OFFICE OF INSPECTOR GENERAL

# CBP's Configuration Management Practices Did Not Effectively Prevent System Outage

Homeland Security

**December 21, 2020**

**OIG-21-13**

**OFFICE OF INSPECTOR GENERAL**
Department of Homeland Security

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

December 21, 2020

MEMORANDUM FOR: Mark A. Morgan
Senior Official Performing Duties of the Commissioner
U.S. Customs and Border Protection

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2020.12.18 12:41:59 -05'00'

SUBJECT: *CBP's Configuration Management Practices Did Not Effectively Prevent System Outage*

Attached for your action is our final report, *CBP's Configuration Management Practices Did Not Effectively Prevent System Outage*. We incorporated the formal comments from CBP in the final report.

This report contains five recommendations aimed at improving the training, procedures, processes, and employee awareness for CBP's outage mitigation applications. CBP concurred with all five recommendations. Based on the information provided, we consider each recommendation 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 review the recommendations for closure. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

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

Please call me with any questions, or your staff may contact Sondra McCauley, Assistant Inspector General for Audits, at (202) 981-6000.

Attachment

cc: Sanjeev "Sonny" Bhagowalia, Acting Assistant Commissioner for OIT

# DHS OIG Highlights

## *CBP's Configuration Management Practices Did Not Effectively Prevent System Outage*

**December 21, 2020**

## Why We Did This Review

U.S. Customs and Border Protection's (CBP) officers rely on information technology systems to screen arriving international passengers and prevent terrorists and known criminals from entering the country. On August 16, 2019, a CBP system outage disrupted processing of incoming international travelers at airports nationwide for as long as 2.5 hours, similar to a January 2, 2017 outage on which we previously reported. We conducted this review to determine why CBP's actions to implement previous OIG recommendations did not prevent the onset and length of the August 16, 2019 nationwide outage.

## What We Recommend

We recommend CBP improve training, procedures, processes, and employee awareness to mitigate the risks posed by any future system outages.

**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

While CBP's actions to implement prior Office of Inspector General (OIG) outage-related recommendations could not have prevented the onset of the nationwide outage on August 16, 2019, the steps taken did help minimize the length and severity of disruptions to passenger screening. Specifically, by addressing OIG recommendations, CBP established a more effective control structure for monitoring passenger screening systems, enabling prompt action to identify and resolve the outage.

However, CBP's configuration management policies and procedures were not sufficient to prevent the 2019 outage. We determined CBP's critical passenger applications were operating on an Oracle database device that was not properly configured and did not have up-to-date patches. This lapse occurred because the Oracle patch did not execute properly and CBP did not ensure its configuration management policies and procedures were followed and patches were applied promptly. The outage resulted in longer wait times, delays for arriving passengers, and the need for CBP to revert to less effective backup systems to support passenger screening procedures.

CBP personnel faced additional challenges during the outage, as they were unable to quickly access "offline" backup systems and were not fully prepared for backup procedures. This was due to inadequate training and ineffective communication from CBP Headquarters during the outage. CBP should address these deficiencies which, in the event of future system outages, may again risk the entry of unauthorized individuals who could threaten our Nation's security.

## CBP Response

CBP concurred with all five recommendations.

## Table of Contents



## Appendixes



## Abbreviations

| | |
|---|---|
| CBP | U.S. Customs and Border Protection |
| C.F.R. | Code of Federal Regulations |
| ISVM | Information Security Vulnerability Management |
| IT | information technology |
| NUMA | Non Uniform Memory Architecture |
| OFO | Office of Field Operations |
| OIT | Office of Information and Technology |
| PALS | Portable Automated Lookout System |
| TPAC | Traveler Primary Arrival Client |
| U.S.C. | United States Code |

## Background

U.S. Customs and Border Protection (CBP) is the front-line border protection component in the Department of Homeland Security, responsible for securing the Nation's borders and facilitating lawful international travel and trade. CBP plays a crucial role in enforcing laws and regulations related to immigration and border security, intercepting malicious criminals and materials, and maintaining domain awareness to prevent terrorist attacks. CBP is one of the world's largest law enforcement organizations, with more than 60,000 officers, agents, and support personnel nationwide. On a typical day in 2019, CBP welcomed more than 1.1 million visitors, screened more than 78,000 cargo containers, apprehended more than 2,300 individuals, and seized more than 3,700 pounds of narcotic drugs.

CBP's primary immigration enforcement mission at its 328 land, sea, and air ports of entry is to confirm eligible travelers and exclude inadmissible foreign nationals from entering the United States. Timely screening and processing of arriving international passengers is vital to prevent terrorists and known criminals from entering the United States. CBP officers assigned to the Office of Field Operations (OFO) rely on information technology (IT) systems to expedite high-volume screening operations at airports each day. For example, TECS[1] is the principal system used by CBP officers at ports of entry to assist with passenger screening and admissibility determinations upon arrival. Additional inspection and screening applications reside on the TECS platform, including the Traveler Primary Arrival Client (TPAC). This is the primary passenger screening module used to process, document, and confirm the identity of international travelers at air and sea ports of entry.

Outages in any one of CBP's systems can have a detrimental impact on its ability to screen arriving international passengers. The CBP Assistant Commissioner in the Office of Information and Technology (OIT) provides infrastructure, technology, and communications to carry out border security operations at ports of entry and related locations. It is critical that CBP's OIT maintain adequate IT systems and infrastructure to support CBP's day-to-day, front-line border security operations.

### Passenger Screening Process at Airports

Upon arrival, all international air travelers and baggage entering the United States must undergo inspection by a CBP officer to ensure admissibility in

[1] TECS (not an acronym) provides traveler processing and screening, investigations, case management, and intelligence functions for multiple Federal, state, and local agencies.

accordance with Federal statutes and regulations.[2] For example, CBP officers must determine the nationality of each in-bound traveler and, if a foreign national, whether the individual meets the requirements for admission to the United States.[3] CBP officers use a two-step inspection procedure to screen each traveler upon arrival at international airports around the country. Table 1 outlines the two phases of the CBP passenger screening process at international airports.

**Table 1. CBP OFO Passenger Screening Process**

| Inspection Phase | Passenger Screening Process |
|---|---|
| **Primary** | Upon arrival, each international traveler must clear passport control, also referred to as primary inspection. A foreign national entering the United States is required to present a passport and valid visa issued by a U.S. Consular Official, unless the individual is a citizen of a country eligible for the Visa Waiver Program, a lawful permanent resident of the United States (possessing a Green Card), or a citizen of Canada. CBP officers inspect these and other travel documents before the traveler is admitted into the United States. If the CBP officer determines additional screening is needed, the traveler will be referred to secondary inspection. |
| **Secondary** | During secondary inspection, a CBP officer may run law enforcement queries to screen the traveler for admissibility issues. On average, 5% of travelers are referred to secondary inspection. If the officer determines there are no admissibility issues, the traveler is permitted to enter the country. |

*Source:* OIG-17-114, Table 2: CBP OFO Passenger Screening Process,[4] page 8

[2] According to Title 19, Code of Federal Regulations (C.F.R.), Section 162.6, "All persons, baggage and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection by a CBP officer."
[3] *The Immigration and Nationality Act*, as amended, sets forth Federal immigration and naturalization requirements, e.g., 8 United States Code (U.S.C.) § 1101 et seq.
[4] *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations*, OIG-17-114, September 28, 2017.

**Prior Oversight on CBP Systems Outages**

We previously reported on CBP's efforts to maintain adequate IT systems and infrastructure to fully support front-line border security operations. Two OIG engagements in 2017 focused on system outages that caused significant disruptions to CBP's processing of incoming international travelers at airports nationwide. Specifically:

- We conducted an audit to assess the effectiveness of CBP's IT systems supporting its border security objective to prevent entry of inadmissible aliens who may pose threats to national security. We determined that CBP's IT systems and infrastructure did not fully support this border security objective. Specifically, TECS performance was slow and greatly reduced CBP's identification of passengers who might be security threats. In addition, we found that frequent system outages hampered incoming passenger screening at U.S. international airports and created passenger delays and public safety risks. We made seven recommendations to address passenger screening and border security IT systems and infrastructure challenges, listed in Appendix C. Since publication of our September 2017 report, CBP has implemented corrective actions and closed all but one recommendation.

- We conducted a review of a January 2, 2017 4-hour system outage that disrupted the processing of incoming international travelers at airports nationwide.[5] Specifically, we conducted this review to determine the effectiveness of CBP's efforts to address the system outage, as well as the sufficiency of its plans to minimize the possibility and impact of future system outages. We determined CBP took adequate steps to resolve the outage on the day it occurred, but found remaining underlying issues that could cause future outages. For example, we disclosed inadequate CBP software capacity testing, deficient software maintenance, ineffective system status monitoring, and inadequate recovery capabilities to minimize the impact of system failures on the traveling public contributed to the outage. We made five recommendations, listed in Appendix C, to address CBP's software testing, vulnerability patching, and disaster recovery challenges. Since publication of our November 2017 report, CBP has implemented and closed all five recommendations.

[5] *Review of CBP Information Technology System Outage of January 2, 2017 (Redacted)*, OIG-18-19 (revised), November 21, 2017.

CBP actions to implement the 12 recommendations from these two reports were expected to help CBP prevent, limit the severity of, and improve its response to any potential future system outage.

**August 16, 2019 Nationwide Outage**

Despite our previous oversight reports, on August 16, 2019, CBP experienced another system outage that delayed CBP's processing of incoming international travelers at airports nationwide. The outage caused CBP passenger processing delays as long as 2.5 hours at several airports nationwide, including cities such as Miami, New York, Los Angeles, San Francisco, Philadelphia, Chicago, Newark, Dallas, and Seattle. According to CBP, the systems were running again by early evening on the East Coast, and there was "no indication of any nefarious activity" during the outage. CBP officers were also still able to access security-related databases, though not easily, and maintain security standards while screening people manually.

We conducted this review to determine why CBP's actions to implement previous OIG recommendations did not prevent the onset and length of the August 16, 2019 nationwide outage.

## Results of Review

While CBP's actions to implement prior OIG outage-related recommendations could not have prevented the onset of the nationwide outage on August 16, 2019, the steps taken did help minimize the length and severity of disruptions to passenger screening. Specifically, by addressing OIG recommendations, CBP established a more effective control structure for monitoring passenger screening systems, enabling prompt action to identify and resolve the outage.

However, CBP's configuration management policies and procedures were not sufficient to prevent the 2019 outage. We determined CBP's critical passenger applications were operating on an Oracle database device that was not properly configured and did not have up-to-date patches. This lapse occurred because the Oracle patch did not execute properly and CBP did not take steps to ensure its configuration management policies and procedures were followed and patches were applied promptly. The outage resulted in longer wait times, delays for arriving passengers, and the need for CBP to revert to less effective backup systems to support passenger screening procedures.

CBP personnel faced additional challenges during the outage, as they were unable to quickly access "offline" backup systems and were not fully prepared for backup procedures. This was due to inadequate training and ineffective

communication from CBP Headquarters during the outage. CBP should address these deficiencies which, in the event of future system outages, may again risk the entry of unauthorized individuals who could threaten our Nation's security.

## CBP's Response to Prior OIG Recommendations Helped Lessen the Impact of the Outage

CBP's actions in response to the 12 recommendations in our two prior reports helped limit the severity of the August 16, 2019 system outage. We concluded that four recommendations, listed in Table 2, were relevant to the 2019 outage. To address these four recommendations, CBP took a number of steps between 2017 and 2019 to improve system availability, establish performance measures, adjust alert criteria, and implement a policy for recovery operations. Collectively, these actions helped CBP establish a more effective control structure for monitoring passenger screening applications.

**Table 2. Prior OIG Recommendations and CBP's Corrective Actions**

| OIG Report Recommendation | CBP Corrective Actions |
|---|---|
| **OIG-17-114, Recommendation 2:** Develop a plan to address maintenance, infrastructure, dependencies on external systems, and other factors that contributed to challenges regarding availability of primary traveler screening applications. | **Improved system availability:** CBP finalized its Availability Improvement Plan in January 2018, which ensures primary traveler system availability. The plan includes infrastructure upgrades, system patching, maintenance release strategies, and options for external partner dependencies to improve the availability of their services. CBP OIT officials stated that prior to this recommendation, the TECS application required complete shutdown and restart in the event of an outage. Upgrades to the TECS application since then have helped minimize the impact when data services provided by external organizations are interrupted. This helped limit the severity of the August 16, 2019 degradation by ensuring it did not become a full outage. |
| **OIG-17-114, Recommendation 3**: Assess the need for performance measures to monitor, evaluate, and ensure the availability of primary traveler screening applications from the end-user perspective at ports of entry. | **Establish performance measures:** CBP OIT officials implemented a TECS Dashboard to monitor system health and evaluate the availability of primary traveler screening applications so traveler processing can continue with minimal interruption during periods of degraded performance or system outage. According to OIT officials, the monitoring dashboard was set up in an easy-to-view visualization to show the monitored application and system status, and provide early warnings to CBP staff. This has |

| | |
|---|---|
| | enabled CBP personnel to recognize when an application/system is not functioning as expected and respond promptly. |
| **OIG-18-19, Recommendation 3:** Adjust the [Technology Operations Center] alert criteria for TECS to ensure earlier notifications of slowdowns and outages. | **Adjust alert criteria:** According to officials, CBP OIT put a more detailed monitoring approach in place, adding a monitoring feature for the passenger screening applications and adjusting the monitoring alert threshold. These actions now provide timely notification of system issues so technical teams can begin working the issue. In addition, CBP personnel enhanced protocols to establish a quick escalation path to OIT leadership when the TECS primary applications experience issues. OIT staff has incorporated outreach to field sites to ensure they understand the impact of the issues on end users. OIT staff also increased use of social media monitoring for alerts on traveler wait times. Since the August 2019 outage, additional IT incident monitoring tools have been put in place and the knowledge level of how to interpret them has improved. |
| **OIG-18-19, Recommendation 4:** Establish policy to implement TECS recovery operations within 1 hour of an outage. | **Policy for recovery operations:** According to officials, CBP OIT developed and published a failover playbook and mitigation procedures, which are steps to be followed in the event of a system degradation, as required by the recommendation. CBP officials also established the minimum functionality required to support primary processing in the event of an outage and now has the capability to have all required systems available to run in the alternate data center. CBP staff were able to use these mitigation procedures during the system degradation on August 16, 2019. |

*Source:* OIG analysis of CBP's corrective actions

## Actions to Address Recommendations Have Led to an Effective Monitoring Control Structure

The steps CBP took to address our report recommendations resulted in a more effective monitoring control structure for the passenger screening applications on the TPAC system. The capabilities and functionality CBP OIT instituted, as outlined in Table 2, enabled OIT to rapidly detect intermittent timeouts and longer response times in the system on August 16, 2019. To illustrate, at the start of the outage, at 8:16 am (Eastern Daylight Time), the CBP Enterprise Operations Center received alerts of intermittent timeouts causing longer

response times for passenger screening applications on the TPAC system. CBP staff immediately notified appropriate stakeholders to collaborate on identifying and resolving the outage in a timely manner. By 6:51 pm (Eastern Daylight Time) OIT had cleared all errors for the impacted applications.

## CBP's Configuration Management Policies and Procedures Were Not Followed

Despite CBP corrective actions to implement our prior outage-related recommendations, these actions did not prevent the onset of the August 16, 2019 outage. This was because the root cause of the outage was not related to the issues discussed in our prior reports. We determined the outage occurred because CBP (1) did not verify that prior configuration changes had been successfully implemented, and (2) did not detect a corrupted patch on an Oracle database device. In both cases, CBP did not take adequate steps to ensure existing configuration management policies and procedures were followed, or that security updates were applied promptly. The performance disruptions to passenger systems were experienced as a processing outage at airports across the country, resulting in longer wait times for arriving passengers and the need to revert to less effective backup systems to support screening procedures.

### Improper Configuration Settings on an Oracle Device Supporting Passenger Systems Contributed to the Outage

CBP reported the cause of the outage was missing code, allowing a "software bug"[6] that caused memory to be mismanaged, resulting in a service degradation. However, relying on support from Oracle contractors, we determined that an incorrect configuration setting on an Oracle device was the primary cause.

Specifically, an Oracle Exadata device,[7] a primary database for some Passenger Systems Program Directorate applications, was not properly configured at the time of the August 2019 outage. Two years prior, on October 19, 2017, Oracle had published a document concerning a known issue with the Non Uniform Memory Architecture (NUMA)[8] support. The reported issue was that a "bug" could cause systems to experience a sharp increase in workload, and/or

[6] A software bug is an unexpected defect, fault, flaw, or imperfection in system operations.
[7] The Oracle Exadata Database Machine is a computing platform optimized for running the Oracle Database. Oracle Exadata is an intelligent and extremely high speed appliance that connects the database and storage servers.
[8] Oracle NUMA (Non Uniform Memory Architecture) support can be used with large multiprocessor environments like Exadata Database Machines. When enabled, Oracle NUMA support facilitates efficient use of the hardware and may improve database performance.

decrease in database performance. A CBP official said that this issue was addressed between the last quarter of 2017 and first quarter of 2018 on all 18 Exadata devices in the CBP data center[9] except one. We could not confirm the exact timing of the configuration setting update due to a lack of CBP documentation. As of August 16, 2019, CBP's Data Machine (DM31), a primary database for some Passenger Systems Program Directorate applications, did not have the up-to-date configuration setting Oracle had prescribed.

According to *DHS Sensitive Systems Policy Directive 4300A*, system owners should document initial system configuration in detail and control all subsequent changes according to the configuration management process. The directive also recommends that components oversee systems to reduce vulnerabilities through testing and management, promptly installing patches, and eliminating or disabling unnecessary services.[10]

CBP had existing configuration management policies and procedures,[11] in accordance with DHS guidelines, but CBP IT staff did not consistently follow them. CBP IT staff adherence to the configuration management policies and procedures would have enabled detection of the incorrect configuration on DM31, thereby preventing the outage. We requested change control documentation, but CBP could not provide such documentation related to the configuration setting that could be traced to DM31. Because documentation was lacking, we were not able to verify which change controls leading to the incorrect configuration on DM31 were weak or missing.

**Corrupted Patch on Oracle Device Contributed to Service Degradation and Outage**

In addition to not having the proper configuration setting, the DM31 database did not have up-to-date patches. This prevented the database from operating as designed and led to service degradation of Passenger Systems Program Directorate applications that contributed to the August 16, 2019 outage.

According to *DHS Sensitive Systems Policy Directive 4300A,*[12] components should administer systems to reduce vulnerabilities through testing and management, and installing patches promptly. Component information

[9] CBP operates a data center in Virginia that houses the Enterprise Operations Center and Exadata Database Machines.
[10] *DHS Sensitive Systems Policy Directive 4300A* at §§ 3.7.d & 4.8.3.d, ver. 13.1, July 27, 2017.
[11] *Office of Information and Technology Change Control Board Process Handbook* at §§ 4.1-4.2 ver. 5.0.
[12] *Sensitive Systems Policy Directive 4300A* at § 4.8.3.d.

security personnel should ensure their systems are fully patched and comply with DHS configuration guidance. Additionally, continuous monitoring is performed by reviewing current vendor patch notifications, security configuration best practices, security architecture guidance, and emerging threats and vulnerabilities.[13] Information Security Vulnerability Management (ISVM) is a program to proactively increase security situational awareness of, and minimize risks to, DHS' information systems.[14] ISVM guidance sets a timeline for components to acknowledge and comply with bulletins related to servers.

In the case of the Oracle patch update, CBP had 5 business days to acknowledge the requirement and 25 business days to comply, as shown in Table 3.

**Table 3. Historical ISVM Timelines for Oracle Critical Patch Updates**

| Information Security Vulnerability Management | Type | Release Date | Acknowledgement Due Date | Compliance Due Date |
|---|---|---|---|---|
| 2019-6153237-0-B-Oracle Critical Patch Update - July 2019 - Multi-Product Multiple | Bulletin | Jul 17, 2019 | Jul 24, 2019 | Aug 21, 2019 |
| 2019-6080590-0-B-Oracle April 2019 Critical Patch Update Multi-Product Multiple Vulnerabilities | Bulletin | Apr 17, 2019 | Apr 24, 2019 | May 22, 2019 |
| 2019-5822419-1-B-Oracle January 2019 Critical Patch Update Multi-Product Multiple Vulnerabilities | Bulletin | Jan 29, 2019 | Feb 5, 2019 | Mar 5, 2019 |
| 2018-4884847-0-B-Oracle October 2018 Critical Patch Update Multi-Product Multiple Vulnerabilities | Bulletin | Oct 19, 2018 | Oct 29, 2018 | Dec 11, 2018 |
| 2018-4820254-0-B-Oracle Critical Patch Update July 2018 | Bulletin | Jul 18, 2018 | Jul 25, 2018 | Sep 6, 2018 |

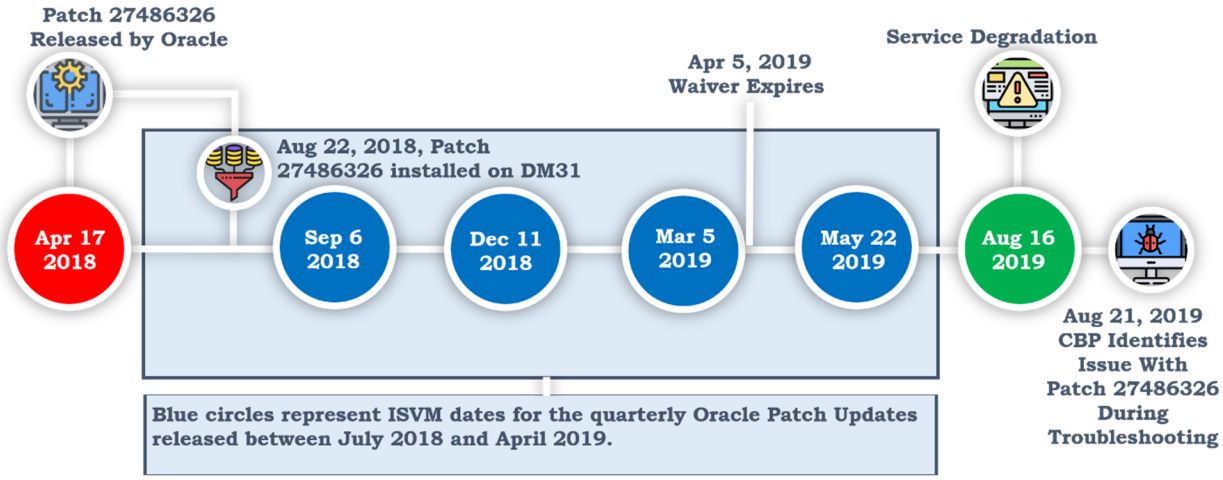
*Source:* CBP Vulnerability Assessment Team

However, rather than adhering to the 25-day requirement, CBP requested and received a DHS waiver in 2018 for Exadata databases and the underlying operating system to be routinely patched every 6 to 12 months. According to CBP officials, they requested the waiver because vendor patches often have

[13] *Sensitive Systems Handbook* at att. O; *see* also *Vulnerability Management Program* at § 2.1, ver. 15, May 2, 2019, Section 2.3.1.
[14] *Sensitive Systems Handbook* at att. O; *see* also *Vulnerability Management Program* at § 2.1.

defects and Exadata devices have to be offline for 12 to 20 hours to apply image patch bundles. CBP officials also stated that the coordination required to install these patches can take up to 12 weeks. The waiver expired prior to the ISVM compliance due date for the Oracle April 2019 Critical Patch Update. This update should have been applied prior to the outage. Additionally, the risk mitigation section of the waiver states, "All critical patches will be applied as soon as the vendor releases them." Figure 1 outlines the last patch applied to DM31, as well as subsequent ISVM due dates for additional patches prior to the outage.

**Figure 1. CBP DM31 Patching Timeline**




*Source:* OIG-generated based on CBP data

Despite the various requirements, CBP did not take adequate steps to ensure that a patch was applied promptly to DM31. On April 17, 2018, Oracle released a quarterly patch bundle. However, CBP did not apply this patch to DM31 until August 22, 2018, 4 months later. The following year, on August 21, 2019, CBP observed during recovery from the system outage that the patch had been applied, but it lacked the corresponding code. This prevented the patch from operating as designed and led to service degradation of the Passenger Systems Program Directorate applications and a multi-day recovery effort.

CBP officials were unable to determine why the corrupted patch did not execute properly. An Oracle representative we spoke with stated that a patch may start out working correctly, but may become corrupt over time. Subsequent to the patch released in April 2018, Oracle released five additional patch set updates in July 2018, October 2018, January 2019, April 2019, and July 2019. However, the first three patch set updates were still

covered by the waiver and the July 2019 update had an ISVM compliance date of August 21, 2019.

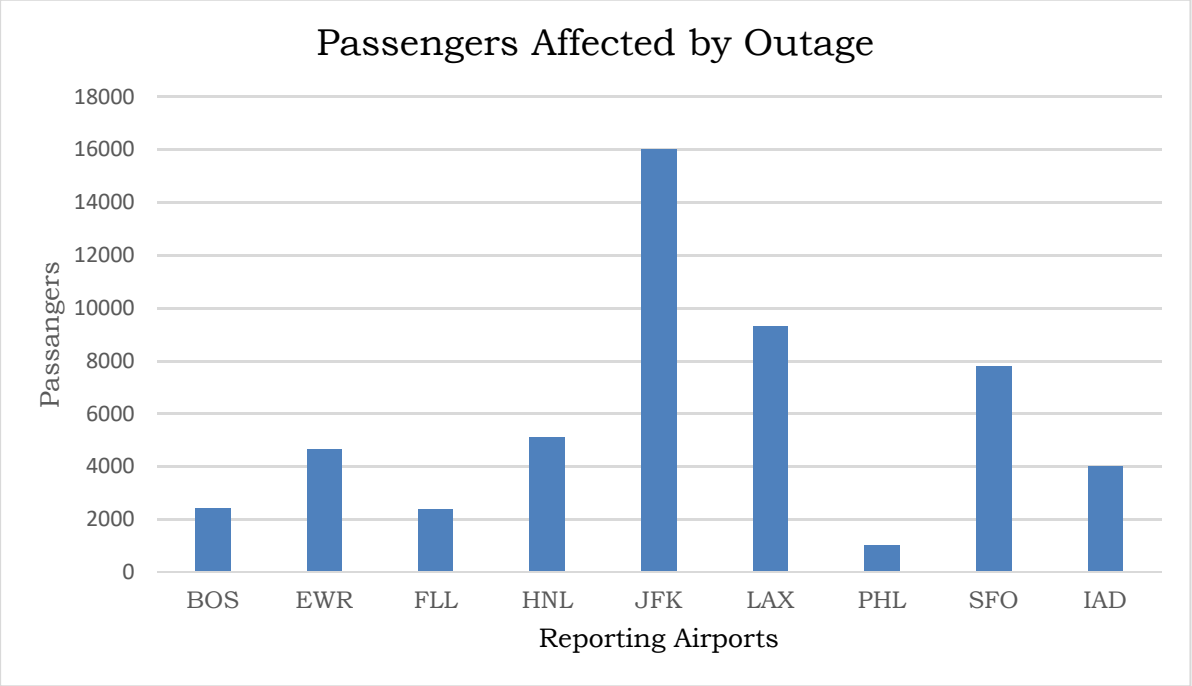
According to CBP officials, they now spend extra time in the test environment and run a script Oracle provided to detect issues similar to the out-of-date patch management that helped cause the August 2019 outage. Although it is not clear that up-to-date patching would have corrected the corrupted patch, CBP should have ensured that at least the April 2019 patch bundle was applied promptly.

**System Degradation Led to Increased Wait Times at Airports**

Lacking the proper configuration setting in DM31, CBP's Passenger Systems Program Directorate applications experienced significant system performance degradation. The system degradation was so severe, CBP officials at as many as nine international airports perceived it as a full-fledged system outage. The nine international airports that responded to our survey reported delays in processing incoming international passengers. This led to increased wait times for their entry into the United States. For example, some airport personnel estimated their wait times doubled while staff at one airport reported it was unable to process any arriving passengers during the outage. Figure 2 illustrates the reported number of passengers who experienced delays due to the outage, as reported by each airport.[15]

[15] The number of passengers affected varies based on the volume of international traffic to the airports at the time of the outage.

**Figure 2. Survey Responses from Airports,[16] Passengers Affected**




*Source:* OIG-generated based on CBP data from airport surveys

The system outage also led CBP to undergo a multi-day system recovery effort, requiring up to a full week to address some of the issues. As part of the effort to identify and resolve issues related to the outage, CBP noted in its root cause analysis that as more databases began running on DM31, services began to crash unexpectedly. Upon confirming that all of CBP's other devices had the recommended configuration setting, Oracle concluded that system performance degradation was primarily due to the configuration issue. According to a CBP official, the incorrect configuration on DM31 was probably caused by human error, but CBP could not provide documentation to confirm that assertion.

According to a CBP official, CBP staff now run infrastructure checks weekly and specifically check for configuration issues using a script developed in-house. Additionally, CBP added procedures to ensure two people verify system changes and scripts. Such actions are tailored to addressing the issue that led to the August 2019 system degradation.

[16] Boston Logan Airport (BOS), Newark Liberty International Airport (EWR), Fort Lauderdale–Hollywood International Airport (FLL), Inouye International Airport (HNL), John F. Kennedy International Airport (JFK), Los Angeles International Airport (LAX), Philadelphia International Airport (PHL), San Francisco International Airport (SFO), and Washington Dulles International Airport (IAD).

## CBP Faced Additional Challenges that Hindered Operations during the Outage

CBP personnel faced additional difficulties that hindered traveler screening operations during the system outage. Specifically, CBP officers at airports were unable to access the backup system, as required. They also were not prepared to effectively implement and manage backup procedures. The difficulties CBP officers experienced were due to inadequate training as well as ineffective communication from CBP Headquarters about the outage.

### CBP Personnel Experienced Difficulties Accessing and Using Backup Screening Systems

The August 2019 performance disruptions and outage resulted in the need for CBP officers to revert to "offline" backup systems to sustain screening operations. CBP has standard operating procedures that outline protocols, known as mitigation procedures, to follow during an unscheduled system outage or a significant system slowdown.[17] According to these procedures, a CBP port of entry Shift Supervisor should initiate mitigation procedures in the event that operations are adversely affected. Once such procedures are initiated, CBP officers should begin to use the backup systems within 30 minutes of an outage to continue screening incoming travelers. Specifically, when the TPAC system is unavailable, CBP officers should use the Portable Automated Lookout System (PALS)[18] instead. PALS provides a basic "watch list" of people designated as inadmissible to the United States.[19] PALS is a basic, standalone application that does not interface with other technology when primary passenger screening systems are offline. Each month, OIT updates PALS data and distributes it electronically to all ports of entry to ensure they have the most up-to-date watch list data.

In keeping with CBP policy, some ports of entry used PALS during the August 16, 2019 outage. However, when attempting to deploy PALS to process incoming international travelers, CBP officers we surveyed from some of the airports stated they experienced difficulties accessing and using the system. The CBP OIT practice of sending a PALS password monthly to points of contact at ports of entry did not prove effective, especially to support exigent circumstances. For example, several CBP officers expressed difficulty finding

[17] CBP Directive 3340-041, *Standard Operating Procedures During System Outages at Air, Land, and Sea Ports of Entry* (Nov. 26, 2007).
[18] PALS is an alternate, offline international passenger screening system to be used during outages as a backup.
[19] PALS contains an extract of TECS law enforcement data, including a list of people who are not allowed entrance into the United States, and has the capability to run queries on this data.

the correct password in their emails, and some could not find it at all. Additionally, a number of officials had trouble entering the PALS password, delaying their access to the system needed to sustain passenger screening operations.

Further, the process for distributing PALS thumb drives and data to the CBP ports of entry was not adequate. Some CBP officers we surveyed stated that they had insufficient PALS equipment, such as USB thumb drives with the PALS data, at terminals where they were processing passengers. Moreover, not all CBP officers were aware that it was their responsibility to request PALS equipment commensurate with the number of workstations used to process passengers at their ports. The officials were also expected to regularly make sure they had adequate numbers of points of contact designated at their airports to receive the password, and to verify that it worked so the backup system would not be held up during emergency time of need.

Some CBP officers expressed difficulty using PALS because they had not been properly trained on the system. For example, they did not know how to access the system, or once accessed, how to properly screen passengers using PALS data. During our review in March 2020, CBP OIT representatives stated that there was no requirement at the time for CBP officers to take PALS training.

Ultimately, the use of the backup procedures resulted in less effective passenger screening practices. Without sufficient access to and training on PALS, CBP officers at ports of entry will be unable, delayed, or limited in their ability to process international passengers if a system disruption occurs in the future. More importantly, processing incoming international passengers without real-time screening applications increases the risk of allowing inadmissible people entry into the United States. Because PALS does not interface with other technology, CBP officers are not able to identify individuals who might be traveling under aliases or have criminal records, which poses inherent risks to national security.

As of March 2020, CBP had already begun to make some necessary changes in attempts to prevent some of the PALS issues it faced during the August 2019 outage. For example, OIT officials have updated PALS policies and procedures to include new requirements for ports of entry, such as:

- CBP officers are now required to check thumb drives and PALS access to ensure they have the latest data and passwords for PALS.
- CBP officers are now required to reboot PALS host machines every 21 days to ensure all patches and upgrades are installed regularly.

- The PALS database is now updated and provided to ports daily, rather than monthly.

**CBP Personnel Received Inadequate Communication about the Nationwide Outage**

CBP Headquarters did not sufficiently communicate information about the system outage. Therefore, CBP personnel at airports did not know whether the outage was nationwide, when it was fully resolved, or what caused it. CBP Headquarters maintains real-time information on the health of the system on a nationwide OIT National System Health Dashboard,[20] including immediate notifications of slowdowns and outages for nationwide awareness. However, some CBP personnel at airports were unaware of the dashboard, did not remember it was an option, or did not access it to obtain available information. This was, at least partly, because the dashboard was not listed in guidance as a mitigation step for laptops or workstations. As a result, CBP officers only began following mitigation steps after they noticed delays in processing passengers.

CBP Headquarters also did not provide sufficient information to the field offices about the outage, as it does not routinely communicate system issues to ports of entry. When CBP Headquarters does not adequately inform field offices about OIT's methods of communicating information (i.e., the National System Health Dashboard) regarding nationwide system outages, field offices may waste resources looking elsewhere for information that is readily available on the OIT dashboard. Without reminders, field offices can waste time and resources continually checking systems instead of processing passengers. For example, CBP personnel at one airport said that they had to assign a CBP officer to periodically access Passenger Systems Program Directorate applications to see if response times were normal. Other locations called the Help Desk to determine whether the system outage was local or nationwide.

## Conclusion

CBP's response to prior report recommendations contributed to the implementation of a robust monitoring system that helps CBP identify and respond to system outages in a timely manner. When first alerted of the August 16, 2019 system outage, OIT immediately implemented its mitigation strategy to identify and resolve the outage. However, even with OIT's timely response to the outage alerts, CBP field offices experienced significant delays processing incoming international air travelers. The system performance

[20] Formerly known as TECS Dashboard.

degradation that led to the delays occurred because CBP had not verified the DM31 was properly configured and patches were up-to-date. In addition, inadequate access to backup systems, inadequate training of CBP officers, and ineffective communication about the outage, contributed to its severity.

System outages, such as the one in August 2019, severely hamper screening operations at airports. CBP officers rely on IT systems and applications to expedite high volumes of inspections and flight security operations at airports each day. Performance disruptions and outages require CBP officers to revert to backup systems to continue their screening operations. Using backup systems and procedures result in less effective screening, which poses increased risk to safety and national security. Any future, repeat system outages could imperil CBP's mission of safeguarding the Nation's borders, allowing inadmissible or unsuitable people to enter the United States. The degraded throughput at international points of entry may also erode confidence in DHS' ability to effectively carry out its border security mission.

## Recommendations

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

**Recommendation 1**: Implement a verification process to ensure that configuration changes are fully implemented and patches are installed in a timely manner.

We recommend the CBP Assistant Commissioner for the Office of Field Operations:

**Recommendation 2**: Require new employee and recurring training for CBP staff performing passenger screening using OFO outage mitigation applications, including deploying the PALS system.

**Recommendation 3**: Require regular tests of outage mitigation applications such as PALS deployment procedures, and update those procedures based on the results.

**Recommendation 4**: Ensure all CBP field offices and ports of entry are able to access outage mitigation applications such as the PALS system, by increasing awareness of the process to request necessary equipment and receive updated passwords for all workstations used to screen international passengers.

**Recommendation 5**: Ensure all CBP field offices are aware of the National System Health Dashboard communication process for keeping field staff informed of system interruptions.

**Management Comments and OIG Analysis**

CBP concurred with all of five of our recommendations. Appendix B contains a copy of CBP's response in its entirety. CBP also provided technical comments and suggested revisions to our report in a separate document. We reviewed the technical comments and made changes to the report where appropriate.

We obtained written comments on the draft report from the Senior Component Accountable Official, who emphasized that CBP takes the restoration of systems service very seriously and detailed CBP's actions to promptly identify and resolve the outage. A summary of CBP's response to each recommendation and OIG's analysis follows.

**CBP Comments to Recommendation #1:** Concur. CBP OIT Enterprise Data Management and Engineering Directorate will implement new processes in its operations, such as additional discipline and peer review for quality assurance of all changes. This will include reviews of configuration elements to ensure no negative impact to enterprise systems beyond those directly impacted by changes as patches may become corrupt or deteriorate over time. The estimated completion date is November 30, 2020.

**OIG Analysis of CBP Comments:** CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation to support that all planned corrective actions are completed.

**CBP Comments to Recommendation #2:** Concur. CBP OFO will ensure that all CBP officers receive recurring training on outage mitigation backup systems, including PALS. OFO, in collaboration with OIT, is crafting a training webinar, which will be recorded and re-used as needed at the ports of entry. The estimated completion date is December 31, 2020.

**OIG Analysis of CBP Comments:** CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation to support that all planned corrective actions are completed.

**CBP Comments to Recommendation #3:** Concur. OFO will ensure that PALS deployment procedures are tested and updated, and OFO will issue a

memorandum and muster instructing field offices to test back up procedures, including PALS, semi-annually. The estimated completion date is December 31, 2020.

**OIG Analysis of CBP Comments:** CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation to support that all planned corrective actions are completed.

**CBP Comments to Recommendation #4:** Concur. OFO will ensure that field offices and ports of entry: 1) have access to PALS; 2) are familiar with outage protocols; and 3) have the necessary equipment and passwords. The new password is also available to all PALS users through the CBP Technology Service Desk 24/7 toll-free number. OFO will send guidance to field offices outlining the proper handling of outage protocols and the mechanism to request equipment and password updates. The estimated completion date is December 31, 2020.

**OIG Analysis of CBP Comments:** CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation to support all planned corrective actions are completed.

**CBP Comments to Recommendation #5:** Concur. OFO will send a reminder memorandum and muster field offices to ensure compliance with the National System Health Dashboard communication for keeping CBP officers informed of system interruptions. The estimated completion date is November 30, 2020.

**OIG Analysis of CBP Comments:** CBP's actions are responsive to the intent of this recommendation. This recommendation will remain open and resolved until CBP provides documentation to support all planned corrective actions are completed.

## Appendix A
## Objective, Scope, and Methodology

Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107−296) by amendment to the *Inspector General Act of 1978*. We conducted this review to determine whether CBP's actions to implement previous outage-related recommendations could have prevented the onset and length of the August 16, 2019 nationwide system outage at U.S. ports of entry.

To answer the objective, we researched and evaluated Federal, DHS, and DHS component guidance related to CBP system outages and degradation issues. In addition, we reviewed relevant U.S. Government Accountability Office and DHS OIG reports, CBP documents, and congressional testimonies. The team requested, obtained, and reviewed policies and procedures for deploying PALS at OIT Headquarters and local ports of entry level, both before and after the August 16, 2019 outage.

We conducted interviews with Oracle and CBP OIT staff with system-specific knowledge and firsthand accounts of the system degradation and recovery efforts. We conducted a site visit to CBP OIT in Newington, VA. We interviewed the Passenger Systems Program Directorate Division Director, Enterprise Data Management and Engineering Directorate Deputy Program Manager, and Accenture Program Manager (contractor) Director. Additionally, we conducted interviews with personnel at two international airports, and provided surveys to personnel at 17 airports nationwide.

We provided a survey to CBP OIT officials to determine whether CBP's actions to implement previous OIG outage-related recommendations from prior reports OIG-18-19 and OIG-17-114 were relevant to the August 16, 2019 outage, and determine if they helped prevent or minimize the onset and length of the outage. Information obtained from these interviews and surveys were used to identify steps CBP staff took during the outage at each airport, whether they encountered any issues with the PALS backup system, and whether they complied with CBP policies and procedures. We obtained and reviewed system logs, documented evidence related to the event and the recovery effort, and provided an assessment and analysis for this review.

We used the work of internal specialists from the OIG's Information Assurance and Testing Branch to assess why previous OIG recommendations did not prevent the onset of the nationwide outage. In addition, the Information Assurance and Testing Branch evaluated CBP's ability to protect and safeguard mission-critical passenger processing systems from outages and determined

whether adequate test and recovery environments were in place. The specialists completed the following reviews:

- A configuration management review of CBP's Exadata DM31. Specifically, we reviewed the configuration settings to determine whether there was an issue with the NUMA balancing configuration.

- A vulnerability patch management review of CBP's Exadata DM31 to identify if any were patches missing. Specifically, we determined whether a missing patch contributed to the service degradation.

We incorporated the results of the Information Assurance and Testing Branch specialists' work in our findings as appropriate.

We conducted this review between October 2019 and April 2020 pursuant to the *Inspector General Act of 1978*, as amended, and in accordance with Council of the Inspectors General on Integrity and Excellence *Quality Standards for Inspection and Evaluation*. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our review objectives. Major OIG contributors to the review 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

October 16, 2020

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

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

SUBJECT: Management Response to Draft Report: "CBP's Configuration Management Practices Did Not Effectively Prevent System Outage" (Project No. 19-070-AUD-CBP)

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

CBP is pleased with the OIG's recognition that CBP's actions to address prior outages minimized the length and severity of disruptions to passenger screening during the August 2019, temporary outage. CBP takes restoration of service for systems very seriously and took steps to improve troubleshooting procedures. For example, CBP's more effective control structure for monitoring passenger screening systems enabled CBP to take prompt action to identify and resolve the outage to ensure that the disruption of service was quickly abated.

In addition, the CBP Office of Information Technology (OIT) completed several IT Modernization efforts during fiscal year 2019, with the following goals in mind: 1) maintaining a highly reliable and secure network infrastructure; 2) improving application and infrastructure performance, reliability availability, and resiliency; and 3) enabling field operators to execute their mission. CBP OIT will continue to enhance the agency's resiliency through 2020, and beyond, to ensure that mission-critical systems are always available and prepared for the unexpected.

However, we are concerned that the OIG draft report incorrectly attributes the outage to CBP not taking steps to ensure its configuration management policies and procedures

were followed or that patches were applied promptly, despite the draft report also noting that an Oracle representative stated to the OIG that a patch may start out working correctly, but may become corrupt over time. CBP database administrators and Subject Matter Experts do not have control over this potential issue. CBP maintains that the outage was initiated by the application of the Oracle patch provided, and that the Non-Uniform Memory Access configuration setting was a contributing factor or became a tipping point under operational load. CBP does not maintain the source code or the vendor's development of patches.

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

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

Attachment

**Attachment: Management Response to Recommendations Contained in Project No. 19-070-AUD-CBP**

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

**Recommendation 1:** Implement a verification process to ensure that configuration changes are fully implemented and patches are installed in a timely manner.

**Response:** Concur. CBP Office of Information and Technology (OIT) Enterprise Data Management and Engineering Directorate will implement new processes within its operations to include additional discipline and peer review for quality assurance of all changes. This will include reviews of configuration elements to balance and ensure no negative impact to enterprise systems beyond those directly impacted by changes, as patches may become corrupt or deteriorate over time. Unfortunately, CBP database administrators and Subject Matter Experts (SMEs) do not have control over the potential issue, as CBP does not maintain the source code or the vendor's development of patches. However, to aid in quickly identifying this issue in the future, CBP will implement several monitoring and configuration management improvements.

For example, CBP will expand the use of Oracle's Oracle Enterprise Manager (OEM) to review and validate that configuration items are set and in alignment with approved baselines. OIT SMEs will develop a script that checks each Exadata system on a weekly basis against the approved configuration and highlight any deviations, and output of this script will be reviewed by engineers for Exadata weekly. CBP OIT will also engage with the vendor to review and baseline all Oracle databases and Exadata. This baseline includes new technology elements to support a more rapid failover to secondary systems. Improvements in the overall Exadata enterprise and faster failover of databases will allow CBP to reduce the time between patches and install more "hot patches" in line with vendor recommendations. Estimated Completion Date (ECD): November 30, 2020.

OIG recommended that the Executive Assistant Commissioner for the Office of Field Operations:

**Recommendation 2:** Require new employee and recurring training for CBP staff performing passenger screening using OFO mitigation outage protocol applications, including deploying the PALS system.

**Response:** Concur. CBP Office of Field Operations (OFO) will ensure that all CBP officers (CBPO) receive recurring training on outage backup systems, including PALS.

OFO, in collaboration with OIT, is crafting a training webinar which will be recorded and re-used as needed at the Ports of Entry (POE). ECD: December 31, 2020.

**Recommendation 3:** Require regular tests of outage mitigation applications such as PALS deployment procedures and update those procedures based on the results.

**Response:** Concur. OFO will ensure that PALS deployment procedures are tested and updated, and OFO will issue a memorandum and muster instructing Field Offices to test back up outage procedures including PALS semi-annually. ECD: December 31, 2020.

**Recommendation 4:** Ensure all CBP field offices and ports of entry are able to access mitigation outage applications such as the PALS system, by increasing awareness of the process to request necessary equipment and receive updated passwords for all workstations used to screen international passengers.

**Response:** Concur. OFO will ensure that Field Offices and POEs: 1) have access to PALS; 2) are familiar with the outage protocols; and 3) have the necessary equipment and passwords. OIT currently distributes the new password via email monthly to the PALS Points of Contact (POC), reminding them to change and disseminate the newly issued password to staff. The new password is also available to all PALS users through the CBP Technology Service Desk 24/7 toll free number. In collaboration with OFO, OIT created a Share Point Site in July 2018] where POEs can electronically request equipment.

Additionally, automated emails are sent by OIT to all PALS POCs whose equipment is more than 14 days out of compliance with OIT's password updates. OFO will send guidance to Field Offices outlining the proper handling of outage protocols and the mechanism to request equipment and password updates. ECD: December 31, 2020.

**Recommendation 5:** Ensure all CBP field offices are aware of the National System Health Dashboard communication process for keeping field staff informed of system interruptions.

**Response:** Concur. OFO will send a reminder memorandum and muster to Field Offices to ensure compliance with the National System Health Dashboard communication to keep CBPOs informed of systems interruptions. ECD: November 30, 2020.

## Appendix C
## Prior Audit Recommendations

The following tables depict recommendations from each audit effort, the current status, and our assessment of whether the corrective action prevented the onset and length of the August 16, 2019 outage.

| ***CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations* (OIG-17-114)**<br><br>**Recommendations** | **Current Recommendation Status** | **Did the recommendation and corrective action prevent the onset and length of the August 16, 2019 incident?** |
|---|---|---|
| 1. Conduct a user assessment of the TECS Portal to identify, evaluate, and address performance challenges in traveler pre-screening operations in the field. | Closed | No |
| 2. Develop a plan to address maintenance, infrastructure, dependencies on external systems, and other factors that contributed to challenges regarding availability of primary traveler screening applications. | Closed | Yes |
| 3. Assess the need for performance measures to monitor, evaluate, and ensure the availability of primary traveler screening applications from the end-user perspective at ports of entry. | Closed | Yes |
| 4. Complete backup process improvement initiatives, including development of a dashboard for port-level visibility on system latency and outage status to assist management with mitigation decision making and upgrade of mitigation applications, as appropriate. | Closed | No |
| 5. Complete modernization plans for the Enforce 3 system to ensure adequate availability and functionality to support border security mission needs. | Open | No |

| ***CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations* (OIG-17-114)**<br><br>**Recommendations** | **Current Recommendation Status** | **Did the recommendation and corrective action prevent the onset and length of the August 16, 2019 incident?** |
|---|---|---|
| 6. Develop a plan to improve resolution time and mitigate the impact of network outages that degrade the capabilities of the Air and Marine Operations Surveillance System. | Closed | No |
| 7. Develop and implement a comprehensive technology refresh strategy and budget plan to upgrade outdated IT infrastructure and ensure adequate system availability and performance to support CBP's border security missions. | Closed | No |

*Source:* OIG table based on *CBP's IT Systems and Infrastructure Did Not Fully Support Border Security Operations,* OIG-17-114, September 28, 2017.

| ***Review of CBP Information Technology System Outage of January 2, 2017* (OIG-18-19)**<br><br>**Recommendations** | **Current Recommendation Status** | **Did the recommendation and corrective action prevent the onset and length of the August 16, 2019 incident?** |
|---|---|---|
| 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. | Closed | No |
| 2. Ensure that OIT staff receive timely notifications of critical vulnerabilities to CBP operating systems. | Closed | No |
| 3. Adjust the Technology Operations Center alert criteria for TECS to ensure earlier notifications of slowdowns and outages. | Closed | Yes |
| 4. Establish policy to implement TECS recovery operations within 1 hour of an outage. | Closed | Yes |

| ***Review of CBP Information Technology System Outage of January 2, 2017* (OIG-18-19)**<br><br>**Recommendations** | **Current Recommendation Status** | **Did the recommendation and corrective action prevent the onset and length of the August 16, 2019 incident?** |
|---|---|---|
| 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. | Closed | No |

*Source:* OIG table based on *Review of CBP Information Technology System Outage of January 2, 2017,* OIG-18-19, November 21, 2017.

## Appendix D
## Office of Audits Major Contributors to This Report

Kevin Burke, Audit Director
Katrina Reuben Dorman, Audit Manager
Alexander Stewart, Audit Manager
Stephanie Matthews, Senior Auditor
Ken Schoonover, Program Analyst
Tessa Clement, Program Analyst
Thomas Rohrback, Branch Chief Information Assurance and Testing Branch
Rashedul Romel, Information Technology Specialist
Jane DeMarines, Communications Analyst
Nedra Rucker, Referencer

# Appendix E
# Report Distribution

## Department of Homeland Security

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

## 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