

**CBP's Global Entry
Program Is Vulnerable to
Exploitation (REDACTED)**





~~SENSITIVE SECURITY INFORMATION~~

DHS OIG HIGHLIGHTS

CBP's Global Entry Program Is Vulnerable to Exploitation

June 24, 2019

Why We Did This Audit

U.S. Customs and Border Protection (CBP) created the Global Entry Program (Global Entry) to allow expedited entry for pre-approved, low-risk travelers arriving in the United States. We conducted this audit to determine to what extent CBP controls over Global Entry prevent high-risk travelers from obtaining expedited screening.

What We Recommend

We made six recommendations to CBP that when implemented should mitigate a number of vulnerabilities in its Global Entry Program.

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

CBP's controls over the Global Entry Program do not always prevent ineligible and potentially high-risk Global Entry members from obtaining expedited entry into the United States. Specifically, during vetting, CBP approved 4 of [REDACTED] applicants in our statistically valid random sample for FYs 2016–2017 who did not meet the eligibility requirements and should not have been considered low risk. This occurred because CBP officers did not always comply with policies when reviewing Global Entry applications nor do CBP's policies sufficiently help officers determine an applicant's level of risk. Based on the sample of approved members, we infer there could be [REDACTED] ineligible, potentially high-risk members in CBP's Global Entry Program.

Additionally, during the airport arrival process, CBP officers granted some Global Entry members expedited entry without verifying the authenticity of their kiosk receipts. CBP officers also did not properly respond to a breach of the Daily Security Code. These weaknesses were due to officers not following policy, as well as CBP's insufficient verification procedures. Unless CBP officers authenticate kiosk receipts, someone could use a fake receipt to enter the United States.

Finally, CBP does not effectively monitor Global Entry to ensure members continue to meet program requirements. In particular, CBP did not conduct the required number of internal audits and did not use its Self-Inspection Program effectively. CBP's lack of adherence to its compliance program's policies and procedures creates vulnerabilities in Global Entry by allowing potentially ineligible members to continue to participate.

CBP's Response

CBP concurred with all six of our recommendations and initiated corrective actions to address the findings.

~~SENSITIVE SECURITY INFORMATION~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

June 24, 2019

MEMORANDUM FOR: Todd Owen
Executive Assistant Commissioner
Office of Field Operations
U.S. Customs and Border Protection

FROM: Sondra F. McCauley 
Assistant Inspector General for Audits

SUBJECT: *CBP's Global Entry Program Is Vulnerable to
Exploitation – ~~Sensitive Security Information~~*

Attached for your action is our final report, *CBP's Global Entry Program Is Vulnerable to Exploitation – ~~Sensitive Security Information~~*. We incorporated the formal comments provided by your office.

The report contains six recommendations aimed at improving the Global Entry Program. Your office concurred with all six recommendations. Based on information provided in your response to the draft report, we consider recommendations 1-6 to be 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. 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 be considered open and resolved.

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

Consistent with our responsibility under the *Inspector General Act of 1978*, 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.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Please call me with any questions (202) 981-6000, or your staff may contact Maureen Duddy, Deputy Assistant Inspector General for Audits, at (617) 565-8723.

Attachment



~~**SENSITIVE SECURITY INFORMATION**~~
OFFICE OF INSPECTOR GENERAL
 Department of Homeland Security

Table of Contents

Background 1

Results of Audit 5

Weaknesses Identified in Global Entry’s Vetting Process 6

Weaknesses Identified in Global Entry’s Airport Arrival Process 8

Weaknesses Identified in Global Entry’s Compliance Programs 11

Recommendations..... 15

Management Comments and OIG Analysis.....16

Appendixes

Appendix A: Objective, Scope, and Methodology 19

Appendix B: CBP Comments to the Draft Report..... 22

Appendix C: Vetting Systems/Databases 27

Appendix D: Ineligible Global Entry Members 29

Appendix E: Report Distribution..... 32

Abbreviations

CBP	U.S. Customs and Border Protection
CFR	Code of Federal Regulations
GAO	Government Accountability Office
OIG	Office of Inspector General



Background

U.S. Customs and Border Protection’s (CBP) mission is to safeguard U.S. borders by preventing illegal movement of people and contraband through U.S. ports of entry. Each day at ports of entry, CBP processes more than one million travelers, including more than 340,000 international air passengers and crew. In 2008, CBP created the Global Entry Program (Global Entry)¹ to expedite entry for pre-approved, low-risk travelers arriving in the United States. As of June 5, 2018, there were more than 5.4 million members approved to enter the United States using automated kiosks at 53 selected U.S. airports and 15 preclearance locations.² As shown in figure 1, CBP offers Global Entry membership to U.S. citizens, U.S. lawful permanent residents, and citizens of 16 partner countries.

Figure 1: Global Entry Membership by Country



Source: Office of Inspector General (OIG) analysis of CBP data

Over the last two fiscal years, CBP obligated approximately \$89 million³ to Global Entry. CBP funds Global Entry entirely through revenue collected by its application fees. CBP carries the application fees over from year to year; they

¹ 8 Code of Federal Regulations (CFR) 235.12, *Global Entry Program*

² Preclearance is the strategic stationing of CBP officers overseas to inspect travelers prior to boarding United States-bound flights. Travelers are subject to the same immigration, customs, and agriculture inspections of international air travelers typically performed upon arrival in the United States.

³ We calculated the average using Global Entry Program obligations for FYs 2016–2017.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

are not tied to fiscal year appropriations. On average, CBP collects \$126 million⁴ in application fees.

CBP's Office of Field Operations, Trusted Traveler Program Office is responsible for overseeing all of CBP's Trusted Traveler Programs, including Global Entry. The Trusted Traveler Program Office developed the *Consolidated Trusted Traveler Programs Handbook (April 2016)* (hereafter referred to as "Handbook"), which outlines the traveler enrollment process. Additionally, the Handbook details the procedures for inspecting Global Entry members at ports of entry. The Trusted Traveler Program Office relies heavily on its vetting center, enrollment centers, and airport personnel to accomplish Global Entry objectives.

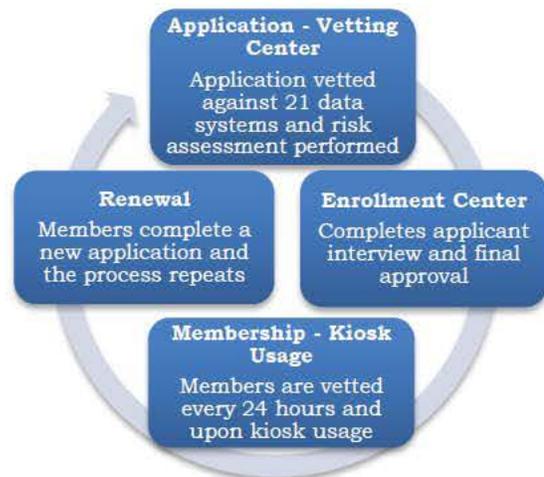
Global Entry Vetting Process

Global Entry vetting occurs at various times throughout the program, from application through membership and renewal. For vetting, CBP checks individuals' biographic information against law enforcement information to ensure that Global Entry applicants and members meet or continue to meet trusted traveler eligibility determinations. Figure 2 depicts the vetting process.

Application and Vetting Center

To become a Global Entry member, applicants complete and submit an application to CBP via the Trusted Traveler Program System on CBP's website. CBP then routes the application to the vetting center where officers query applicant biographic data against 21 different systems. (See appendix C for a description of the vetting data systems.) The database query discloses any derogatory information based on non-compliance with Federal laws and regulations, as well as any criminal history and terrorism matches. A vetting center officer reviews each potential match to determine whether additional information is required. The officer uses

Figure 2: Global Entry Vetting



Source: OIG analysis of Global Entry vetting process

⁴ We calculated the average using Global Entry Program fee collection for FYs 2016–2017.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

a Risk Assessment Worksheet to record vetting actions and query results for each applicant.

Enrollment Center

Once a vetting center officer completes the application review, it is marked as “conditionally approved” and the applicant then schedules an interview at an enrollment center. The enrollment center officer reviews the information provided by the applicant and resolves any vetting center comments on the Risk Assessment Worksheet. The enrollment center officer must also confirm the identity of the applicant, validate travel documents, query fingerprints, and address any additional eligibility questions.

Membership

Upon application approval and membership in Global Entry, CBP continuously vets approved members every 24 hours. The vetting center re-processes the Global Entry population to identify new or active TECS⁵ records with name and date of birth exact matches, National Crime Information Center⁶ wants and warrants, and any Terrorism Watchlist hits. Vetting center officers adjudicate any potential matches resulting from the re-vetting process.

Renewal

Global Entry membership has a 5-year duration. CBP provides Global Entry members the opportunity to renew their membership 1 year prior to its expiration date. If a member chooses not to renew, CBP removes the individual from the program. Members seeking renewal may submit renewal requests prior to the expiration date and may bypass some of the initial vetting steps.

Global Entry Arrival Process

When a Global Entry member arrives at a participating airport, the member bypasses a CBP officer’s primary inspection and proceeds directly to a Global Entry kiosk to scan his or her travel documents. The kiosk system prompts the member to scan fingerprints, initiates checks against various law enforcement

⁵ TECS (not an acronym) serves as a data repository to support law enforcement “lookouts,” border screening, and reporting for CBP’s primary and secondary inspection processes.

⁶ The National Crime Information Center is the Federal Bureau of Investigation’s electronic clearinghouse of criminal justice agency records nationwide, which provides CBP updates on current criminal history, warrants, protection orders, or potential ties to terrorist activities.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

databases, takes the member’s photo, and prompts the member to complete CBP declaration questions.

The kiosk system may deny a member expedited entry if queries reveal a potentially disqualifying record, declaration, Global Entry system failure, or random selection. Similarly, a member may not be eligible for expedited processing if the member declares commercial merchandise, more than \$10,000 or a foreign equivalent in currency, or certain restricted or prohibited goods. As detailed in 8 CFR 235.12(g), a member denied entry will be referred to the “nearest open passport control primary inspection station.” At primary inspection, the officer attempts to resolve any identified referrals. The member either is cleared or is directed to secondary inspection for further resolution. If secondary results are negative, participants will be permitted entry to the United States. If a violation exists, officers must refer to a supervisor for a decision on whether the Global Entry membership should be revoked.

If the kiosk system approves the member, the printed receipt will direct the member to a Federal Inspection Service Area exit point. Members then provide the time-stamped kiosk receipt to the CBP officer working at the exit point. The officer uses the kiosk receipt to verify membership in Global Entry. CBP officers must verify security features on the receipt prior to granting the member entry. After the CBP officer determines the receipt’s authenticity, the officer either allows expedited entry or refers the member for additional inspection. Figure 3 depicts the arrival process.

Global Entry Internal Audit and Compliance Process

CBP monitors effectiveness, adherence to standard operating procedures, and compliance with Global Entry policies through its vetting center internal audits and its Self-Inspection Program. Vetting center personnel are required to audit at least 20 Global Entry applications per month to ensure adherence to policy. Further, personnel at enrollment centers and ports of entry measure compliance with policies and procedures through the Self-Inspection Program. The responsible program

Figure 3: Global Entry Arrival



Source: OIG analysis of CBP processes



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

office officials receive compliance program results and take necessary corrective actions.

Results of Audit

CBP's controls over Global Entry do not always prevent ineligible and potentially high-risk Global Entry members from obtaining expedited entry into the United States. Specifically, during vetting, CBP approved 4 of [REDACTED] applicants in our statistically valid random sample for FYs 2016–2017 who did not meet the eligibility requirements and should not have been considered low risk. This occurred because CBP officers did not always comply with policies when reviewing Global Entry applications nor do CBP's policies sufficiently help officers determine an applicant's level of risk. Based on the sample of approved members, we infer there could be [REDACTED] ineligible, potentially high-risk members in Global Entry.

Additionally, during the airport arrival process CBP officers granted some Global Entry members expedited entry without verifying the authenticity of their kiosk receipts. CBP officers also did not properly respond to a breach of the Daily Security Code. These weaknesses were due to officers not following policy, as well as CBP's insufficient verification procedures. Unless CBP officers authenticate kiosk receipts, someone could use a fake receipt to enter the United States.

Finally, CBP does not effectively monitor Global Entry to ensure members continue to meet program requirements. In particular, CBP Office of Field Operations did not conduct the required number of internal audits and did not use its Self-Inspection Program Worksheet effectively. CBP's lack of adherence to its compliance program's policies and procedures creates vulnerabilities in Global Entry by allowing potentially ineligible members to continue to participate.

⁷ We identified these errors during our review of a random statistical sample of [REDACTED] of 663,936 approved Global Entry members for FYs 2016–2017, identified by CBP as having a “potential match” on its Risk Assessment Worksheet. The range of anomalies for ineligible Global Entry members is [REDACTED], based on a 90 percent confidence interval, 5 percent tolerance for error, and a 50 percent population proportion. Appendix A explains our methodology.



Weaknesses Identified in Global Entry’s Vetting Process

Our review of a statistically valid random sample of [REDACTED] applicants showed that from FYs 2016–2017, CBP approved 4 potentially high-risk, ineligible applicants for Global Entry membership. According to Federal regulations and the Handbook, an individual is ineligible to participate in the program if the person presents a potential risk for terrorism, criminality, or is otherwise not a low-risk traveler. These four applicants were approved because CBP officers did not always adhere to Global Entry policies when reviewing Global Entry applications. In addition, CBP had insufficient policies to guide the officer’s determination of low risk when exercising his or her discretion. Based on our sample of approved Global Entry members, we can infer with 90% confidence there could be [REDACTED] ineligible and potentially high-risk members participating in Global Entry.

CBP may have [REDACTED] ineligible and potentially high-risk members participating in Global Entry.

CBP Approved Ineligible Applicants

CBP approved four Global Entry applicants who did not meet low-risk program eligibility requirements. According to the Handbook, the vetting center must create and review an applicant’s Risk Assessment Worksheet to determine an applicant’s risk. If the vetting center discovers issues (e.g., possible name matches to records and possible address matches) the vetting center will “conditionally approve” the application and send it to the enrollment center. Officers at the enrollment center will address these issues during the applicant’s interview and document conclusions in the Global Enrollment System. According to page 11 of the Handbook, “if low-risk status cannot be determined, the application must be denied.” Table 1 briefly explains the four members’ risk determination factors that made them ineligible. See appendix D for more details about each ineligible member we identified.

Table 1: Global Entry Ineligible Members

	Global Entry Member Risk Determination Factors
Member 1	Used a lost/stolen passport on application
Member 2	[REDACTED] linked to an investigation
Member 3*	Multiple arrests and criminal misdemeanors
Member 4	Narcotics violation

Source: DHS OIG analysis of CBP data

*Successfully used Global Entry benefits on February 20, 2018.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Insufficient Policies to Support CBP Officer's Enrollment Decisions

CBP officers did not always adhere to required vetting procedures when reviewing applications. For example, Member 4's query returned a criminal narcotics violation. According to the Handbook, officers should not approve applications before receipt of court documents, when court documents are required. The officer at the enrollment center did not obtain required court documentation showing the severity and disposition of the charges and approved the member in error. Additionally, CBP approved Members 2 and 3 in error because officers did not follow vetting policies and procedures.

The Handbook is not sufficient to guide an officer's determination when to exercise his or her discretion as to what constitutes low risk. Specifically, the Handbook lacks definitions, explanations, and examples to help vetting center officers classify and understand potential query matches on an applicant's Risk Assessment Worksheet during the vetting process. For example, Member 1's query returned a potential match related to a lost/stolen passport. The officer at the vetting center classified the query as "positive-irrelevant." CBP's Trusted Traveler Program Office provided definitions for the match classifications shown in table 2. However, these definitions are not included in official policy. By definition, a positive-irrelevant classification means that an officer identified a positive match, but the information examined is not relevant and would not disqualify the applicant from obtaining Global Entry benefits. Based on this informal guidance, the vetting center officer should have marked the query as "positive-relevant" and provided comments for the enrollment center to address. At that point, the enrollment center would have had to verify the identity of the applicant and inquire why the applicant possessed a lost or stolen passport. Because the vetting center officer did not have sufficient policies, the officer incorrectly classified the member's query match. As a result, the officers at the enrollment center did not conduct any further review and approved Member 1 for participation in Global Entry in error.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
 Department of Homeland Security

Table 2: Global Entry Match Classification Definitions

Vetting Center Classification	Definition Provided by Trusted Traveler Program Office Officials	Enrollment Center Action
Positive-Relevant	Appears to be a positive identity match and the derogatory information is relevant to Global Entry Standard Operating Procedures, potentially disqualifying.	Officers verify derogatory information and make final determination.
Positive-Irrelevant	Appears to be a positive identity match; the information examined is not relevant to being disqualifying.	Officers do not conduct further review.
False-Match	Based on information provided, appears to be a mismatch in identity.	Officers do not conduct further review.
Inconclusive	Based on information alone, unable to determine an identity match.	Officers conduct further review and make a final determination.

Source: OIG analysis of CBP Office of Field Operations, Trusted Traveler Program Office definitions

CBP’s Trusted Traveler Program officials confirmed the correct classification was “positive-relevant” and revoked Member 1’s Global Entry membership. They also agreed that Members 3 and 4 were ineligible and revoked their memberships. Conversely, the same program officials believed that Member 2 should remain eligible for Global Entry because they could not determine a high-risk association. However, CBP made its eligibility determination without resolving potentially disqualifying query results. Specifically, Member 2 was

[REDACTED]

Weaknesses Identified in Global Entry’s Airport Arrival Process

Control weaknesses exist in CBP’s airport arrival process. Specifically, CBP officers granted Global Entry members expedited entry at nine airports without verifying the authenticity of their Global Entry kiosk receipts (sample shown in figure 4). CBP officers also failed to follow protocols related to a breach of the Daily Security Code, which is a [REDACTED] and [REDACTED] on Global Entry kiosk receipts. These weaknesses occurred in part because officers do not always adhere to established policy, but also because of insufficient and ineffective policies. Based on our testing at nine



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

airports, 5,751⁸ Global Entry members may not have had their Global Entry receipts authenticated by CBP officers. Unless CBP officers authenticate kiosk receipts, someone could use a fraudulent receipt to enter the United States.

CBP Officers Did Not Verify the Authenticity of Global Entry Receipts

At the nine airports tested, CBP officers at the Federal Inspection Service area granted expedited entry to 231⁹ Global Entry members without verifying the authenticity of their Global Entry receipts. The kiosk receipt contains two inherent security features — the Security Check Digit, which is the [REDACTED] and the Daily Security Code. During the arrival process, CBP officers are required to verify both security features before allowing Global Entry members to exit. CBP created these controls to prevent potential use of fraudulent receipts and ensure the kiosk receipt is authentic.

At all nine airports we tested, none of the CBP officers at the Federal Inspection Service area verified the Security Check Digit printed on the receipt. To verify this feature, a CBP officer must [REDACTED]. For example, as shown in figure 4, if the [REDACTED] on the Global Entry kiosk receipt is [REDACTED], then the Security Check Digit should be [REDACTED]. If the [REDACTED] the Security Check Digit, an officer escorts the member to passport control secondary inspection for further examination. However, officers at the exit lanes we interviewed were either unaware of the requirement or did not include the Security Check Digit when explaining the receipt verification process. After we explained the Security Check Digit process, all of the officers we spoke with described the process as cumbersome and expressed concerns that it could slow passenger movement. CBP supervisors also said the check digit feature

Figure 4: Global Entry Kiosk Receipt



Source: OIG obtained from the internet

⁸ According to CBP, 5,751 is the total number of Global Entry passengers that CBP processed at the Federal Inspection Service area during the days tested.

⁹ CBP processed 231 Global Entry members at the Federal Inspection Service area during our observation period.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

was cumbersome and they do not use it when processing Global Entry members through the Federal Inspection Service area.

CBP supervisors at seven of the nine airports did not disseminate the Daily Security Code, also shown in figure 4. Each day, supervisors are supposed to disseminate the daily code and the officers at the exit area are required to ensure the [REDACTED]. However, supervisory officers we interviewed were either unaware of the requirement or did not follow policies and procedures. Failure to disseminate the Daily Security Code prevents officers from validating the authenticity of Global Entry receipts.

CBP Officers Did Not Properly Respond to a Breach in the Daily Security Code

Figure 5: Discarded Global Entry Receipt



Source: OIG Photograph

CBP officers did not properly respond to a Daily Security Code breach. During testing, as shown in figure 5, we observed a receipt left unattended on a Global Entry kiosk. According to the Handbook, “A DSC breach is an event whereby the DSC has been compromised. Examples include: finding a discarded receipt; utilization of the receipt by someone other than the Global Entry member; and discovery or suspicion of a tampered or counterfeited receipt. When a DSC breach is suspected, the Watch Commander and all appropriate CBP personnel must be notified immediately. The breach circumstances may warrant further reporting and/or changing of the security code.” During our visit, CBP officers failed to take corrective action when we notified staff of the breach. According to the officers, they were

unaware of the Daily Security Code breach procedures. A traveler with malicious intent could use a compromised Daily Security Code to gain expedited entry into the United States.

Additionally, we found a picture of an actual Global Entry receipt containing a member’s photo, a Daily Security Code, and the Security Check Digit readily available on the internet, as shown in figure 4. According to the Handbook, the receipt found on the internet may constitute a breach of the Daily Security Code because it can be reproduced and fraudulently used. To illustrate, in 2 of



~~**SENSITIVE SECURITY INFORMATION**~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

11 (18 percent)¹⁰ covert tests conducted by CBP's Operational Field Testing Division from FY 2010 to FY 2017, testers successfully entered the United States using fake Global Entry receipts created from easily obtainable, open source materials, such as the kiosk receipt we found on the internet. CBP cannot prevent Global Entry members from sharing photos, Daily Security Codes, and Security Check Digits of Global Entry receipts. As a result, CBP cannot prevent breaches of the Daily Security Code and a person could enter the United States using a fraudulent receipt created from an open source displaying an authentic Daily Security Code and Security Check Digit.

CBP's Manual Verification Policy Is Insufficient

CBP's manual verification of Global Entry receipts is cumbersome, ineffective, and inadequate to authenticate Global Entry receipts. CBP officers we spoke with agreed with our assessment that the manual process is cumbersome and ineffective. A manual process that requires an officer [REDACTED] on each receipt and check a Daily Security Code composed of a [REDACTED] is time consuming and does not meet the intent of expedited Global Entry. Additionally, the process in the policy cannot prevent a compromised code or the use of fraudulent receipts.

We inquired whether the Trusted Traveler Program considered verifying receipt authenticity through a real-time system rather than manually. CBP officials explained that officers at exit lanes have access to multiple data systems they can use to verify the authenticity of Global Entry receipts in real time. However, according to the officials, the policy does not require this type of real-time authentication because the Global Entry receipt has built-in security features such as the Daily Security Code and the Security Check Digit. Unless CBP redesigns its Global Entry receipt authentication process to make it less complicated and easier for CBP officers to use, travelers with malicious intent may gain expedited entry using a fraudulent receipt.

Weaknesses Identified in Global Entry Compliance Programs

CBP does not effectively monitor the program to ensure members continue to meet Global Entry requirements. Specifically, CBP did not conduct the required number of internal audits or adequately document the results of the audits. In addition, CBP did not use its Self-Inspection Program effectively. CBP's lack of adherence to its compliance program's policies and procedures creates

¹⁰ We identified a number of concerns with CBP's Operation Field Testing Division covert testing procedures. As a result, we initiated a review of CBP's Operation Field Testing Division.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
 Department of Homeland Security

vulnerabilities in Global Entry by allowing potentially ineligible members to continue to participate.

CBP Did Not Conduct Required Vetting Center Internal Audits

CBP did not conduct the required number of internal audits. According to *CBP’s Vetting Center Policy-Internal Audits of Trusted Traveler Program Application Vetting SOP (April 2013)* (hereafter referred to as “audit policy”), vetting center officers are required to review 20 randomly selected completed applications monthly. This monitoring helps ensure continued compliance with Global Entry requirements and identify ineligible members for removal. As shown in table 3, for 16 of the 24 months in 2016 and 2017, CBP did not review the required number of randomly selected completed applications. For 12 of the 16 months, CBP did not review any applications at all. Not adhering to its policy raises the possibility that CBP will allow ineligible members to continue to participate in Global Entry.

Table 3: Vetting Center Global Entry Audits of Randomly Selected Applications, Calendar Years 2016–2017

Month	2016 Number of Applications Reviewed	Did Not Meet Minimum of 20 Applications Reviewed (✓)	2017 Number of Applications Reviewed	Did Not Meet Minimum of 20 Applications Reviewed (✓)
January	57		0	✓
February	33		0	✓
March	78		1	✓
April	48		35	
May	29		0	✓
June	19	✓	0	✓
July	0	✓	12	✓
August	0	✓	0	✓
September	0	✓	0	✓
October	10	✓	0	✓
November	0	✓	122	
December	0	✓	179	

Source: OIG analysis of CBP data

Vetting Center Internal Audits Lacked Documentation and Trend Analysis

CBP did not document the results of internal audits or any actions taken by the vetting center. According to CBP’s internal audit policy, “any audit findings which indicate a previously approved applicant should be revoked due to a risk



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

indicator or non-compliance with policy will be revoked.” During one internal audit of an approved Global Entry member (see “Member 5” in appendix D), CBP identified an incident in which an officer found marijuana seeds in the member’s vehicle during a routine vehicle inspection at a border crossing. However, vetting center officials did not document whether they decided the incident warranted revoking Global Entry benefits. CBP officials explained audit policy does not require such documentation, but without properly documenting the rationale for actions taken, there is no way to understand or know whether the decisions were appropriate.

Although CBP identified this discrepancy during an internal audit, vetting center officials believed the member’s potential query match did not warrant Global Entry membership denial or revocation. After we brought this situation to Trusted Traveler Program officials at headquarters, CBP revoked the individual’s Global Entry membership. After discussions with the vetting center, the Trusted Traveler Program Office reversed its decision and re-granted Global Entry benefits to the member. This occurred because CBP’s audit policy does not require the vetting center to communicate audit results to program offices at headquarters for concurrence and appropriate action. Without adequate documentation and coordination with headquarters, vetting center internal audits will not lead to corrective actions or identification of areas where vetting needs improvement.

CBP also did not analyze trends in its internal audit results, which may limit the audits’ effectiveness. According to *GAO’s Standards for Internal Controls*, management should evaluate results of ongoing monitoring activities to ascertain the effectiveness of internal controls. However, CBP’s audit policy does not direct CBP officers to track or analyze internal audit results and corrective actions. Trend analysis can benefit Global Entry by better focusing its resources to mitigate risk. When we questioned CBP officials, they said they analyze trends in other Trusted Traveler Programs but not Global Entry. CBP officials further explained they could use the framework in place for other Trusted Traveler Programs to track and analyze trends in Global Entry.

CBP Did Not Use Its Self-Inspection Program Effectively

CBP did not use its Self-Inspection Program to ensure CBP officer compliance with Global Entry policies and procedures. According to the Handbook, enrollment centers and ports of entry should focus inspection efforts on effectiveness and adherence to standard operating procedures. However, CBP focused its compliance measures on customer service. By focusing on customer



~~**SENSITIVE SECURITY INFORMATION**~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

service, CBP may be missing opportunities to identify and correct the issues identified in this report.

For FYs 2016–2017, to test Global Entry nationally at 70 and 76 locations, respectively, CBP incorporated three customer service-focused questions from a previously developed list. CBP used the following three questions:

1. Did the enrollment center take appropriate action to ensure timely appointment availability for interviewing applicants conditionally approved for the Trusted Traveler Programs?
2. Did the Enrollment Center supervisor perform a review and approve all denials and revocations?
3. Were all trusted travelers referred to secondary screening for compliance checks given priority processing in secondary screening?

In these two fiscal years, self-inspection results for Global Entry showed about 93 percent compliance with these measures. However, answering these questions showed whether CBP enhanced the experience of customers but did not elicit information about adherence to standard operating procedures and program requirements. CBP officials did not explain why they asked customer-focused questions instead of questions related to procedures and requirements.

To test compliance and ultimately respond more effectively to risks and issues identified in this report, CBP would benefit from using the questions already developed in its Handbook focused on operational procedures. For example:

- Are the proper comments concerning eligibility determinations recorded in the Global Enrollment System?
- Does the enrollment center staff cover the issues listed in the Handbook?
- Are employees trained on Trusted Traveler Program procedures and policies?

CBP might also focus its Self-Inspection Program on testing operational procedures to effectively measure compliance. Without doing so, CBP cannot respond to potential risks and issues identified through its Self-Inspection Program.

Conclusion

Global Entry allows expedited entry for pre-approved, low-risk travelers. However, even one traveler using Global Entry to enter the United States with the intent to cause harm or carry out illicit activities constitutes a threat. CBP officers entrusted to protect the public against such threats must adhere to



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Federal law and internal policies and procedures. Strengthening controls will help ensure compliance with policies and procedures, as well as effective operations. Until CBP addresses the vulnerabilities we identified, individuals intending to do harm or carry out criminal activities may exploit Global Entry.

Recommendations

Recommendation #1: We recommend the Executive Assistant Commissioner for the Office of Field Operations develop a method, including but not limited to enhanced training and oversight to ensure CBP officers at the vetting, enrollment centers, and ports of entry follow Federal regulations and Global Entry Program policies and procedures.

Recommendation #2: We recommend the Executive Assistant Commissioner for the Office of Field Operations properly document results of analysis conducted for potential query matches for Member 2, Member 5, and all members going forward to ensure they meet Global Entry low-risk requirements. After CBP completes its analysis, it should re-evaluate whether Member 2 and Member 5 meet the low-risk criteria and determine each member's Global Entry eligibility.

Recommendation #3: We recommend the Executive Assistant Commissioner for the Office of Field Operations update the policies and procedures in CBP's *Consolidated Trusted Traveler Programs Handbook (April 2016)* to include descriptions, explanations, and examples of how CBP officers should use record match-type classifications.

Recommendation #4: We recommend the Executive Assistant Commissioner for the Office of Field Operations develop and evaluate improved methods to ensure CBP officers authenticate Global Entry membership prior to travelers exiting the Federal Inspection Service area.

Recommendation #5: We recommend the Executive Assistant Commissioner for the Office of Field Operations update the policies and procedures in the *CBP Vetting Center Policy-Internal Audits of Trusted Traveler Program Application Vetting SOP* to include:

- performance of compliance reviews;
- communication of results to the Global Entry Program Office for concurrence and appropriate action; and
- identification of risk areas, and a method to track, analyze, and address trends.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Recommendation #6: We recommend the Executive Assistant Commissioner for the Office of Field Operations add operational Global Entry Program procedures to the Self-Inspection Worksheet to effectively measure Global Entry Program compliance.

Management Comments and OIG Analysis

CBP concurred with our six recommendations, and is taking steps or has implemented actions to address them; however, it did not concur with our conclusion that Global Entry is vulnerable to exploitation. We titled our report based on the entirety of our audit results. Additionally, CBP based its non-concurrence with the report title on our statistical sample results, which account for a portion of our audit. CBP did not consider the number of potentially ineligible members participating in the program, the vulnerabilities in the airport arrival process, nor its ineffective compliance programs. As a result, the weaknesses identified in Global Entry make it vulnerable to exploitation.

Appendix B contains CBP's management comments in their entirety. We also received technical comments to the draft report and revised the report as appropriate. We consider all recommendations resolved and open. A summary of CBP's responses and our analysis follow.

CBP Comments to Recommendation 1: Concur. CBP will create a nationwide training team to implement best practices in support of national, standardized training. Additionally, CBP will develop job aids for the management of Global Enrollment System data, interpretation of Risk Assessment Worksheet data, and interview Enrollment Center scenarios. Estimated Completion Date: February 29, 2020.

OIG Analysis of CBP Comments: CBP has taken steps to satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that all planned corrective actions are completed.

CBP Comments to Recommendation 2: Concur. CBP will update the Trusted Traveler Programs Handbook to include a series of questions to address where there is doubt as to whether an applicant meets the strict standards of the program. Estimated Completion Date: February 29, 2020.

OIG Analysis of CBP Comments: CBP has taken steps to satisfy the intent of this recommendation. We consider this recommendation resolved, but it will



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

remain open until CBP provides documentation to support that all planned corrective actions are completed.

CBP Comments to Recommendation 3: Concur. CBP will update the Trusted Traveler Programs Handbook to include policy, operational, procedural, and technological changes and advancements focused on strengthening identified program security vulnerabilities. Additionally, CBP will update its SharePoint website to include updated policy documents, memos, musters, and reference guides. Estimated Completion Date: February 29, 2020.

OIG Analysis of CBP Comments: CBP has taken steps to satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that all planned corrective actions are completed.

CBP Comments to Recommendation 4: Concur. CBP management will engage Field Offices immediately to reinforce policy and will re-publish field memoranda regarding Global Entry receipt security features. Additionally, CBP management has mandated a Training Cohort to travel to ports of entry to reiterate basic Global Entry security training. Estimated Completion Date: June 30, 2019.

OIG Analysis of CBP Comments: CBP has taken steps to satisfy the intent of this recommendation. However, CBP did not address the development and evaluation of improved methods to ensure CBP officers authenticate Global Entry membership prior to travelers exiting the Federal Inspection Service area. We will work closely with CBP to ensure CBP addresses the vulnerabilities identified within the Federal Inspection Service Area in its corrective actions. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that all corrective actions are completed.

CBP Comments to Recommendation 5: Concur. CBP will revise policy to include regular performance of compliance reviews conducted by supervisors, sharing of compliance reviews with Trusted Traveler Program Office management, and a method of identifying risk areas and tracking, analyzing, and addressing trends. Estimated Completion Date: June 30, 2019.

OIG Analysis of CBP Comments: CBP has taken steps to satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that all planned corrective actions are completed.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

CBP Comments to Recommendation 6: Concur. CBP will update the Global Entry Self-Inspection Program worksheet to include the critical elements of policy and procedure, inclusive of training, oversight, and quality control. Estimated Completion Date: February 29, 2020.

OIG Analysis of CBP Comments: CBP has taken steps to satisfy the intent of this recommendation. We consider this recommendation resolved, but it will remain open until CBP provides documentation to support that all planned corrective actions are completed.



~~SENSITIVE SECURITY INFORMATION~~
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*.

Our audit objective was to determine to what extent CBP controls over Global Entry prevent high-risk travelers from obtaining expedited screening. To accomplish our objective, we reviewed Federal laws and regulations related to Global Entry and CBP's internal controls, policies, procedures, and guidance associated with Global Entry.

We interviewed CBP personnel from the Office of Field Operations, Trusted Traveler Program Office, Office of Information Technology, and Office of Intelligence. Additionally, we interviewed officials at CBP's vetting center in Williston, Vermont, and observed Global Entry vetting processes. We also interviewed representatives from TSA's Office of Intelligence and Analysis.

We analyzed CBP data on Global Entry; revocations associated with violations; and approved members identified by CBP as having a "potential match" on its Risk Assessment Worksheet for FYs 2016–2017. We used IDEA data analysis software to draw a statistically random sample of Global Entry-approved members identified by CBP as having a "potential match" on its Risk Assessment Worksheet for FYs 2016–2017. We based our sample on a population size of 663,936, a 90 percent confidence interval, a 5 percent sampling error, and a 50 percent population proportion. With this statistically valid random sample, each member in the population had a nonzero probability of being included. Based on these parameters, a statistically valid sample would need to include at least 272 participant files. We drew a random sample of [REDACTED] participant files ([REDACTED] files more than the required 272 files) from the universe of 663,936 participant files that CBP's Office of Information Technology provided.

We tested each file for accurate vetting of criminal, customs, and immigration violation history. For example, we considered an error to be a disqualifying offense if a CBP officer either missed or improperly classified a member during the vetting process. Additionally, we tested each participant's file by comparing CBP data contained in its Global Enrollment System to enforcement queries listed in appendix C for each item in our sample. We considered an error or classified a member as ineligible for the program if CBP did not identify a disqualifying factor in accordance with 8 CFR 235.12(b), *Program Eligibility Criteria* and CBP's *Trusted Traveler Programs Handbook (April 2016)*, or did not



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

properly classify vetting results as relevant to the application. Based on our sample results, 4 of [REDACTED] participants are ineligible for Global Entry. Therefore, based on the [REDACTED] percent of ineligibles in our sample, we inferred that the point estimate of the total population of Global Entry participants identified by CBP as having a “potential match” on its Risk Assessment Worksheet contained [REDACTED] potentially ineligible members.

We tested Global Entry operations at nine airports during FY 2018: Philadelphia International Airport; Baltimore-Washington International Airport; Newark Liberty International Airport; Miami International Airport; Fort Lauderdale-Hollywood International Airport; Orlando International Airport; San Francisco International Airport; Oakland International Airport; and San Jose International Airport. We selected these airports because they represented four of seven CBP port regions and based on the geographic proximity to other U.S. airports we tested. At these airports, we tested operations and interviewed CBP officers including port directors, assistant port directors, supervisors, and officers stationed in Federal Inspection Service areas and enrollment centers.

We conducted 6 days of testing at nine airports. At each airport, we observed Global Entry members’ kiosk usage and exit procedures for at least one international flight. We observed 231 Global Entry members. We also conducted interviews at all nine airports with CBP officers regarding Global Entry kiosk and exit procedures, including the authentication of kiosk receipts. Further, we obtained from CBP the total number of Global Entry members who successfully used Global Entry kiosks for the 6 days we performed testing. We used this information to determine that 5,751 travelers used the Global Entry kiosks during the 6 days we tested to gain expedited entry to the United States. Additionally, we obtained and analyzed results of CBP’s Office of Field Testing Division for all Global Entry tests conducted during the history of the program.

We also observed 43 enrollment center interviews. We selected these travelers and interviews based on arrival times of international flights during the days of our testing and enrollment center interview schedules. We cannot generalize our testing results of 9 airports to all 61 airports with Global Entry. However, we believe the evidence obtained provides a reasonable basis for our conclusions.

We obtained and analyzed CBP data on vetting center internal audits for calendar years 2016 and 2017 and Global Entry evaluation results from its Self-Inspection Program for FYs 2016–2017. We data mined the population of vetting center internal audit results for Global Entry members identified as having a “discrepancy” for calendar years 2016–2017. We compared those



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

results to the population of approved Global Entry members identified as having a “potential match” on their Risk Assessment Worksheet. We found and analyzed five members meeting our criteria. We tested each file for accurate vetting of criminal, customs, and immigration violation history (as described previously in our statistical sample). For the Global Entry Program Evaluation results from its Self-Inspection Program for FYs 2016–2017, we analyzed the questions and results to determine how CBP monitors Global Entry performance.

To assess the reliability of CBP’s Global Entry data, we identified CBP’s Global Enrollment System as the primary storage database for all CBP Trusted Traveler Programs, including Global Entry. We reviewed existing information related to the Global Enrollment System, received a walkthrough of the system while we interviewed CBP’s Office of Information Technology subject matter experts, performed electronic testing to include tracing and verifying key data elements, and reviewed selected Global Enrollment System controls. Prior to performing electronic testing of data files, we watched CBP officials extract and replicate the data we requested because we did not have access to the Global Enrollment System. Following our data reliability assessment of CBP’s Global Enrollment System, we determined the data to be sufficiently reliable to support the findings, recommendations, and conclusions in this report.

We conducted this performance audit between September 2017 and August 2018 pursuant to the *Inspector General Act of 1978*, as amended, 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
CBP Comments to the Draft Report

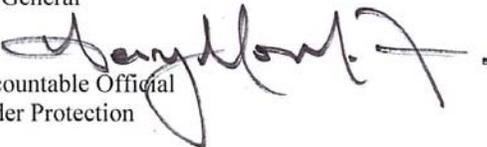
~~SENSITIVE SECURITY INFORMATION~~

1300 Pennsylvania Avenue NW
Washington, DC 20229



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

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General for Audits
Office of the Inspector General

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

SUBJECT: Management Response to Draft Report: "CBP's Global Entry
Program is Vulnerable to Exploitation"
(Project No. 17-102-AUD-CBP)

Thank you for the opportunity to review and 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 that the OIG has recognized its effort to monitor Global Entry (GE) effectiveness, compliance and adherence to standard operating procedures through its vetting center, internal audits and its Self-Inspection Program. Today, there are more than 6.1 million GE members approved to enter the United States using automated kiosks at 60 U.S. airports and 15 preclearance locations.

CBP utilizes a layered management approach for greater control over the roles in vetting, approval and redress for Trusted Traveler Programs (TTP) applicants. CBP's Office of Field Operations (OFO), Admissibility and Passenger Programs (APP), TTP Program Management Office (PMO), exercises policy oversight over CBP's TTP, inclusive of GE. The TTP PMO relies heavily on the vetting center (VC), enrollment centers (EC), and airport personnel to accomplish the GE program objectives. The OFO, Director of Field Operations (DFO), Boston has oversight of the TTP VC in Williston, Vermont. The relevant port of entry (POE) and DFO over the respective POE manage the TTP ECs. The CBP Ombudsman provides a redress opportunity for individuals who believe their TTP membership is denied or revoked due to incomplete or incorrect information.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need-to-know", as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~



~~**SENSITIVE SECURITY INFORMATION**~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

~~**SENSITIVE SECURITY INFORMATION**~~

CBP has begun implementation of the recommendations in the OIG's draft report. With the recent installation of new leadership for both the TTP PMO and VC, CBP has initiated an ambitious, phased plan to develop and deliver enhanced TTP training for CBP officers at the POEs, as well as the ECs and VC. The CBP Consolidated Trusted Traveler Programs Handbook (revised April 2016), is currently being updated. In addition, OFO is developing a more operationally conducive method, leveraging advances in technology and their application to border controls to ensure that only authorized GE members are able to exit the Federal Inspection Service areas at airports where GE is operational.

However, OFO disagrees with many of the OIG's broader conclusions, which do not take into account the complete GE process, to include the redress opportunity with the CBP Ombudsman. Following an official review by the CBP Ombudsman, two of the four GE applicants pulled from the OIG's random sample of [REDACTED] (Member 1 and Member 2) as having been identified as approved for GE membership in error, have either had their GE benefits reinstated or sustained. The CBP Ombudsman also completed a formal review of Member 5, concluding that the individual merits reinstatement of GE benefits. The OIG's conclusion, reflected by the report's title, that CBP's Global Entry Program is Vulnerable to Exploitation does not accurately reflect CBP's effectiveness in preventing ineligible foreign nationals and/or those linked to national security concerns from enrollment in GE.

The draft report contained six recommendations, with which CBP concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under separate cover.

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.

Attachment

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

~~SENSITIVE SECURITY INFORMATION~~

**Attachment: Management Response to Recommendations Contained in
OIG Project Number 17-102-AUD-CBP**

The Office of Inspector General (OIG) recommended that the Executive Assistant Commissioner for the Office of Field Operations (OFO):

Recommendation 1: Develop a method, including but not limited to enhanced training and oversight to ensure CBP officers at the vetting, enrollment centers, and ports of entry follow Federal regulations and Global Entry Program policies and procedures.

Response: Concur. The CBP OFO, Trusted Traveler Program (TTP) will create a nationwide TTP Training Team composed of CBP supervisors from Field Offices, TTP Enrollment Centers (EC), the TTP Vetting Center (VC) and the TTP Program Management Office (PMO) to implement best practices in support of national, standardized TTP training. The training will include eight modules that CBPOs will have to complete in order to be granted access to the TTP network of systems. TTP Headquarters personnel will conduct and implement the training across all Field Offices to disseminate to the Ports of Entry (POE). The TTP PMO is developing TTP job aids for the management of the internal Global Enrollment System (GES), interpretation of the Risk Assessment Worksheet data, standardized interviews and routine EC scenarios. Estimated Completion Date (ECD): February 29, 2020

Recommendation 2: Properly document results of analysis conducted for potential query matches for Member 2, Member 5, and all members going forward to ensure they meet Global Entry low-risk requirements. After CBP completes its analysis, it should re-evaluate whether Member 2 and Member 5 meet the low-risk criteria and determine each member's Global Entry eligibility.

Response. Concur. The update to the Consolidated Trusted Traveler Programs Handbook (revised April 2016), Standard Operating Procedures (SOP) will include a series of questions to address when there is doubt as to whether an applicant meets the strict standards of the program. ECD: February 29, 2020

Recommendation 3: Update the policies and procedures in CBP's Consolidated Trusted Traveler Programs Handbook (April 2016) to include descriptions, explanations, and examples of how CBP officers should use record match-type classifications.

Response: Concur. The OFO, Admissibility and Passenger Programs (APP), TTP management is updating CBP's Consolidated Trusted Traveler Programs Handbook to

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need-to-know", as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

~~SENSITIVE SECURITY INFORMATION~~

include policy, operational, procedural, and technological changes and advancements focused on strengthening identified program security vulnerabilities. TTP personnel are currently reviewing and updating the TTP SharePoint website to transform the TTP SharePoint website into a user-friendly repository where CBPOs can reference any updated policy documents to include memos, musters, and reference guides. ECD: February 29, 2020

Recommendation 4: Develop and evaluate improved methods to ensure CBP officers authenticate Global Entry membership prior to travelers exiting the Federal Inspection Service area.

Response: Concur. OFO, APP, TTP management will have immediate engagement with the Field Offices to reinforce the SOP and reinforce the requirements for Daily Security Code (DSC) / Security Check Digit (SCD) on the GE kiosk receipts. In addition to the DSC or SCD, the printed receipt has two other security features. They are: 1) [REDACTED] and, 2) [REDACTED]. The [REDACTED] was added as a security feature in 2012.

OFO, APP, TTP management will re-publish field memoranda requiring Supervisory CBPOs to daily brief CBPOs regarding issue of the DSC and to verify additional GE receipt security features to include [REDACTED] and [REDACTED].

OFO, APP, TTP management has also mandated a Training Cohort to travel to the POEs to reiterate basic Global Entry (GE) security training. ECD: June 30, 2019

Recommendation 5: Update the policies and procedures in the CBP Vetting Center Policy-Internal Audits of Trusted Traveler Program Application Vetting SOP to include:

- performance of compliance reviews;
- communication of results to the Global Entry Program Office for concurrence and appropriate action; and
- identification of risk areas, and a method to track, analyze, and address trends.

Response: Concur. Trusted Traveler VC management will revise the CBP VC Policy entitled "*Internal Audits of Trusted Traveler Program Application Vetting SOP*," dated February 2018. The updated policy will meet the criteria outlined in the audit recommendation including:

- Regular performance of compliance reviews conducted by supervisors on their direct report employees' vettings. Reviews are to be done on a quarterly basis utilizing a random sample of a minimum of 20 applications per employee.

WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need-to-know", as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

~~SENSITIVE SECURITY INFORMATION~~

- Quarterly summaries of the compliance reviews are to be saved within the VC management records and actionable items derived from the analysis can be shared with TTP management.
- A method of identifying risk areas, tracking, analyzing and addressing trends has been devised with actionable items to be addressed by VC management.

ECD: June 30, 2019

Recommendation 6: Add operational Global Entry Program procedures to the Self-Inspection Worksheet to effectively measure Global Entry Program compliance.

Response: Concur. TTP PMO will update the GE Self-Inspection Program worksheet to include the critical elements of policy and procedure, inclusive of training, oversight and quality control. ECD: February 29, 2020

WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R parts 15 and 1520.



~~**SENSITIVE SECURITY INFORMATION**~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C

Vetting Systems, Databases, and Modules

1. Unified Passenger (UPAX)	UPAX aggregates data in a consolidated, automated interface, and serves as a web-based enforcement and decision support tool used to collect, analyze, and disseminate information for the identification of potential terrorists, transnational criminals, and other persons who pose a higher risk of violating U.S. law.
2. TECS	Serves as a data repository to support law enforcement “lookouts,” border screening, and reporting for CBP’s primary and secondary inspection processes, which are generally referenced as TECS Records or Subject Records.
3. U.S. Citizenship and Immigration Service (USCIS) Person Centric Query Service (PCQS)	PCQS allows users to submit a single query and view all transactions involving an immigrant or nonimmigrant across multiple DHS and external systems. PCQS queries 15 different USCIS data systems.
4. Automated Biometric Identification System (IDENT)	IDENT stores and processes biometric data and links biometric information to establish and verify identities. IDENT serves as the biographic and biometric repository for DHS.
5. Global Enrollment System	Information Technology system that facilitates enrollment and security vetting for CBP’s voluntary Trusted Traveler, Registered Traveler, and Trusted Worker Programs.
6. Advanced Passenger Information System (APIS)	DHS collects certain information on all passenger and crew members who arrive in or depart from (and, in the case of crew members, overfly) the United States on a commercial air or sea carrier in APIS.
7. Passenger Name Record (PNR)	U.S. law requires airlines operating flights to, from, or through the United States to provide CBP with certain passenger reservation information, called PNR data, primarily for purposes of preventing, detecting, investigating, and prosecuting terrorist offenses and related crimes and certain other crimes that are transnational in nature.
8. Automated Targeting System (ATS)	ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments.
9. Enforcement Integrated Database (EID)	EID captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by certain DHS components, namely Immigration and Customs Enforcement (ICE) and CBP.
10. Electronic System for Travel Authorization (ESTA)	ESTA is a web-based application and screening system used to determine whether citizens and nationals are from countries participating in the Visa Waiver Program.
11. Student and Exchange Visitor Information System (SEVIS)	SEVIS is an internet-based system, located on-site at ICE, that maintains real-time information on nonimmigrant students (F-1 and M-1 classes of admission), exchange visitors (J-1 class of admission), and their dependents and spouses (F-2, M-2, and J-2 classes of admission).
12. Arrival and Departure Information System (ADIS)	ADIS contains biographic information, biometric indicators, and encounter data consolidated from various systems from DHS and the Department of State (DOS). ADIS facilitates the identification and investigation of individuals who may have violated their admission status by remaining in the United States beyond their authorized terms of entry.



~~**SENSITIVE SECURITY INFORMATION**~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

13. Border Crossing Information (BCI)	BCI includes certain biographic and biometric information; photographs; certain responses to inspection questions; certain mandatory or voluntary itinerary information provided by air, sea, bus, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing. BCI resides on the TECS information technology platform.
14. Seized Assets and Cases Tracking System (SEACATS)	SEACATS provides CBP with a single repository for enforcement actions related to the Treasury Forfeiture Fund, as well as seized property inventory and case processing information related to arrests, seized and forfeited property, fines, penalties, and liquidated damages.
15. Department of State Consular Consolidated Database (CCD)	CCD is a data warehouse that holds current and archived data from the Bureau of Consular Affairs domestic and post databases. The CCD stores information about U.S. persons (U.S. citizens and legal permanent residents), as well as foreign nationals (non-U.S. persons) such as Immigrant Visa applicants and Non-Immigrant Visa applicants. This information includes names, addresses, birthdates, biometric data (fingerprints and facial images), race, identification numbers (e.g., social security numbers and alien registration numbers) and country of origin.
16. Department of Justice, Federal Bureau of Investigation's (FBI) National Crime Information Center, Interstate Identification Index	The FBI maintains an automated database that integrates criminal history records, including arrest information and corresponding disposition information, submitted by Federal, state, local, tribal, and certain foreign criminal justice agencies. Each state has a criminal records repository responsible for the collection and maintenance of criminal history records submitted by law enforcement agencies in its state. The state record repositories are the primary source of criminal history records maintained at the FBI.
17. National Law Enforcement Telecommunications System (NLETS)	NLETS is a private not-for-profit corporation owned by the states that was created more than 50 years ago by the 50 state law enforcement agencies. The user population is made up of all of the United States and its territories, all Federal agencies with a justice component, selected international agencies, and a variety of strategic partners that serve the law enforcement community; users cooperatively exchange data. The types of data being exchanged varies, from motor vehicle and drivers' data, to Canadian and INTERPOL database records located in Lyon, France, to state criminal history records and driver license and corrections images.
18. Terrorist Screening Database (TSDB)	TSDB, a consolidated database maintained by the FBI's Terrorist Screening Center (TSC) provides information about those known or reasonably suspected of being involved in terrorist activity in order to facilitate DHS mission-related functions, such as counterterrorism, law enforcement, border security, and inspection activities.
19. INTERPOL	Information from INTERPOL in IDENT includes INTERPOL fingerprint files for valid INTERPOL notices issued since January 2002. These include fingerprints for wanted, missing, and deceased persons, persons with criminal histories, and persons of interest to law enforcement authorities.
20. Department of State Lost and Stolen Passports	The Department of State maintains a record of all lost or stolen passports and provides necessary information to CBP to facilitate its mission critical functions.
21. Lexis Nexis	Lexis Nexis, a private corporation, provides Government agencies a service that helps create reliable, timely, and actionable intelligence to defend against threats and maintain homeland security.



Appendix D

Ineligible Global Entry Members Statistical Sample

Member 1: A vetting center officer did not identify the passport used for the Global Entry application as reported lost/stolen. Our analysis revealed that this member used a lost/stolen passport to submit a Global Entry application. According to 8 CFR 235.12(f) each participant must possess a valid, machine-readable passport. Additionally, *CBP's Consolidated Trusted Traveler Programs Handbook (April 2016)* (hereafter referred to as "Handbook") states, "Generally, if low-risk status cannot be determined, the application must be denied." The vetting center officer should have provided comments directing the enrollment center officer to verify the identity of the applicant and to inquire why the applicant was in possession of a lost or stolen passport.

Member 2: An enrollment center officer did not have the information required to determine eligibility. This occurred because a vetting center officer did not clearly identify what additional information was needed from the applicant. We identified a Homeland Security Investigation, for [REDACTED]

[REDACTED] According to 8 CFR 235.12(b)(2)(vii), an applicant may not qualify for participation if the applicant cannot satisfy CBP of his or her low-risk status or meet other program requirements. Additionally, according to *CBP's Vetting Center Strict Standard Policy Review: Substantiating Risk (June 2013)* guidance, "[REDACTED]

[REDACTED] Additionally, the Handbook states, "Generally, if low-risk status cannot be determined, the application must be denied." The vetting center officer classified this query match as "Inconclusive" because the enrollment center officer needed to gather additional information to determine eligibility. Section 5.2, Risk Assessment Worksheet, of the Handbook states that if the vetting center discovers issues that need to be addressed during an interview (i.e., possible [REDACTED] etc.) the vetting center will pass the risk assessment and "conditionally approve" the applicant, providing comments in the Risk Assessment Worksheet. However, the enrollment center officer was not aware of what information the vetting center officer needed because it was not included in the "Findings" section of the Risk Assessment Worksheet. The enrollment center officer therefore approved the applicant in error.



~~**SENSITIVE SECURITY INFORMATION**~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Member 3: A vetting center officer did not properly assess the totality of the applicant's risk. Our analysis revealed that this member had multiple criminal misdemeanors. According to 8 CFR 235.12(b)(2)(ii), an applicant may not qualify for participation if the applicant has been arrested for, or convicted of, any criminal offense or has pending criminal charges or outstanding warrants in any country. The Handbook, Section 3.2, The Strict Standard for SENTRI, NEXUS, and Global Entry, states, "The standards for vetting NEXUS, SENTRI, and Global Entry applicants include the following: Allowance for one, single misdemeanor or summary conviction over ten years old, provided the conviction does not involve narcotics, weapons, pornography, any type of smuggling, trafficking or currency reporting violations." Additionally, the Handbook states, "Generally, if low-risk status cannot be determined, the application must be denied." The vetting center officer granted discretion for two charges; however, the remaining criminal history did not meet The Strict Standard. As a result, the enrollment center officer approved the applicant in error. This ineligible member successfully used Global Entry benefits to bypass primary screening and gain expedited entry into the United States on February 20, 2018.

Member 4: An enrollment center officer did not obtain all of the necessary court documentation as required by CBP policy. Our analysis revealed that this member had a criminal narcotics violation. According to 8 CFR 235.12(b)(2)(ii), an applicant may not qualify for participation if the applicant has been arrested for, or convicted of, any criminal offense or has pending criminal charges or outstanding warrants in any country. Additionally, the Handbook, Section 3.2, The Strict Standard for SENTRI, NEXUS, and Global Entry, states, "The standards for vetting NEXUS, SENTRI, and Global Entry applicants include the following: Allowance for one, single misdemeanor or summary conviction over ten years old, provided the conviction does not involve narcotics, weapons, pornography, any type of smuggling, trafficking or currency reporting violations." Furthermore, the Handbook, Section 6.6.4, Adjudicating Criminal History Data, states, "Applications should not be approved before the receipt of court documents when court documents are required." Finally, the Handbook states, "Generally, if low-risk status cannot be determined, the application must be denied." The vetting center officer entered comments on the Risk Assessment Worksheet identifying the need for court documentation for multiple criminal violations. However, the enrollment center officer failed to obtain documentation for a 2010 narcotics violation. As a result, the enrollment center officer approved the applicant in error.

Member 5: A vetting center officer did not classify a record properly for a narcotics seizure. According to 8 CFR 235.12(b)(2)(iii), an applicant may not qualify for participation if the applicant has been found in violation of any



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

customs, immigration, or agriculture regulations, procedures, or laws in any country. Additionally, the Handbook, Section 3.2, The Strict Standard for SENTRI, NEXUS, and Global Entry, states, “The standards for vetting NEXUS, SENTRI, and Global Entry applicants include the following: Allowance for one, single misdemeanor or summary conviction over ten years old, provided the conviction does not involve narcotics, weapons, pornography, any type of smuggling, trafficking or currency reporting violations.” The Handbook also states, “Generally, if low-risk status cannot be determined, the application must be denied.” The vetting center officer should have classified this record as “Positive-Relevant” instead of “Positive-Irrelevant.” Because the match was misclassified, the application bypassed supervisory review and the enrollment center officer was not aware of this disqualifying charge and approved the applicant. As a result, this member used Global Entry benefits on multiple occasions: May 19, 2017; August 18, 2017; November 4, 2017; November 21, 2017; and April 7, 2018.



~~SENSITIVE SECURITY INFORMATION~~
OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix E
Report Distribution

Department of Homeland Security

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

U.S. Customs and Border Protection

Commissioner
Executive Assistant Commissioner, Office of Field Operations
Audit Liaison

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committee

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