack of Planning Hinders Effective Oversight and Management of ICE's Expanding 287(g) Program*, OIG-18-77, September 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-09/OIG-18-77-Sep18.pdf>.
4. *Special Review – Initial Observations Regarding Family Separation Issues Under the Zero Tolerance Policy*, OIG-18-84, September 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-10/OIG-18-84-Sep18.pdf>.
5. *CBP Should Improve Its Air Coordination in the Rio Grande Valley Sector*, OIG-19-02, October 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-10/OIG-19-02-Oct18.pdf>.
6. *ICE Does Not Fully Use Contracting Tools to Hold Detention Facility Contractors Accountable for Failing to Meet Performance Standards*, OIG-19-18, January 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-02/OIG-19-18-Jan19.pdf>.
7. *A Joint Review of Law Enforcement Cooperation on the Southwest Border between the Federal Bureau of Investigation and Homeland Security Investigations*, OIG-19-57, July 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-08/OIG-19-57-Jul19.pdf>.
8. *CBP Separated More Asylum-Seeking Families at Ports of Entry Than Reported and For Reasons Other Than Those Outlined in Public Statements*, OIG-20-35, May 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-06/OIG-20-35-May20.pdf>.
9. *Early Experiences with COVID-19 at ICE Detention Facilities*, OIG-20-42, June 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-06/OIG-20-42-Jun20.pdf>.
10. *U.S. Customs and Border Protection Compliance with Use of Force Policy for Incidents on November 25, 2018 and January 1, 2019*, OIG-20-64, August 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-64-Aug20.pdf>.
11. *Children Waited for Extended Periods in Vehicles to Be Reunified with Their Parents at ICE's Port Isabel Detention Center in July 2018*, OIG-20-65, August 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-65-Aug20.pdf>.
12. *Management Alert – CBP Needs to Award A Medical Services Contract Quickly to Ensure No Gap in Services*, OIG-20-70, September 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-70-Sep20.pdf>.
13. *CBP Did Not Adequately Oversee FY 2019 Appropriated Humanitarian Funding*, OIG-20-78, September 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-78-Sep20.pdf>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

14. *CBP Has Taken Steps to Limit Processing of Undocumented Aliens at Ports of Entry*, OIG-21-02, October 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-10/OIG-21-02-Oct20.pdf>.
15. *DHS Has Not Effectively Implemented the Prompt Asylum Pilot Programs*, OIG-21-16, January 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-01/OIG-21-16-Jan21.pdf>.
16. *DHS' Fragmented Approach to Immigration Enforcement and Poor Planning Resulted in Extended Migrant Detention during the 2019 Surge*, OIG-21-29, March 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-03/OIG-21-29-Mar21.pdf>.
17. *ICE Did Not Consistently Provide Separated Migrant Parents the Opportunity to Bring Their Children upon Removal*, OIG-21-36, May 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-05/OIG-21-36-May21.pdf>.
18. *Review of the February 16, 2020 Childbirth at the Chula Vista Border Patrol Station*, OIG-21-49, July 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-07/OIG-21-49-Jul21.pdf>.
19. *ICE's Management of COVID-19 in Its Detention Facilities Provides Lessons Learned for Future Pandemic Responses*, OIG-21-58, September 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-58-Sep21.pdf>.
20. *DHS Needs to Enhance Its COVID-19 Response at the Southwest Border*, OIG-21-60, September 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-60-Sep21.pdf>.
21. *Many Factors Hinder ICE's Ability to Maintain Adequate Medical Staffing at Detention Facilities*, OIG-22-03, October 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-11/OIG-22-03-Oct21.pdf>.
22. *ICE Spent Funds on Unused Beds, Missed COVID-19 Protocols and Detention Standards while Housing Migrant Families in Hotels*, OIG-22-37, April 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-04/OIG-22-37-Apr22.pdf>.
23. *U.S. Border Patrol Faces Challenges Administering Post-Apprehension Outcomes Consistently Across Sectors*, OIG-22-68, September 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-68-Sep22.pdf>.

Unannounced Inspections

1. *Concerns about ICE Detainee Treatment and Care at Detention Facilities*, OIG-18-32, December 2017 <https://www.oig.dhs.gov/sites/default/files/assets/2017-12/OIG-18-32-Dec17.pdf>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

2. *Management Alert – Issues Requiring Action at the Adelanto ICE Processing Center in Adelanto, California*, OIG-18-86, September 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-10/OIG-18-86-Sep18.pdf>.
3. *Results of Unannounced Inspections of Conditions for Unaccompanied Alien Children in CBP Custody*, OIG-18-87, September 2018 <https://www.oig.dhs.gov/sites/default/files/assets/2018-10/OIG-18-87-Sep18.pdf>.
4. *Management Alert – DHS Needs to Address Dangerous Overcrowding Among Single Adults at El Paso Del Norte Processing Center (Redacted)*, OIG-19-46, May 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-05/OIG-19-46-May19.pdf>.
5. *Concerns about ICE Detainee Treatment and Care at Four Detention Facilities*, OIG-19-47, June 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-06/OIG-19-47-Jun19.pdf>.
6. *Management Alert – DHS Needs to Address Dangerous Overcrowding and Prolonged Detention of Children and Adults in the Rio Grande Valley (Redacted)*, OIG-19-51, July 2019 <https://www.oig.dhs.gov/sites/default/files/assets/2019-07/OIG-19-51-Jul19.pdf>.
7. *Capping Report: CBP Struggled to Provide Adequate Detention Conditions During 2019 Migrant Surge*, OIG-20-38, June 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-06/OIG-20-38-Jun20.pdf>.
8. *Capping Report: Observations of Unannounced Inspections of ICE Facilities in 2019*, OIG-20-45, July 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-07/OIG-20-45-Jul20.pdf>.
9. *Five Laredo and San Antonio Area CBP Facilities Generally Complied with the National Standards on Transport, Escort, Detention, and Search*, OIG-20-67, September 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-67-Sep20.pdf>.
10. *ICE Needs to Address Prolonged Administrative Segregation and Other Violations at the Imperial Regional Detention Facility*, OIG-21-12, December 2020 <https://www.oig.dhs.gov/sites/default/files/assets/2020-12/OIG-21-12-Dec20.pdf>.
11. *Violations of Detention Standards amid COVID-19 Outbreak at LA Palma Correctional Center in Eloy, AZ*, OIG-21-30, March 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-04/OIG-21-30-Mar21.pdf>.
12. *Violations of ICE Detention Standards at Otay Mesa Detention Center*, OIG-21-61, September 2021 <https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-61-Sep21.pdf>



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

13. *Rio Grande Valley Area Border Patrol Struggles with High Volumes of Detainees and Cases of Prolonged Detention but Has Taken Consistent Measures to Improve Conditions in Facilities*, OIG-22-22, January 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-02/OIG-22-22-Feb22.pdf>.
14. *CBP Border Patrol Stations and Ports of Entry in Southern California Generally Met TEDS Standards*, OIG-22-26, February 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-02/OIG-22-26-Feb22.pdf>.
15. *Management Alert – Immediate Removal of All Detainees from the Torrance County Detention Facility*, OIG-22-31, March 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-05/OIG-22-31-Mar22-mgmtalert.pdf>.
16. *Yuma Sector Border Patrol Struggled to Meet TEDS Standards for Single Adult Men but Generally Met TEDS Standards for Other Populations*, OIG-22-38, April 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-04/OIG-22-38-Apr22.pdf>.
17. *Violations of ICE Detention Standards at South Texas ICE Processing Center*, OIG-22-40, April 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-04/OIG-22-40-Apr22.pdf>.
18. *El Paso Sector Border Patrol Struggled with Prolonged Detention and Consistent Compliance with TEDS Standards*, OIG-22-57, August 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-57-Aug22.pdf>.
19. *Violations of ICE Detention Standards at Torrance County Detention Facility*, OIG-22-75, September 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-09/OIG-22-75-Sep22.pdf>.
20. *Del Rio Area Struggled with Prolonged Detention, Consistent Compliance with CBP's TEDS Standards, and Data Integrity*, OIG-22-80, September 2022 <https://www.oig.dhs.gov/sites/default/files/assets/2022-10/OIG-22-80-Oct22.pdf>.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix D: Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief, CBP – U.S. Border Patrol
Executive Assistant Commissioner, CBP – Office of Field Operations
Acting Executive Associate Director, ICE – Homeland Security Investigations
Acting Executive Associate Director, ICE – Enforcement and Removal Operations
Associate Director, USCIS – Refugee, Asylum, and International Operations Directorate
CBP Audit Liaison
ICE Audit Liaison
USCIS Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov



DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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