~~SENSITIVE SECURITY INFORMATION~~

OFFICE OF INSPECTOR GENERAL

Review of CBP Information Technology System Outage of January 2, 2017 (Redacted)

~~WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR Parts 15 and 1520. Do not disclose any part of this report to persons without a "need to know," as defined in 49 CFR Parts 15 and 1520, without the expressed written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department of Homeland Security.~~

Homeland Security

~~SENSITIVE SECURITY INFORMATION~~

November 21, 2017

OIG-18-19 (revised)

~~SENSITIVE SECURITY INFORMATION~~

DHS OIG HIGHLIGHTS

Review of CBP Information Technology System Outage of January 2, 2017

November 21, 2017

Why We Did This Audit

On January 2, 2017, a 4-hour system outage disrupted Custom and Border Protection's (CBP) processing of incoming international travelers at airports nationwide. We conducted this review to determine the effectiveness of CBP's efforts to address this system outage, as well as the sufficiency of its plans for minimizing the possibility and impact of similar system outages in the future.

What We Recommend

We are recommending that CBP implement improvements to its software testing, vulnerability patching, and disaster recovery capabilities.

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

What We Found

CBP took sufficient steps to resolve the January 2, 2017, outage on the same day it occurred. CBP's initial actions to resolve this outage were unsuccessful for several hours until CBP leadership decided to revert system queries from the TECS Modernization server environment to the TECS Legacy mainframe environment. As a result of this action, airports began to report that they could once again process passengers. After 4 hours, airports began reporting they were back online.

The transition back to the legacy environment worked to resolve the January 2 system outage. However, underlying issues that might result in future outages persisted in the CBP environment. Specifically, we identified:

- inadequate CBP software capacity testing, leaving the potential for recurrence of processing errors;
- deficient software maintenance, resulting in high vulnerabilities that remain open;
- ineffective system status monitoring to ensure timely alerts in case of business disruptions; and
- inadequate business continuity and disaster recovery capabilities to minimize the impact of system failures on the traveling public.

Until such deficiencies are addressed, CBP lacks a means to minimize the possibility and impact of similar system outages in the future.

Agency Response

CBP concurred with four of our five recommendations. A copy of CBP's formal response is in appendix B.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

May 3, 2019

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

FROM: Kristen Bernard
Deputy Assistant Inspector General
Information Technology Audits

SUBJECT: Revised Final Report: *Review of CBP Information Technology System Outage of January 2, 2017, (Report #OIG-18-19)*

Attached for your information is our revised final report, *Review of CBP Information Technology System Outage of January 2, 2017, OIG-18-19*. We are reissuing the report with a correction to the methodology under which the fieldwork for this report was conducted. This revision does not change the overall findings or recommendations in the report. Please see the attached errata sheet for details.

Please call me with any questions, or your staff may contact Kevin Burke, Director, Information Systems and Acquisitions at (202) 981-6360.

Attachment

cc:
Jim Crumpacker, Director, Departmental GAO/OIG Liaison Office
Robin White, Director, Management Inspections Division
OIG's DHS Liaison

Errata page for OIG-18-19

Review of CBP Information Technology System Outage of January 2, 2017

Change made to the Appendix A, 5th paragraph (see below):

Changed from:
We conducted this audit between January and March 2017 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.

Changed to:
We conducted this audit between January and March 2017 pursuant to the Inspector General Act of 1978, as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.

Table of Contents

Appendixes

Abbreviations

APIS	Advanced Passenger Information System
BIA	Business Impact Analysis
CBP	U.S. Customs and Border Protection
CPU	control processor unit
[redacted]	[redacted]
EDME	Enterprise Data Management and Engineering
EST	Eastern Standard Time
IT	information technology

JFK	John F. Kennedy International Airport
LAN	local area network
MIA	Miami International Airport
[redacted]	[redacted]
OIG	Office of Inspector General
OIT	Office of Information and Technology
PSPD	Passenger Systems Program Directorate
TOC	Technology Operations Center
TSD	Technology Service Desk

Background

U.S. Customs and Border Protection (CBP) information technology (IT) systems and tools support the component's day-to-day mission operations along the border and across its 328 land, sea, and air ports of entry. On a typical day, CBP welcomes nearly 1 million visitors, screens more than 67,000 cargo containers, arrests more than 1,100 individuals, and seizes nearly 6 tons of illicit drugs.

Critical systems provide capabilities for CBP officers to make real-time determinations of admissibility for passengers and pedestrians entering the United States, as well as to conduct border enforcement activities such as the apprehension of illegal aliens. For example, TECS (not an acronym) is the principal system used by officers at the border to assist with screening and determinations regarding admissibility of arriving persons. Originally developed in the 1980s, TECS provides traveler processing and screening, investigations, case management, and intelligence functions for multiple Federal, state, and local agencies. Over time, TECS became increasingly difficult and expensive to maintain due to technology obsolescence and its inability to support new mission requirements. In 2008, DHS initiated TECS Modernization to update existing system functionality, address known capability gaps, and move the program's infrastructure to DHS' new data centers.

Further, the Advanced Passenger Information System (APIS) is used to process queries of TECS databases about passengers on inbound and outbound flights before their arrival in or departure from the United States. TECS provides border inspection, investigative, interdiction, intelligence analysis and integrity tracking support software and communications. TECS' major functions support passenger processing and investigations. Outages in TECS can have a severe impact on arriving international passengers.

On January 2, 2017, a CBP system outage caused significant disruptions in CBP's processing of incoming international travelers at airports nationwide. Specifically, at approximately 4:15 p.m. Eastern Standard Time (EST), a slowdown in APIS hindered CBP officers' ability to process international passengers arriving at air and sea ports nationwide. At approximately 5:00 p.m. EST, this slowdown effectively became an outage in both APIS and

TECS, given the extreme delays experienced in processing queries on CBP's APIS. More than 13,000 passengers and 109 flights were significantly delayed by the 4-hour outage at Miami International Airport (MIA) alone. (See figure 1.) According to CBP staff at MIA, challenges in managing the outage included difficulties with crowd control, temperature, health emergencies, and officer safety. CBP brought in additional support from the Miami police department to help manage the crowds of delayed passengers during this outage.

Figure 1: Passenger Backlog at Miami International Airport during the January 2, 2017 Outage

Source: CBP staff at Miami International Airport

We conducted this review to explore the root cause of the January 2, 2017 outage, given its impact on CBP mission operations and the traveling public. Specifically, our objective was to determine the effectiveness of CBP's efforts to address the system outage, as well as the sufficiency of its plans for minimizing the possibility and impact of similar system outages in the future.

Results of Audit

CBP took sufficient steps to resolve the January 2, 2017 outage on the same day it occurred. CBP's initial actions to resolve this outage were unsuccessful for several hours. Ultimately, the CBP Assistant Commissioner of the Office of Information and Technology (OIT) decided to revert system queries from the TECS Modernization server environment to the TECS Legacy mainframe environment. As a result of this action, airports began to report that they could process passengers again. After 4 hours, airports began reporting that they were back online.

The transition back to the legacy environment worked to resolve the January 2, 2017 system outage. Nevertheless, underlying causes that might result in future outages were not addressed and persist today in the CBP environment. Specifically, we identified:

- inadequate CBP software capacity testing, leaving the potential for the recurrence of processing errors;
- deficient software maintenance, resulting in high vulnerabilities that remain open;
- ineffective system status monitoring to ensure timely alerts in case of mission-business disruptions; and
- inadequate business continuity and disaster recovery processes and capabilities to minimize the impact of system failures on the traveling public.

Until such deficiencies are addressed, CBP lacks a means to minimize the possibility and impact of similar system outages in the future.

CBP Actions to Resolve the Recent Outage

CBP's actions were adequate to resolve the January 2, 2017 system outage on the same day it occurred. As previously stated, the outage started at 4:15 p.m. EST, as a sporadic TECS slowdown, but by 5:03 p.m. EST had become a full outage, given the severity of the processing delays. For several hours, CBP was unsuccessful in its efforts to address the outage. For example, CBP tried shutting down and restarting TECS servers, but this did not alleviate the problem.

At 8:22 p.m. EST, the CBP Assistant Commissioner of OIT directed CBP staff to revert from working in the TECS Modernization server environment to the TECS Legacy mainframe environment to process queries about arriving passengers. This action proved successful and by approximately 8:40 p.m. EST, airports began to report that they could process passengers again. By 10:15 p.m. EST, all airports had indicated that they were back online. Appendix C provides more detailed information on this timeline and actions taken by CBP.

CBP's initial investigation into the cause of the outage determined that processing in the TECS Modernization server environment was taking too long due to the large volume of queries on January 2, 2017. CBP was challenged with managing an inordinately high number of travelers just after the New Year holiday. According to CBP staff, the 451,182 queries processed on January 2, 2017, before the outage, exceeded the highest daily number of queries for all days in the previous month. Table 1 shows the total number of queries run on Monday, January 2, 2017, as well as for three previous Mondays.

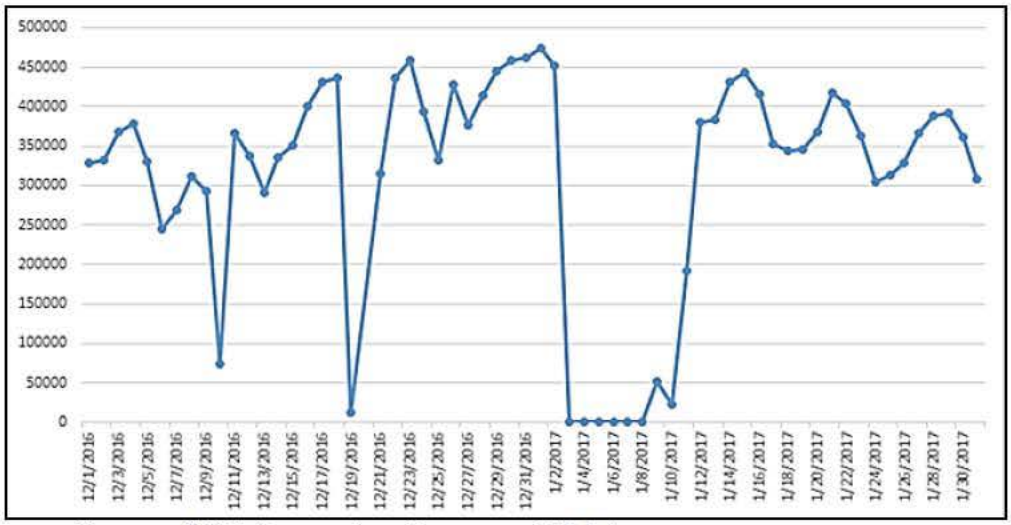
Table 1: Total Number of Queries in the TECS Modernization Server Environment for Three Mondays in December 2016 and on January 2, 2017

Date	Number of Queries per Day
December 4, 2016	377,382
December 11, 2016	366,668
December 18, 2016	437,519
January 2, 2017	451,182 (up to the point where queries were switched to the TECS Legacy environment)

Source: CBP's Inspection Processes Division

Similarly, figure 2 shows an incremental climb in the daily number of TECS queries from December to January, with the high point on January 2, 2017. Following the outage and the transition back to legacy system use on January 2, 2017, no queries were processed in the TECS Modernization server environment until January 9, 2017. The full use of the TECS Modernization server environment resumed on January 11, 2017.

Figure 2: Daily Total Number of Queries in the TECS Modernization Server Environment, December 1, 2016, through January 31, 2017



Source: CBP's Inspection Processes Division

According to CBP staff, a programming change involved in the move from performing queries from the TECS legacy environment to the TECS Modernization server environment also contributed to the problem. The programming change started in April 2016 and was rolled out nationwide by November 2016.

Further review of application logs by CBP staff and contractors determined that an error handling routine in the TECS Modernization server environment was a direct cause of the outage. Specifically, when processing a large number of queries, this error handling routine sometimes did not terminate processing as designed. As such, computer processing resources used by the routine remained unavailable to support other software applications. CBP staff changed the amount of memory and processing resources allocated to this routine and also added code to ensure that the error handling routine stopped processing and closed correctly. CBP implemented these changes, and by January 12, 2017, TECS queries were being successfully processed in the TECS Modernization server environment.

Conditions that Could Result in Future Outages

The transition back to the legacy environment worked to resolve the January 2, 2017 system outage. However, underlying causes that might result in future outages were not addressed and persisted in the CBP environment. Specifically, we identified:

- inadequate CBP software capacity testing, leaving the potential for the recurrence of processing errors;
- deficient software maintenance, resulting in high vulnerabilities that remain open;
- ineffective system status monitoring to ensure timely alerts in case of mission-business disruptions; and
- inadequate business continuity and disaster recovery processes and capabilities to minimize the impact of system failures on the traveling public.

Until such deficiencies are addressed, CBP lacks a means to minimize the possibility and impact of similar system outages in the future.

Inadequate Software Testing

TECS software testing was not performed as required. According to the DHS 4300A *Sensitive Systems Handbook* (DHS 4300A Handbook), version 12.0:

> *As new systems and newly modified systems proceed through the System Engineering Life Cycle, changes must be documented and tested prior to placing the systems into an operational environment. The objective is to ensure that new vulnerabilities are not introduced during the change process. The same requirements apply to operational systems as they undergo periodic modifications.*

Specifically, the inability of the error handling routine to terminate processing as designed when there are a large number of queries should have been identified and resolved during testing before being implemented in a production environment. However, CBP's testing of TECS software changes was not adequate to identify problems that might occur when there are a large number of queries. For example, CBP staff only performed 34 test queries of a TECS software change before it was implemented on December 28, 2016. According to CBP staff, CBP does not have the ability to test hundreds of thousands of queries prior to implementing a TECS change because the test environment infrastructure is not on the same scale as the production environment.

Without a TECS test environment similar to the TECS production environment, CBP lacked a means to prevent the error of January 2, 2017. This problem persists, and the risk remains that a similar outage may occur again and prevent CBP officers from processing arriving international passengers in a timely fashion.

Inadequate Software Maintenance

CBP did not install operating system patches as required to keep the software up to date. According to DHS 4300A Handbook Attachment O, *Vulnerability Management Program*, version 9.1:

> *By continuous monitoring of their systems, DHS Component Vulnerability Analysis Teams, Information System Security*

Managers, and Information Systems Security Officers, ensure that their systems include the latest patch levels and comply with configuration guidance. Continuous monitoring is performed by reviewing current vendor patch notifications, security configuration best practices, security architecture guidance, and emerging threats and vulnerabilities.

However, the server operating system involved in the outage had a critical vulnerability associated with the error handling routine. CBP staff did not timely identify the vulnerability and install the relevant operating system patch in [redacted].

This critical vulnerability was identified by the operating system vendor on December 20, 2016. At that time, the vendor released a description of the critical vulnerability (e.g., an 'errata'), as well as a software patch to fix the problem. Neither CBP information systems security staff nor the vendor's onsite staff provided software testing staff with information concerning this critical vulnerability and its associated patch. Software testing staff remained unaware of this critical vulnerability until we discussed it with them in February 2017.

Additionally, CBP did not apply the software patch until February 2017. This occurred in part because the vulnerability was announced after CBP had already applied [redacted] operating system patches in December 2016. Further, CBP did not apply [redacted] patches to the operating system during January 2017 because it wanted to keep the system up and running during all of the preparations and activities related to [redacted]

To the extent that CBP does not provide timely notifications of critical operating system vulnerabilities and install the corresponding patches, the risk remains that a system failure similar to the January 2, 2017 outage could occur again.

Inadequate TECS Status Monitoring

CBP did not adequately monitor TECS processing to recognize that system performance was degrading to the point that an outage would occur. According to DHS 4300A Handbook, version 12.0:

> *Appropriate operational and security staff will constantly monitor for trigger events. Triggers can be either routine or non-routine. Routine triggers are events that are normal or scheduled occurrences. They are planned and are known to the operations and security personnel. Non- routine triggers are events that are out-of-cycle, anomalies, of unknown origin or activity. They are detected through Continuous Monitoring mechanisms (e.g., Intrusion Detection/Prevention Systems and Firewalls).*

CBP's monitoring of TECS did not yield timely notification of the magnitude of the outage on January 2, 2017.[1] First, the applications being used to monitor TECS did not show that an outage was going to occur. CBP's Technology Operations Center (TOC) at [redacted] provides 24x7 monitoring pertaining to mission support applications, systems infrastructure, and infrastructure support applications. At 4:15 p.m. EST, January 2, 2017, the primary automated monitoring applications used by the TOC staff observed a sporadic TECS slowdown. TOC staff then started using other applications to determine the problem. Twenty-five minutes later, at 4:40 p.m. EST, the TOC applications showed that TECS had returned to a healthy state. However, 23 minutes later, at 5:03 p.m. EST, TOC staff observed that TECS required immediate attention as it had degraded to a system outage. The erratic indicators of system performance did not provide the alerts needed for timely CBP corrective action.

Since the January 2, 2017 outage, the TOC has strengthened procedures for monitoring critical applications. TOC is also in the process of implementing a new automated monitoring tool that the center expects will provide more timely information.

[1] Although it is outside the scope of our audit, we are also concerned that the processes that CBP has implemented to monitor the responsiveness of TECS are focused on the data center or the IT systems, not passengers.

Second, the office space used by CBP staff to monitor applications was inadequate to support full oversight of all the mission-critical systems that were being monitored. The TOC was temporarily operating out of a smaller room while the primary TOC room was being expanded. This temporary room provided limited desktop screen space for individual TOC staff to monitor the various critical CBP IT systems, including TECS. The room size also precluded adding multiple large wall-mounted screens for adequate monitoring. In January 2017, CBP was in the process of building a larger, expanded TOC to provide additional screen space to monitor its mission-critical applications.

Third, the criteria for TECS performance alerts were inadequate to ensure effective monitoring. The primary monitoring applications that the TOC relied on for indications of TECS responsiveness included alerts based on business criteria provided by the TECS application owner. TECS application owners had not yet provided the TOC with updated business criteria that might have yielded quicker indications of failing TECS health.

Until CBP updates TECS monitoring applications and facilities, and also updates business criteria for monitoring TECS performance, the TOC may be unable to provide timely information to prevent a TECS slowdown from becoming an outage in the future. Until these issues are addressed, the risk remains that a system failure similar to the January 2, 2017 outage will occur again.

Inadequate Business Continuity and Disaster Recovery Capabilities

CBP's business continuity processes and disaster recovery capabilities need improvement. A delayed decision to implement TECS failover to the legacy environment extended the January 2, 2017 outage to 4 hours nationwide. If not corrected, several disaster recovery deficiencies could result in even more extensive system outages in the future.

Delayed Implementation of TECS Immediate Failover Capability

CBP delayed implementation of a TECS immediate failover capability, extending the outage longer than necessary.

According to CBP's most recent Business Impact Analysis (BIA), October 2004:[2]

- some TECS subsystems are critical to the performance of the CBP mission and [redacted], and
- CBP business functions that control the movement of people, carriers, cargo, and mail across the borders of the United States are examples of uninterruptible functions.

In accordance with this BIA, CBP had established a failover capability in case of TECS Modernization failure. However, CBP did not immediately implement this failover capability as required when the TECS Modernization environment was no longer responsive on January 2, 2017, at 5:03 p.m. EST. It was not until 8:22 p.m. EST, more than 3 hours later, that CBP's Assistant Commissioner ordered implementation of the failover capability. According to CBP staff, the failover capability was not implemented immediately because the initial indicators only showed slow or degraded response times and CBP staff expected that restarting the servers would correct the problem. Delayed implementation of the failover capability extended the impact of this outage on the traveling public for 4 hours.

Inadequate Disaster Recovery Capability

As of February 2017, TECS's disaster recovery capabilities remained unable to meet CBP's requirements. According to CBP's October 2004 BIA, some TECS subsystems are critical to the performance of the CBP mission and must always be available without any downtime. Nonetheless, the identified alternate processing sites for both TECS Modernization and TECS Legacy did not have all the required resources to function as disaster recovery facilities. Lacking this, there is an increased risk that a future TECS systems outage could be much longer than the 4-hour outage experienced on January 2, 2017.

[2] Although the BIA was developed prior to TECS Modernization, TECS business requirements remain the same.

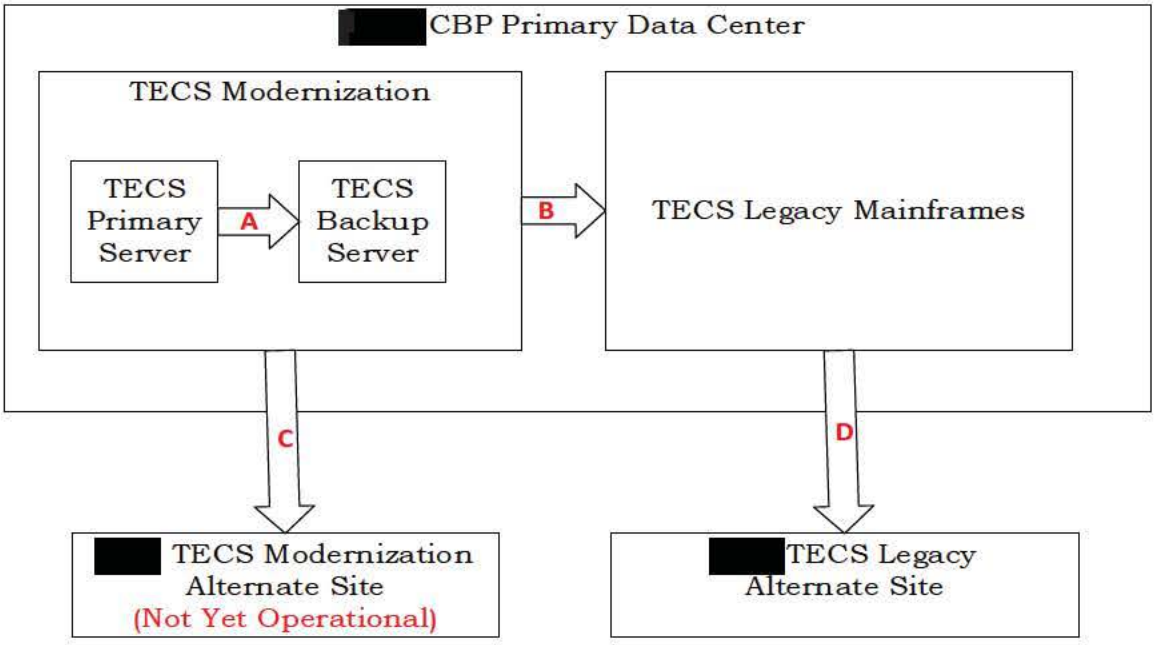
CBP's Primary and Alternate Processing Sites

CBP's TECS disaster recovery capabilities involved three data centers:

- [redacted], which is the primary operating site for both TECS Modernization (servers) and TECS Legacy (mainframes);
- [redacted], which is the TECS Legacy alternate processing site and
- [redacted], which is the TECS Modernization planned alternate site.

Figure 3 illustrates the relationships among these three locations and how processing capability could be shifted to avoid disruption in the event of an outage.

Figure 3: TECS Primary and Alternate Data Centers



Source: OIG based on CBP-provided information

As illustrated in the figure at arrow **B**, the January 2, 2017 outage was resolved by moving from the TECS Modernization environment to TECS Legacy mainframes, but not without significant delay.

TECS Modernization Servers at [redacted] Lack Immediate Failover Capability

TECS servers at [redacted] lacked immediate failover capability. If the primary TECS server were to fail, CBP would rely on a backup TECS server, also at [redacted]. See figure 3, arrow **A**. According to the October 2004 BIA, TECS should be immediately available with no downtime in the transition from primary to backup servers. However, per CBP staff, a delay of 15 to 60 minutes can be anticipated before the backup server comes online, depending on the error. Any such delay can have a detrimental effect on business operations.

TECS Mainframe Does Not Have an [redacted]

TECS mainframes at [redacted] also lacked immediate failover capability. CBP officials said that if both the TECS primary and secondary servers at [redacted] stop processing, they should immediately failover to the TECS Legacy environment. See figure 3, arrow **B**.

However, the TECS Modernization servers and TECS Legacy mainframes are both housed at [redacted]. If [redacted] becomes unavailable for TECS processing, TECS must failover to the TECS Mainframe environment at the [redacted] alternate site, but [redacted] lacks the mainframes necessary to restart TECS operations.[3] See figure 3, arrow **D**. According to CBP staff, following an NDC outage, it could take 3 – 4 weeks to obtain and implement mainframes at [redacted] so that TECS Legacy could become operational. This is because CBP did not renew the licenses for mainframes at [redacted]. Meanwhile, CBP's mission-critical functions, including passenger processing, would be severely impacted.

A similar lack of an adequate disaster recovery capability was previously reported in *DHS Needs to Strengthen Information Technology Continuity and Contingency Planning Capabilities* (OIG-13-110), August 2013. However, the Department non-concurred with our recommendation, which advised the DHS

[3] Although outside our scope, in addition to TECS, there are other mission-critical CBP systems that still operate in the Legacy mainframe environment at [redacted].

Chief Information Officer to coordinate with CBP and "perform full failover contingency testing for enterprise mission essential systems." In March 2017, John Roth, DHS Inspector General, requested that the DHS Acting Under Secretary for Management assist in resolving this issue. In June 2017, we were informed that the Department was preparing a response to John Roth's March 2017 memo.

Alternate TECS Modernization Site Is Not Yet Operational

TECS Modernization lacked an alternate processing site. Although TECS should be immediately available with no downtime, the TECS Modernization [redacted] alternate site is not fully developed and it is not equivalent to the [redacted] production environment. See figure 3, arrow **C**.

According to CBP staff, CBP was installing the necessary hardware and software resources so that [redacted] could become an alternate processing site for TECS Modernization. As of February 2017, CBP was in the process of completing the [redacted] TECS Modernization configuration (e.g., firewalls, telecommunications). However, the TECS Modernization failover capability from [redacted] to [redacted] had not yet been tested to ensure operational effectiveness.

Conclusion

CBP was responsive in addressing the outage of January 2, 2017 — the symptom of a problem. Nonetheless, much work is still needed to address root causes of the problem itself. Specifically, CBP needs to improve its software testing environment, identify and implement critical operating system patches in a timely fashion, and update the criteria used for TECS performance monitoring. Additionally, CBP lacked adequate business continuity processes and an effective TECS disaster recovery capability. Completing the transition to the TECS Modernization environment and enabling [redacted] as a fully functional backup site are critical ingredients for recovering operations in case of disruption.

CBP has some actions underway to address these deficiencies. Until they are complete, however, CBP lacks the means to minimize the possibility and impact of similar system outages in the future. Additionally, there is an

increased risk that a TECS systems outage could be much longer than 4 hours. The problems experienced in processing passengers on January 2, 2017, would only be compounded by increased duration of any future outage.

Recommendations

We recommend that the Assistant Commissioner for the Office of Information and Technology:

Recommendation 1: Ensure that the TECS test environment is sufficiently similar to the TECS production environment so that testing scenarios will be able to identify errors caused by processing a large volume of queries.

Recommendation 2: Ensure that OIT staff receive timely notifications of critical vulnerabilities to CBP operating systems.

Recommendation 3: Adjust the TOC alert criteria for TECS to ensure earlier notifications of slowdowns and outages.

Recommendation 4: Establish policy to implement TECS recovery operations within 1 hour of an outage.

Recommendation 5: Provide the DHS Chief Information Officer with a weekly status of CBP's planned and actual modernization migration schedule and milestones detailing when (a) the Legacy mainframe environment is no longer needed, and (b) the recovery site is fully functional.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Senior Component Accountable Official. We have included a copy of the comments in their entirety at appendix B. CBP concurred with recommendations 1, 3, 4, and 5 and has already started addressing the reported deficiencies. As such, recommendations 1, 3, 4, and 5 are considered resolved, but open, pending verification of all planned actions. CBP non-concurred with recommendation 2, that OIT staff receive timely notifications of critical vulnerabilities. Recommendation 2 is considered open and unresolved.

Agency Comments to Recommendation 1:

CBP concurs with this recommendation. CBP acknowledges that having a production-like environment is a benefit to the overall health of any application system. The inclusion of a production-like testing environment will be part of the requirements as CBP moves to a cloud environment but will be contingent upon necessary funding. CBP has established interim milestones:

- September 30, 2017: Complete TECS system assessments for the current architecture.
- December 21, 2017: Finalize infrastructure requirements and include a test environment for migrating TECS systems to the cloud.
- December 31, 2017: Finalize estimated cost and request funding.
- March 31, 2018: Complete the schedule for TECS system deployments to the cloud environment.
- September 30, 2019: Complete deployments of TECS systems to the cloud environment.

The overall estimated completion date is September 30, 2019.

OIG Analysis of Agency Comments to Recommendation 1:

CBP's plans satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until CBP provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 2:

CBP non-concurred with this recommendation. According to CBP,

- Inadequate software maintenance was not a contributing factor or underlying cause of the outage.
- CBP maintains a mature information systems vulnerability management program and was in full compliance with DHS 4300A, Attachment O, "Vulnerability Management Program."

- Information Security Vulnerability Management bulletins are briefed daily to CBP leadership and are already distributed widely to all CBP Information Systems Security Officers and CBP system administrators as applicable.
- The vulnerability referenced by the OIG was not rated by the operating system vendor as "critical." It dealt with operating system error handling, not error handling which could have contributed to the application outage.
- At the time of the outage, CBP was well within established DHS vulnerability management policy windows for testing and deploying new patches which are not deemed to be critical.

OIG Analysis of Agency Comments to Recommendation 2:

This recommendation is designed to address a lack of communication with the software testing staff. Specifically, neither the CBP information systems security staff nor the vendor's onsite staff provided software testing staff with information concerning this critical vulnerability and its associated patch.

CBP has not provided the steps to increase communications of vulnerabilities with the software testing staff. This recommendation is considered unresolved and will remain open until CBP provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 3:

CBP concurs with this recommendation. According to CBP, detailed monitoring was in place to provide timely notification of system issues so technical teams could begin addressing the issues. Additionally, CBP has updated its protocols to clearly establish a very quick escalation to OIT leadership when the TECS Primary applications have issues. CBP's OIT has also enhanced communications with field offices to ensure full understanding of the end user impact of the issue, and increase its use of social media monitoring for alerts on traveler wait times. Since this incident, additional monitoring tools have been put in place and the knowledge level of how to interpret them has improved. The overall estimated completion date is October 31, 2017.

OIG Analysis of Agency Comments to Recommendation 3:

CBP's plans satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until CBP provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 4:

CBP concurs with this recommendation. CBP plans to develop and implement procedures to limit the time spent troubleshooting alternative recovery paths. With input from the Office of Field Operations, the business owner, CBP established the minimum functionality required to support primary processing in the event of an outage and plans to have all required systems available to run in the alternate data center by December 31, 2017. CBP OIT will collaborate with the Office of Field Operations and other stakeholders to develop procedures on when to implement TECS operations at the alternate site depending upon the nature of an outage to ensure that TECS recovery operations are completed within an hour. The overall estimated completion date is December 31, 2017.

OIG Analysis of Agency Comments to Recommendation 4:

CBP's plans satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until CBP provides supporting documentation that all corrective actions are completed.

Agency Comments to Recommendation 5:

CBP concurs with this recommendation. According to CBP, progress is annotated monthly in the DHS Chief Information Officer's INVEST tool and a summary of the progress will be emailed to this official every month. CBP's OIT leadership has confirmed that the monthly report is adequate.

According to CBP, the TECS team has worked to install the necessary hardware and software resources so that the recovery site can become an alternate processing site for TECS Modernization during the second and third quarter of fiscal year (FY) 2017. The team successfully performed a failover test

to the recovery site for the Traveler Primary Application Client in June 2017, and is working on the remaining required systems. The team anticipates completing this effort in the fourth quarter of FY 2017. The DHS Chief Information Officer was informed of the successful failover test in the June TECS Modernization Executive Steering Committee meeting. The overall estimated completion date is October 31, 2017.

OIG Analysis of Agency Comments to Recommendation 5:

CBP's plans satisfy the intent of this recommendation. This recommendation is considered resolved but will remain open until CBP provides supporting documentation that all corrective actions are completed.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security (DHS) Office of Inspector General (OIG) 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 cause of CBP's information system outage on January 2, 2017, whether CBP effectively and efficiently ended the information system outage, and whether the steps CBP plans to take will minimize the possibility and impact of a similar information system outage in the future.

As part of our review, we interviewed CBP staff and contractors at [redacted] and in Herndon, VA, to determine how the system outage was identified and fixed.[4] In addition, we reviewed January 2, 2017 information system outage timelines to understand the series of events that led to the outage as well as identify the steps CBP took to mitigate the outage.

We also reviewed technical vulnerability assessments of the TECS servers in the Modernization environment and TECS system security documentation to identify critical vulnerabilities. In addition, we reviewed the latest available TECS BIA to determine the impact of an outage on CBP's mission.

We conducted this audit between January and March 2017 pursuant to the Inspector General Act of 1978, as amended, and according to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency.

[4] A separate OIG IT Audit's team reviewed CBP's actions during the audit at Miami International Airport. Their findings will be included in a separate report.

We appreciate the efforts of CBP management and staff to provide the information and access necessary to accomplish this review. Major OIG contributors to the audit are identified in appendix D.

Appendix B
CBP Comments to the Draft Report

1300 Pennsylvania Avenue NW
Washington, DC 20229

U.S. Customs and Border Protection

SEP 30 2017

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

FROM: Sean M. Mildrew
Senior Component Accountable Official
U.S. Customs and Border Protection

SUBJECT: Management's Response to OIG Draft Report:
Review of CBP Information Technology System Outage of
January 2, 2017 (Project No. 17-044-ITA-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 takes restoration of service for systems very seriously and will leverage your report to help us continue to improve our troubleshooting procedures. The outage on January 2, 2017, was noticed quickly through our monitoring alerts and troubleshooting began immediately. While some intermittent remediation was accomplished through the troubleshooting, the restoration of services was lengthy and the incorporation of the OIG's recommendations will help us shorten future outages, where possible.

CBP has already begun implementation of some of the OIG's recommendations. The Office of Information and Technology (OIT) updated protocols to clearly establish a very quick escalation to OIT leadership when the TECS Primary applications have issues. We also enhanced communication with field sites to ensure we fully understand the end user impact of the issue and increased our use of social media monitoring for alerts on traveler wait times. In addition, we are limiting the time spent troubleshooting when there is an alternative recovery path.

As CBP moves to a cloud computing environment, improved performance and load testing to emulate a production environment will be included in the requirements, allowing for better evaluation of code and infrastructure changes prior to deployment.

The draft report contained 5 recommendations. CBP concurs with Recommendations 1, 3, 4 and 5, and non-concurs with Recommendation 2. Please see the attached for our detailed response to each of the recommendations.

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

Attachment

Attachment: CBP Management's Response to Recommendations Contained in 17-044-ITA-CBP

The OIG recommended that the Assistant Commissioner, Office of Information and Technology:

Recommendation 1: Ensure that the TECS test environment is sufficiently similar to the TECS production environment so that testing scenarios will be able to identify errors caused by processing a large volume of queries.

Response: Concur. While having a test environment sufficiently similar to the TECS production environment would likely not have prevented the events of January 2, 2017, CBP acknowledges that having a production-like environment is of benefit to the overall health of any application system. The inclusion of a production-like testing environment will be part of the requirements as CBP moves to a cloud environment and will depend on the necessary funding to establish a production-like test environment. Estimated interim milestones:

- November 15, 2017: Complete TECS system assessments for the current architecture.
- December 21, 2017: Finalize infrastructure requirements for cloud environment for TECS systems to include test environment.
- December 31, 2017: Finalize estimated cost and request for funding.
- March 31, 2018: Complete schedule for TECS system deployments to cloud environment.
- September 30, 2019: Complete deployments for TECS systems to cloud environment.

The overall Estimated Completion Date (ECD) is September 30, 2019.

Recommendation 2: Ensure that OIT staff receive timely notifications of critical vulnerabilities to CBP operating systems.

Response: Non-concur. Inadequate software maintenance was not a contributing factor or underlying cause of the outage. CBP maintains a mature information systems vulnerability management program. At the time of the outage CBP was in full compliance with DHS 4300A, Attachment O, "Vulnerability Management Program."

Information Security Vulnerability Management (ISVM) bulletins are briefed daily to CBP leadership and are already distributed widely to all CBP Information Systems Security Officers and CBP system administrators as applicable.

The vulnerability referenced by OIG was not rated by the operating system vendor as "critical" and it dealt with operating system error handling, not error handling which could have contributed to the application outage. Furthermore, at the time of the outage, CBP was well within established DHS vulnerability management policy windows for testing and deploying new patches which are not deemed to be critical.

CBP will continue to follow established DHS guidelines and requirements for distributing vulnerability notifications and will continue to remediate vulnerabilities within the established timeframes or unless exposures dictate accelerated action.

We request that OIG consider this recommendation resolved and closed.

Recommendation 3: Adjust the TOC alert criteria for TECS to ensure earlier notifications of slowdowns and outages.

Response: Concur. Detailed monitoring was in place that did provide timely notification of system issues so technical teams could begin working the issues. In addition, protocols have been updated to clearly establish a very quick escalation to the OIT leadership when the TECS Primary applications have issues. OIT has also enhanced communications with field offices to ensure we fully understand the end user impact of the issue and increased our use of social media monitoring for alerts on traveler wait times. Since this incident, additional monitoring tools have been put in place and the knowledge level of how to interpret them has improved.

ECD: October 31, 2017.

Recommendation 4: Establish policy to implement TECS recovery operations within one hour of an outage.

Response: Concur. CBP will develop and implement procedures to limit the time we spend troubleshooting alternative recovery paths. With input from the Office of Field Operations (OFO), the business owner, CBP established the minimum functionality required to support primary processing in the event of an outage and plans to have all required systems available to run in the alternate data center by December 31, 2017. CBP OIT will collaborate with OFO and other stakeholders to develop procedures outlining when to implement TECS operations at the alternate site depending on the nature of the outage to ensure that TECS recovery operations are completed within one-hour.

ECD: December 31, 2017.

Recommendation 5: Provide the DHS Chief Information Officer with a weekly status of CBP's planned and actual modernization migration schedule and milestones detailing when (a) the Legacy mainframe environment is no longer needed, and (b) the recovery site is fully functional.

Response: Concur. Progress is annotated monthly in the DHS Chief Information Officer (CIO)'s INVEST tool and a summary of the progress will be emailed to the DHS CIO every month. OIT leadership has confirmed with the DHS/CIO that the monthly report is adequate.

Since the initial draft report was released, the TECS team has worked to install the necessary hardware and software resources so that the recovery site could become an alternate processing

site for TECS Modernization during the second and third quarter of fiscal year (FY) 2017. The team successfully performed a failover test to the recovery site for the Traveler Primary Application Client (TPAC) in June 2017 and is working on the remaining required systems and anticipate completion in the fourth quarter of FY 2017. The DHS CIO was informed of the successful TPAC failover test in the June TECS Modernization Executive Steering Committee (ESC) meeting.

ECD: October 31, 2017.

Appendix C
January 2, 2017 Information System Outage Timeline

Time (EST)	Event
4:15 p.m.	CBP OIT staff received the first automated alerts about sporadic slow responses in two TECS modules. CBP's TOC staff and Duty Officers began investigating the slow response issue.
4:16 p.m.	MIA started having issues with a TECS module used to process arriving passengers.
4:30 p.m.	MIA called CBP's Technology Service Desk (TSD) to report the problem. TSD staff told MIA that this is a nationwide issue and there is no resolution timetable.
4:34 p.m.	TSD reported that they had received calls about the TECS outage.
4:35 p.m.	The MIA Watch Commander was notified of the passenger processing issue.
4:40 p.m.	MIA Watch Commander ordered CBP staff at MIA to start passenger processing mitigation activities.
4:40 p.m.	Automated monitoring systems no longer showed TECS slowdown alerts.
5:03 p.m.	TECS was no longer responsive.
5:10 p.m.	Automated monitoring systems alerts for TECS began again. TOC staff contacted OIT Passenger Systems Program Directorate (PSPD), OIT Enterprise Data Management and Engineering (EDME), Web Services Operations, and local area network (LAN) support staff concerning the TECS outage.
5:26 p.m.	TOC staff contacted PSPD Operations & Maintenance Team concerning the TECS outage.
5:27 p.m.	CBP Duty Officers sent out a Situational Awareness alert concerning the TECS outage.
5:47 p.m.	Due to the TECS outage, some Florida airports started using the TECS backup system called the Portable Automated Lookout System.

Time (EST)	Event
5:47 p.m.	CBP Duty Officers established a bridge call to address the nationwide TECS outage.
6:00 p.m.	TOC notified EDME Database Administration to check TECS application servers due to alerts of high control processor unit (CPU) usage.
6:05 p.m.	EDME Database Administration joined the bridge call.
6:09 p.m.	Duty Officers sent out a Commissioner's Situational Advisory.
6:19 p.m.	PSPD Manifest team joined the bridge call. PSPD asked the TOC to use a new automated monitoring tool. TOC reported that the current onsite staff did not have sufficient knowledge to use the new tool and requested additional assistance of the PSPD application group to use the new automated monitoring tool.
6:23 p.m.	Duty Officers sent an Airline Secure Flight notification to the Transportation Security Administration.
6:24 p.m.	TSD and the government lead for Automated Passport Control joined the bridge call.
6:32 p.m.	CBP Duty Officers requested other EDME groups to join the bridge call.
6:35 p.m.	Two TECS Modernization servers were restarted.
6:36 p.m.	CBP performed a restart of three TECS servers.
6:40 p.m.	PSPD Government Leads requested their team to continue to check TECS status using the new automated monitoring tool.
6:46 p.m.	Using the new monitoring tool, PSPD discovered a 'House Rules Violation,' validating that there was slow response time for TECS. The PSPD Operating System Primary was unavailable to participate in the bridge call. Two TECS servers were recycled, but one was showing slow response times.
6:49 p.m.	CBP checked the connection between the three TECS servers.

Time (EST)	Event
6:51 p.m.	EDME LAN was not seeing any obvious issues with TECS. Specifically, they were not seeing that TECS queries were running for too long.
6:54 p.m.	PSPD Manifest team joined the bridge call.
6:58 p.m.	EDME Operating System joined the bridge call. The PSPD Operating System Secondary was 45 minutes away.
7:04 p.m.	The Commissioner's Situation Room staff called the Duty Officers to report that MIA called them directly as they are manually processing arriving passengers.
7:53 p.m.	CBP's EDME Executive Director joined the bridge call.
7:57 p.m.	PSPD Primary Inspection Process representative joined the bridge call.
8:02 p.m.	A TECS server was rebooted.
8:19 p.m.	A TECS server was rebooted.
8:22 p.m.	The Assistant Commissioner for OIT was conferenced into the bridge call and directed CBP staff to implement TECS Modernization to failover to the TECS Legacy mainframe environment.
8:40 p.m.	MIA confirmed they were operational. Newark Liberty International Airport reported that they could process four or five passengers then it goes into time out again.
8:47 p.m.	TECS queries were switched back to the TECS Legacy mainframe environment.
9:20 p.m.	Los Angeles International Airport was operational since 8:55 p.m. EST. John F. Kennedy International Airport (JFK) was partially down, processing slowly.
10:06 p.m.	All airports, except JFK, confirmed that they were back online.
10:15 p.m.	All Passenger applications were in Mitigation Mode restoring service. JFK confirmed they were 100 percent operational.

Source: OIG-compiled based on data provided by CBP

Appendix D
Office of IT Audits Major Contributors to This Report

Kevin Burke, Supervisory IT Auditor
Charles Twitty, Senior IT Auditor
Sonya Davis, IT Auditor
Scott Wrightson, Referencer

Appendix E
Report Distribution

Department of Homeland Security

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