TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Review of the System Failure That Led to the Tax Day Outage

September 19, 2018

Reference Number: 2018-20-065

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

REVIEW OF THE SYSTEM FAILURE THAT LED TO THE TAX DAY OUTAGE

Highlights

Final Report issued on September 19, 2018

Highlights of Reference Number: 2018-20-065 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The filing season, defined as the period from January 1 through mid-April, is critical for the IRS because it is during this time that most individuals file their income tax returns. If the tax processing system fails, taxpayers may lose confidence in the IRS's ability to administer the tax code.

WHY TIGTA DID THE AUDIT

This audit was initiated to review the IRS systems outage that occurred on Tax Day, April 17, 2018, and identify solutions to prevent future disruptions.

WHAT TIGTA FOUND

On the last day of the 2018 Filing Season (April 17, 2018), the IRS experienced a storage outage due to a firmware bug that caused a storage array to fail. As a result, 59 tax systems, including the Modernized e-File system, were unavailable for about 11 hours. The IRS Computer Security Incident Response Center found no evidence of any breach or cyber threat activity related to the outage. The IRS restored mainframe operations by the afternoon of the day the outage occurred and processed almost 4 million tax returns before midnight.

In June 2017, International Business Machines (IBM) initially discovered the firmware bug associated with the IRS Tax Day outage and developed a fix, made publicly available in a November 2017 microcode bundle. In December 2017, the IRS agreed with the contractor recommendation to remain on the older microcode bundle for the 2018 Filing Season because it was considered more stable.

In January 2018, IBM product engineers developed a script for another client that experienced an outage due to this firmware bug. However, prior to the IRS outage, IBM did not provide the IRS with any details regarding the other client outage or the availability of a script that would have prevented the Tax Day outage.

While the response team's substantial efforts allowed the IRS to resume tax processing operations the same day, improvements are needed to help mitigate or prevent outages. The "lessons learned" process lacks an overall strategy to consolidate multiple action plans, and monthly microcode bundle meetings have no meeting minutes or documentation of decisions made. The current Tier 1 storage environment, with an average equipment age of less than three years, hosts a portion of core tax processing data. However, it does not have an automatic failover or built-in redundancies and is currently a single point of failure.

TIGTA also found that the Enterprise Storage Services contract is not meeting business needs. During the Tax Day outage, the contractor failed to meet several service level objectives, and this failure requires the contractor to pay liquidated damages to the Government. Additionally, the contract lacks detailed service level objectives for performance monitoring and incident management.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer should: 1) document lessons learned and implement a corrective action plan, 2) formalize the monthly microcode bundle meetings, 3) ensure that decisions not to install microcode bundle updates are documented and approved, and 4) seek liquidated damages from the contractor and make modifications to the Enterprise Storage Services contract.

The IRS agreed with all of the recommendations and has formalized the monthly microcode bundle meetings and sought damages from the Enterprise Storage Services contractor. The IRS plans to document a consolidated action plan, ensure decisions to not install microcode bundles are approved, and make modifications to the contract.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 19, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Review of the System Failure That Led to the Tax Day Outage (Audit # 201820027)

This report presents the results of our review to analyze the Internal Revenue Service (IRS) system outage that occurred on April 17, 2018, and identify solutions to prevent future disruptions. This audit addresses the major management challenges of *Security Over Taxpayer Data and Protection of IRS Resources* and *Providing Quality Taxpayer Services and Expanding Online Services*.

Management's complete response to the draft report is included as Appendix VI.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

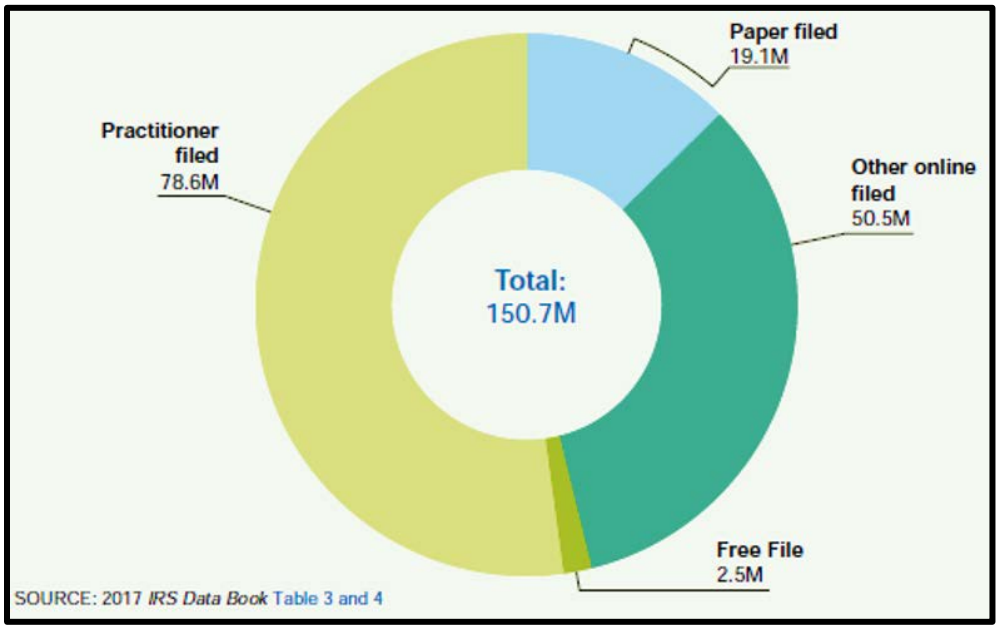
Abbreviations

EOps	Enterprise Operations
ESS	Enterprise Storage Services
IBM	International Business Machines
IRS	Internal Revenue Service
ITOCC	Information Technology Operations Command Center
KISAM	Knowledge, Incident/Problem, and Service Asset Management
MeF	Modernized E-File
SLO	Service Level Objective
SOP	Standard Operating Procedure

Background

The Internal Revenue Service (IRS) relies extensively on information technology systems to annually collect more than $3 trillion in taxes, distribute more than $400 billion in refunds, and carry out its mission of providing service to America's taxpayers in meeting their tax obligations. In Fiscal Year[1] 2017, the IRS processed more than 187 million Federal tax returns. Of those, over 150 million were individual returns, with over 87 percent of these individual returns filed electronically. During Calendar Year 2018, the IRS expects to receive approximately 153.7 million individual income tax returns, with more than 89 percent of those filed electronically. See Figure 1 for a chart of individual returns filed in Fiscal Year 2017 electronically and via paper.

Figure 1: Individual Tax Returns Filed in Fiscal Year 2017



Source: IRS 2017 Data Book.

The IRS continues to modernize its operations and applications by developing and implementing new information technology to provide taxpayers and IRS employees with tools that are more sophisticated. As part of this effort, on June 29, 2012, the IRS awarded the Enterprise Storage Services (ESS) Managed Services contract to the Unisys Corporation to manage planning, designing, building, deploying, and maintaining a new storage environment. According to the

[1] See Appendix V for a glossary of terms.

IRS, this new environment provides an agile solution for rapid deployment of continuous improvements, optimized data storage and retrieval, and flexibility to adapt to IRS growth. The IRS environment consists of 7.5 petabytes of disk space in various configurations in data centers and other facilities across the country. In October 2015, we reported that the ESS contract Service Level Objectives (SLO)[2] do not clearly define important aspects of risk mitigation controls needed to protect data under the ESS Program.[3]

This review was performed from May through July 2018 at the New Carrollton Federal Building in Lanham, Maryland, and the Enterprise Computing Center in Martinsburg, West Virginia. We worked closely with IRS personnel from the Information Technology organization's Enterprise Operations (EOps) organization and the Wage and Investment Division. In addition, we worked with contractor personnel responsible for the performance of the ESS contract. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[2] The SLOs are a means of measuring the performance of the service provider. The SLO may be composed of one or more quality-of-service measurements to produce the SLO achievement value.
[3] Treasury Inspector General for Tax Administration, Ref. No. 2016-20-002, *Measurable Agreements on Security Controls Are Needed to Support the Enterprise Storage Services Solution* (Oct. 2015).

Results of Review

A Storage Device Failure Caused a Tax Processing System Outage for Approximately 11 Hours

On Tax Day, April 17, 2018, the IRS experienced a storage outage due to a firmware bug on one of the IRS's high-availability storage arrays. Because of the outage, 59 tax processing systems, including the Modernized e-File (MeF) system, were unavailable for approximately 11 hours between 2:57 a.m. and 1:40 p.m.[4] See Appendix IV for a detailed timeline of the outage. The IRS Computer Security Incident Response Center concluded that the outage fit the pattern of a previously known firmware bug and determined that there was no evidence of any breach or cyber threat activity related to this outage. The timing and severity of the outage prompted the IRS to allow an additional day to file to April 18, 2018.

The Information Technology Operations Command Center (ITOCC) Incident Management Standard Operating Procedures (SOP)[5] outline the subprocesses, roles, and responsibilities for incident management and supporting functions with the goal of restoring service in a timely manner for Priority 1 and Priority 2 incidents. These procedures identify the activities performed by key personnel to ensure that high-priority incidents are worked and, when needed, activate the Service Restoration Team process to facilitate restoration of service to customers for all production systems. Another document, the Major Outage SOP,[6] addresses the process, activities, and integration relationships required to manage the restoration and continuation of business after a major outage. This SOP also defines the roles and responsibilities for implementing business restoration after a major outage has occurred.

At 2:24 a.m. on April 17, 2018, the IRS's ITOCC received the first system-generated error messages and invoked its established procedures to troubleshoot the problem. At 2:57 a.m., one of the high-availability storage arrays used its automated "call home" capability to send an alert to the vendor, International Business Machines (IBM). It detected a deadlock condition after a warmstart due to cache overflow. IBM never provided an acknowledgement of the performance issue and did not initiate any incident management procedures because IBM identified the call home as a Severity Level 3 (response time for a Severity Level 3 issue is by the end of the next business day). By 3:30 a.m., ITOCC personnel detected problems with several systems and submitted a trouble ticket via the Knowledge, Incident/Problem, and Service Asset Management (KISAM) system.

[4] All times are reported in Eastern Standard Time.
[5] *ITOCC Incident and Problem Management Branch Incident Management Section SOP*, dated January 19, 2018.
[6] *Major Outage SOP*, dated July 28, 2017.

By 6:45 a.m., the ITOCC designated the Incident Manager of Record as part of the Incident Management SOP and worked through several service restoration phases (investigation, assessment, and technical). An hour later, the Toolkit Suite With Command Centre identified a total of 59 tax systems, including the MeF system, affected by the storage array issue. By 9:30 a.m., the IRS declared a Major Outage, initiated the Major Outage SOP, and designated a Major Outage Incident Commander.

By early afternoon on April 17, 2018, the contractors had determined that the root cause of the Tax Day outage was a cache overflow issue causing repeated warmstarts and had deployed a preventive script on the storage device that will monitor and correct the issue if the condition reoccurs. At 1:40 p.m., all IRS mainframes and databases were fully operational and ready to resume tax processing operations. Once these systems were operational, the Wage and Investment Division coordinated a plan with several Electronic Return Originators to initially limit the number of returns submitted in an effort to prevent a second outage due to the system overload. By 3:00 p.m., the IRS started receiving tax returns on a limited basis. Once the initial returns were received with no issues, the IRS notified all taxpayers that the MeF system was online and available for submitting tax returns. By 5:00 p.m., the IRS resumed full tax processing operations. Once tax processing operations resumed, the backlog of unprocessed returns peaked at 12:45 a.m. on April 18, 2018, with 2.3 million returns, but the backlog was fully resolved by 5:30 a.m. that day (April 18, 2018).

Throughout the Tax Day outage, the Communications and Liaison organization released several public messages informing taxpayers of the outage and providing guidance on how taxpayers should continue to file their tax returns. The IRS also sent electronic filing software providers messages, *i.e.*, Quick Alerts, that morning regarding the outage and instructed IRS customer service representatives on how to respond to questions from callers.

Even though tax operations resumed by late afternoon on April 17, 2018, the IRS widely publicized that taxpayers had an additional day to file through midnight on Wednesday, April 18, 2018. The IRS shared this information via a national news release, IRS.gov, and social media.

Established contingency tools, processes, and procedures for mainframe outages served the IRS well during the Tax Day outage. The IRS detected, assessed, repaired, and restored mainframe operations by the afternoon of the day the outage occurred and processed almost 4 million tax returns before midnight within acceptable performance time frames for acknowledgement and receipt.

Improvements Are Needed to Reduce Risks and Response Times for Future Outages

While the IRS effectively responded to the Tax Day outage and timely resumed tax processing operations, the major outage process needs improvement to reduce risks and response times for

future outages. To reduce these risks, the IRS needs to better track lessons learned and vulnerabilities to ensure that remediation and other corrective actions are implemented in full, require sufficient information from contractors about microcode upgrades in order to facilitate better decision-making by IRS management regarding microcode bundle implementation, and improve the resiliency and availability of the Tier 1 architecture.

Lessons learned

The Office of Management and Budget requires that Federal agencies document incident response lessons learned and ensure that processes are in place to verify corrective actions.[7] The IRS's Major Outage SOP requires the EOps Security Operations and Standards Division to conduct after-action activities. Specifically, the Division Director executes the following post-procedural or validation actions as part of the lessons learned process:

- Documents and updates lessons learned and process improvements in the appropriate SOP.
- Creates a corrective action plan and briefs the Information Technology organization for approval and periodic status updates.
- Implements the corrective action plan.
- Verifies completion with approval of the Associate Chief Information Officer, EOps.

EOps organization officials analyzed the Tax Day outage and identified multiple lessons learned and improvements needed to better respond to future outages. However, they did not consolidate all lessons learned and weaknesses into one document for the purposes of monitoring and verifying the completion of the planned corrective actions. Instead, they recorded the corrective actions in multiple documents. The lessons learned process has no overall strategy to consolidate the multiple action plans that would allow the IRS to cohesively track the status of all corrective actions by assigned responsibilities.

For example, two EOps divisions each prepared a separate lessons learned document. One of the two divisions is also tracking major outage weaknesses in a Business Restoration Strategy Plan. In addition, some lessons learned and needed improvements are listed in the notes of EOps monthly meeting minutes. EOps officials told us that corrective actions will be tracked in the 2019 Filing Season Readiness Plan. We reviewed this plan and determined that it does not include some of the corrective actions listed in three of the above four sources. The plan also does not assign responsibilities for task completion and does not include a mechanism for monitoring or tracking the status of work in progress. The 2019 Filing Season Readiness Plan is not appropriate for the purposes of coherently tracking major outage corrective actions.

[7] Office of Management and Budget, OMB Circular No. A-130 (Revised), *Managing Information as a Strategic Resource*, Appendix I (July 2016).

Significant weaknesses identified by the IRS during the outage that are not consolidated centrally for status and tracking purposes include:

- ***Quality of KISAM Tickets*** – The IRS determined that the quality of the KISAM tickets needs to be improved and tickets need to be prepared early on in the outage to better describe the conditions observed so that the description captured in the trouble ticket and the subject line of the e-mail sent are readily identifiable and understood by all recipients. For example, the subject line of the Tax Day outage trouble ticket, *"Warning: Catalog Task Contention wait-time was exceeded,"* was not updated at any point during the incident to adequately reflect outage observations.
- ***Notification of IRS Personnel and Contractors*** – IRS personnel did not inform the Associate Chief Information Officer and the Deputy Associate Chief Information Officer, EOps, about the outage until they arrived at work later that morning, approximately four hours after the outage was first reported. The ITOCC personnel were not sure about whom to contact at Unisys or IBM to begin triage of the mainframes and tried an 800 number they found online for Unisys storage support. Per the ESS Managed Services contract, Unisys or IBM as the managing contractors who are responsible for the IRS Tier 1 storage environment should have been first to identify the outage and contact the IRS. During this outage, it was the IRS who initially recognized a problem, and the IRS had to reach out and notify its contractors to prompt action on remediation. The contractors did not uphold their contractual agreement.
- ***Training Needed for Toolkit Suite With Command Centre*** – IRS executives and managers with outage remediation and decision-making responsibilities expressed the need for a better understanding of the Business Restoration Strategy process and the Toolkit Suite With Command Centre.

The EOps organization has neither clearly assigned responsibility nor created procedures for documenting all problems or issues identified during the outage or for monitoring to ensure the completion of corrective actions. The current Major Outage SOP states that a single individual will be responsible for documenting an action plan. Information Technology organization management told us that the lessons learned after-action requirements documented in the Major Outage SOP apply only to the Continuity Management Office and not to the entire Information Technology organization. Without central tracking and monitoring of corrective actions for all weaknesses identified in the major outage process, there is a risk that the IRS will not correct all weaknesses. This could reduce response effectiveness and add to delays in responding to future outages.

Microcode bundle process

The Information Technology organization holds monthly meetings with Unisys and IBM to discuss current microcode bundle levels on the IRS mainframes. At these meetings, IBM makes recommendations to Unisys, as the prime contractor, as to whether or not to implement the latest

microcode bundle. The IRS will either concur or nonconcur with the proposal. Unisys follows an internal company policy that requires microcode bundles to have, at a minimum, 450 machine weeks in a production environment prior to installation on IRS equipment. This internal policy is part of a draft document, created in 2013, that was never formalized by Unisys.

In June 2017, IBM discovered a firmware bug while conducting testing in a laboratory environment. In response to the bug, IBM developed a fix and made it part of IBM's Microcode Bundle 88.24.6.0, released to the public on November 7, 2017. As part of the bundle release process, IBM includes release notes that provide technical details for each individual update, such as the specific risks associated with each known bug or defect.

The bug discovered in IBM's laboratory in June 2017 is the microcode defect that caused the Tax Day outage. During the December 2017 monthly microcode bundle meeting, upon recommendation from contractors, the IRS agreed with the decision to continue with what was considered a more stable version of the microcode, Bundle 88.23.20.0, for the remainder of the filing season. This decision was based on the relatively recent release date of Microcode Bundle 88.24.6.0 (it did not yet meet Unisys's requirement of 450 machine weeks in a production environment). However, there was no detailed discussion regarding individual fixes and whether these defects and associated updates could affect the IRS environment. Documentation of the monthly microcode meetings is limited to a single spreadsheet that identifies the recommended microcode updates and an e-mail sent to stakeholders containing high-level comments about the meeting. The meeting documentation lacks an agenda, meeting minutes, a list of attendees, and any relevant documentation about decisions made. According to the Internal Revenue Manual, any decision to forego installation of upgrades should be documented as a risk-based decision and approved by the system authorizing official.[8]

In January 2018, another IBM client experienced an outage triggered by the same firmware bug discovered in June 2017. To resolve the issue with the other client, IBM product engineers developed and deployed a script that corrected and monitored the storage array cache that ensured the condition does not reoccur. After this event, IBM made no efforts to communicate this condition to the IRS or notify the IRS about the preventative script it had developed that would have prevented the Tax Day outage. By June 9, 2018, all Tier 1 storage arrays were upgraded to Microcode Bundle 88.24.6.0. In addition, all of the Tier 1 storage arrays show no signs of ongoing system vulnerabilities, and the condition related to the Tax Day outage has not reoccurred.

Tier 1 storage architecture

The Tier 1 storage architecture includes mainframes, storage arrays, computer hardware and software maintenance, and related services. As part of the ESS contract, the Tier 1 architecture

[8] Internal Revenue Manual 10.8.50, *Information Technology Security, Servicewide Security Patch Management* (April 29, 2016).

receives Gold Storage Class service that provides high-speed, high-availability storage for tax processing systems and applications. The Gold Storage Class SLO for mainframe availability requires a 99.999 percent uptime and less than 26.5 minutes of unplanned downtime per year. However, the current configuration of the Tier 1 storage environment cannot meet these requirements.

The Tier 1 storage architecture consists of seven high-speed, high-availability storage arrays with an average age of less than three years. Presently, three of the storage arrays, located at the Martinsburg Computing Center, host a portion of core tax processing data. However, there are no automatic failovers or built-in redundancies for these three storage arrays. Additionally, not all of the applications and systems data hosted in the Martinsburg Computing Center are fully replicated to the Memphis Computing Center. As demonstrated during the Tax Day systems outage, this creates a single point of failure for tax processing operations. Because of this architecture, it takes up to 36 hours for the IRS to conduct disaster recovery operations, shifting tax processing activities from the Martinsburg Computing Center to the Memphis Computing Center.

In response to the outage, the IRS expedited existing plans to eliminate this single point of failure and improve restoration time. This includes the procurement of three additional storage arrays, which will provide automatic failover and built-in redundancy for the Tier 1 storage environment. In addition, each array hosting core tax processing data will fully replicate to the Memphis Computing Center. The project goal is to reduce any system outage to two hours or less. These enhancements are tentatively scheduled to be completed prior to the 2019 Filing Season and will cost approximately $5.8 million.

Recommendations

The Chief Information Officer should:

Recommendation 1**:** Ensure that the Director, Security Operations and Standards Division, collects and formally documents in one consolidated action plan any lessons learned for all major outages and implements the approved corrective action plan per the Major Outage SOP.

> ***Management's Response:*** The IRS agreed with this recommendation. Enterprise Operations created a process that will be used to collect and document a consolidated action plan in accordance with the updated Major Outage SOP.

Recommendation 2: Formalize the monthly microcode bundle meetings with IBM and Unisys to include documenting meeting participants, detailed meeting minutes, and discussions of risks identified in the release notes for the current microcode updates.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS formalized the monthly microcode bundle meetings which includes documenting meeting

participants, meeting minutes, decisions, and discussions of risks identified in the Release Notes for the current microcode upgrades.

Recommendation 3: Ensure that all decisions to not install the latest microcode bundle updates are documented and approved by the system Authorizing Official.

Management's Response: The IRS agreed with this recommendation. The IRS will implement a process to ensure that the Authorizing Official and responsible directors are aware of the content of the microcode bundle updates and approve decisions to not install.

The Current Enterprise Storage Services Contract Is Not Meeting Business Needs

Under the ESS contract, the IRS's Tier 1 storage environment receives Gold Storage Class service. As part of the service, there are several SLOs that the contractor must satisfy in order to meet IRS business needs. These objectives meet the requirements of the Internal Revenue Manual[9] regarding establishing metrics for continuous monitoring. Similar to our Fiscal Year 2016 report, we found issues with the SLOs. Specifically, the SLOs do not clearly define how performance is guaranteed in key areas, including monitoring and incident management. Additionally, we found that the contractor failed to meet several SLOs.

SLOs

The ESS contract SLOs define maximum contractor response times for performance problems. During the Tax Day outage, the contractor failed to meet the SLO requirements for initial acknowledgement of the problem, creating a plan for resolution, and actual resolution of the problem. Additionally, the SLOs define mainframe availability (uptime), maximum unplanned downtime, and array performance average response times. As part of the ESS contract, if the contractor fails to perform the services within the time specified, the contractor shall pay to the Government liquidated damages. Figure 2 summarizes the ESS SLOs for Gold Storage Class and actual contractor performance in these areas.

[9] Internal Revenue Manual 10.8.1, *Information Technology Security, Policy, and Guidance* (July 8, 2015).

Figure 2: ESS SLO for Gold Storage Class

SLO	ESS Contract Requirement	Actual Contractor Performance
Contractor Acknowledgement of Performance Problems	30 minutes	Approximately 3 hours
Contractor Creates a Plan for Resolution	2 hours	Approximately 6.5 hours
Problem Resolution	4 hours	Approximately 11 hours
Mainframe Availability (Uptime)	99.999%	99.877%
Maximum Unplanned Downtime (Per Year)	Less than 26.5 minutes	Approximately 11 hours

Source: Treasury Inspector General for Tax Administration analysis of the ESS contract, outage documentation, and interviews conducted during fieldwork.

Although not defined by an SLO, the ESS contract also states that the contractor must deliver capacity management reports to the IRS on a monthly basis. These reports are the result of prior iterative testing to determine capacity limits. Further, the contract states that the contractor is required to maintain a buffer percentage of no less than 25 percent. We reviewed capacity reports from March 2017 through May 2017 and from March 2018 through May 2018 and found that the contractor failed to meet this contractual requirement. Figure 3 summarizes our review of the capacity management reports.

Figure 3: ESS Capacity Management Review

Report Time Period	Contract Buffer Percentage Requirement	Actual Buffer Percentage
March 2017	25%	11.69%
April 2017	25%	16.39%
May 2017	25%	13.37%
March 2018	25%	20.65%
April 2018	25%	20.88%
May 2018	25%	21.02%

Source: Treasury Inspector General for Tax Administration analysis of contractor's monthly capacity management reports.

Performance monitoring and incident management

The ESS contract states that the contractor shall acknowledge, plan, and resolve performance service failures 24 hours per day, seven days per week, and 365 days per year according to the SLO defined for each storage class. Because the IRS's Tier I storage arrays receive Gold Storage Class service, the contract requires initial acknowledgement of the reported failure within 30 minutes by the contractor sending an electronic trouble ticket to the IRS.

To satisfy the contractors' 24/7/365 service requirement, an embedded software program is used to monitor performance issues for both the mainframe computers and storage arrays. Once a performance issue is detected, the program generates an automated "call home" notification that includes an error code and associated severity level. On the morning of the Tax Day outage, the affected storage array made two automated "call home" notifications. Although the two error codes were different for the automated notifications, both were classified as Severity Level 3 issues.

Per IBM guidance, normal response time to a Severity Level 3 issue is by the end of the next business day. Due to this IBM guidance regarding response time, IBM never provided an acknowledgement of the performance issues and did not initiate any incident management procedures. Furthermore, IBM's stated response time to a Severity 1 issue (most critical) is within two hours, while the ESS contract mandates that the contractor provide the IRS with acknowledgement of performance issues within 30 minutes. These notifications would have alerted the IRS that there was a performance issue with one of the Tier 1 storage arrays. Following the outage, Unisys and the IRS started receiving all "call home" notifications simultaneously with IBM. Unisys now evaluates these notifications at its 24-hour Federal Help Desk. After evaluation of the notification, Unisys is supposed to escalate issues as needed and communicate with the IRS at least daily during a scheduled conference call. However, these interim procedures have not been formalized as part of the ESS contract.

More detailed SLOs for performance monitoring and incident management would strengthen the IRS's ability to ensure that the ESS contractor provides timely notification of any failures and demonstrates evidence that problems have been resolved or mitigated. Without such agreements, the IRS may be unable to determine contractor compliance with applicable policies and procedures that ensure system availability and protect sensitive taxpayer data.

Recommendations

The Chief Information Officer should:

Recommendation 4**:** Seek liquidated damages from the contractor per the ESS contract.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has sought liquidated damages from Unisys in accordance with ESS contract provisions.

Recommendation 5: Modify the ESS contract to require the contractor to provide the IRS with timely notifications of all alerts, to include "call home" events regardless of severity level.

> ***Management's Response:*** The IRS agreed with this recommendation. Enterprise Operations will modify the ESS contract to require the contractor to provide the IRS with notifications of all alert events regardless of severity level.

Recommendation 6: Modify the ESS contract to address specific risks affecting IRS systems related to ESS performance monitoring and incident management, including 24-hour system monitoring and detailed incident response processes.

> ***Management's Response:*** The IRS agreed with this recommendation. Enterprise Operations will modify the ESS contract to address specific risks affecting IRS systems related to ESS performance monitoring and incident management, to include 24-hour system monitoring and detailed incident response processes.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to analyze the IRS systems outage that occurred on April 17, 2018, and identify solutions to prevent future disruptions. To accomplish our objective, we:

I. Evaluated all aspects of the outage.

- A. Interviewed IRS personnel and contractors involved with identifying the outage and restoring the systems affected.
- B. Identified and obtained information about the mainframe[1] computers and software involved in the incident, including age.
- C. Determined how and when the incident was first identified.
- D. Developed a timeline that includes initial warning signs of an imminent outage, notifications or alerts, time of the actual outage, when IRS personnel were first alerted about a warning or the actual outage, and time of resolution.
- E. Obtained and reviewed the Computer Security Incident Response Center incident report and outage assessment.
- F. Identified all affected systems and their outages.
- G. Identified the cause of the outage, including any one or more of the following: firmware, software, or hardware issue; known bugs; capacity management issues; or other causes.

II. Determined whether the IRS could have prevented the outage.

- A. Determined that there was a known update for the firmware bug that was not applied. We also:
  1. Determined when the update was first available to the IRS.
  2. Determined who made the decision to not apply the update and when the decision was made.
  3. Determined whether the decision was documented in a formal risk-based decision.
  4. Obtained and reviewed decision documentation.

[1] See Appendix V for a glossary of terms.

B. Reviewed capacity management of the IRS mainframes.

1. Identified capacity management requirements and procedures for the mainframes.

III. Evaluated the IRS response to the outage, including the timeliness of resumed system operations.

A. Reviewed any IRS contingency plans and procedures for dealing with an incident causing widespread outages and recovery.

1. Determined whether the IRS declared this outage a major outage per the Major Outage SOP.

2. Identified and interviewed the Incident Commander.

3. Evaluated IRS compliance with plans, requirements, and procedures.

4. Reviewed disaster recovery procedures for failover, backup, or redundancy between the Enterprise Computing Centers at Martinsburg, West Virginia, and Memphis, Tennessee.

B. Reviewed documented lessons learned.

C. Evaluated whether the affected systems have ongoing vulnerabilities.

D. Determined whether the IRS has taken or should take any actions to prevent a future outage.

IV. Evaluated the impact of the system outage.

A. Determined whether there is any backlog of returns requiring delayed processing.

B. Determined the total hours of downtime.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Office of Management and Budget guidance on incident response lessons learned; IRS SOPs relating to incident management and major outages; Internal Revenue Manual policies addressing information technology security and Service-wide patch management. We evaluated these controls by interviewing IRS personnel and contractors and reviewing relevant documentation provided by the IRS. We also developed a timeline of events and identified the root cause of the Tax Day outage. Additionally, we examined the ESS contract to determine contractor compliance with stated SLO and other contractual requirements.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
John L. Ledford, Director
Jena Whitley, Audit Manager
Mike Curtis, Lead Auditor
Joan Bonomi, Senior Auditor
Nicholas Reyes, Senior Auditor
Andrea Nowell, Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Chief Information Officer
Chief, Procurement
Commissioner, Wage and Investment Division
IRS Human Capital Officer
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Strategy and Planning
Director, Office of Audit Coordination

Appendix IV

Tax Day Outage Timeline

Date/Time	Description of Event
June 2017	IBM initially discovered the firmware bug associated with the IRS Tax Day outage in a test laboratory.
Nov. 2017	IBM released a Microcode Bundle 88.24.6.0, which included a patch for the firmware bug identified in June 2017.
Dec. 2017	The IRS concurs with a Unisys decision to continue with Microcode Bundle 88.23.20.0 for the 2018 Filing Season because it was considered a more stable version (based on the relatively recent release date of Microcode Bundle 88.24.6.0, which failed to meet Unisys's requirement of 450 machine weeks in a production environment).
Jan. 2018	Another IBM client experienced an outage triggered by the firmware bug previously discovered in June 2017. IBM product engineers developed and deployed a script that monitored and corrected the bug issue for the affected client. After this event, IBM made no efforts to communicate this condition to the IRS or notify the IRS about the preventative script it had developed that would have prevented the Tax Day outage.
Apr. 17, 2018 2:24 a.m.	The ITOCC received the first system-generated error messages and invoked its established procedures to troubleshoot the problem.
2:57 a.m.	Storage array 75FZB70, located at the Martinsburg Computing Center, generated a "call home" notification for the first time (IBM Problem Management Record Ticket #66780).
3:00 a.m.	The ITOCC Incident Management Section Technician informed the IRS's Chief, Mainframe Support Branch, about a performance issue with one of the mainframes.
3:30 a.m.	KISAM Incident Management Ticket # 00222120 was opened as a Priority II.
4:45 a.m.	Storage array 75FZB70 generated a second "call home" notification with a different error code (IBM Problem Management Record Ticket #66783).
4:45 a.m.	Per the ITOCC Incident Management SOP, the ITOCC initiated an Incident Management call (investigation).

Date/Time	Description of Event
5:43 a.m.	The ITOCC contacted Unisys for storage support related to the current incident.
5:45 a.m.	Per the Incident Management SOP, the ITOCC initiated an Incident Management call. ESS contractors, Unisys and IBM, joined the call at 6:45 a.m.
5:56 a.m.	After receiving a call from the ITOCC, Unisys manually opened a Severity 1 IBM Problem Management Record Ticket (#58435) with IBM.
6:20 a.m.	The IRS Chief, Data Storage and Protection Branch, notified the Unisys ESS Program Manager of the outage.
6:38 a.m.	KISAM Incident Management Ticket # 00222120 was upgraded from Priority II to Priority I.
6:45 a.m.	Unisys contractors joined the IRS Incident Management call. The ITOCC designated the Incident Manager of Record as part of the Incident Management SOP and worked through several service restoration phases (investigation, assessment, and technical).
6:45 a.m.	The IRS determined that the mainframe outage was related to the storage array.
7:11 a.m.	The Information Technology Continuity Management Office added the incident to the Toolkit Suite With Command Centre.
7:44 a.m.	The Toolkit Suite With Command Centre identified 59 tax systems, including the MeF system, affected by the storage array issue and created and distributed a report to the incident management team.
8:15 a.m.	A daily conference call with the Chief Information Officer and all Associate Chief Information Officers was held: • Due to a previously planned meeting at IRS Headquarters, several other IRS executives joined this call. • The Enterprise Computing Center Director stated that the technicians were still troubleshooting and reviewing logs. • The team knew the outage related to the storage array but could not determine its extent or if it involved hardware or firmware. • Executives discussed the possibility of moving operations to Memphis (enacting the Disaster Recovery Plan). • The primary directive from the IRS executive level was to have contractors involved to resolve the issue in Martinsburg.

Date/Time	Description of Event
8:46 a.m.	An IRS Quick Alert was issued (a message to electronic filing software providers): ***Subject:*** *MeF Is Unavailable* *The MeF Assurance Testing System and Production systems are unavailable. A Quick Alert will be issued when the systems are back online.* *Thank you in advance for refraining from accessing the MeF Systems during this period.*
9:20 a.m.	The ITOCC coordinated an Incident Management call. • Participants determined that the incident was a Major Outage and designated the Enterprise Computing Center Director as the Major Outage Incident Commander.
9:41 a.m.	A joint conference call with IRS, Unisys, and IBM was held to discuss repair options. IBM presented three options to the IRS: • Clear cache from the affected storage array, restart the mainframe, and install a script that would serve as a monitoring tool. [the IRS selected this option.] • Install Microcode Bundle 88.24.6.0. • Remove FlashCopy use.
9:45 – 10:50 a.m.	IBM product engineers performed the steps to clear out the cache from the affected storage array, followed by a 19-step process to restart the mainframe.
12:45 p.m.	IBM product engineers remotely logged in to the system and deployed the script that monitored and cleared the cache issue.
12:51 p.m.	IRS held an Incident Management call to discuss the deployed script, and participants decided to bring the mainframes back online.
1:00 p.m.	The Incident Commander finalized a Controlled Launch plan with the Commissioner, Wage and Investment Division, to initially control the volume of incoming returns in an effort to prevent a possible second outage due to system overload.
1:39 p.m.	The IRS alerted participating Electronic Return Originators to prepare to submit returns per the Controlled Launch plan.
1:40 p.m.	All IRS mainframes, databases, and regions were back online and available for processing returns.
3:00 p.m.	The IRS began receiving tax returns as part of the Controlled Launch period.

Date/Time	Description of Event
4:47 p.m.	A second IRS Quick Alert was issued: ***Subject:*** *MeF Is Available* *Attention: Software Developers, Transmitters, and States.* *The MeF Assurance Testing System and Production systems are now available. We apologize for any inconvenience.*
4:49 p.m.	A message sent to throttle participants stated that there were no longer any volume constraints and to resume normal processing.
5:00 p.m.	The IRS decided to add an additional day to the tax filing deadline.
6:29 p.m.	Incident status was changed from *Work in Progress* to *Resolved*.
6:46 p.m.	The IRS issued a press release informing the public of an additional day to file.
Apr. 18, 2018 12:45 a.m.	The backlog of returns peaked at 2.3 million.
5:30 a.m.	The system backlog of returns was cleared.

Source: Treasury Inspector General for Tax Administration analysis based on interviews conducted with IRS employees and contractors and by reviewing procedures and documentation obtained throughout fieldwork.

Appendix V

Glossary of Terms

Term	Definition
Buffer	A temporary storage place for data before it is transferred to another location.
Cache	Stores recently used information so that it can be quickly accessed at a later time. Computers incorporate several different types of caching in order to run more efficiently, thereby improving performance.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Firmware	Software instructions residing in nonvolatile memory chips that hold their content without power. Firmware is found on computer motherboards to hold hardware settings and booting data and on a myriad of consumer electronics devices to hold the operating system or control program.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Flash Copy	A process that creates an instant copy of a volume at a specific point-in-time, which is why it is often referred to as Point-in-Time Copy, instantaneous copy or time zero (t0) copy. Flash Copy is a hardware (storage system based) function that the software invokes.
Incident Management	The process for managing incidents with the goal of restoring service as quickly as possible and minimizing the adverse impact on the customer.
Information Technology Operations Command Center	Serves as the Information Technology organization's first line of defense by executing Event Management, Incident Management, and Problem Management activities on the IRS's mainframes, servers, and the enterprise network.
Machine Week	The number of boxes with the code installed multiplied by how many weeks the code has been running.
Mainframe	A powerful, multiuser computer capable of supporting many hundreds of thousands of users simultaneously.

Term	Definition
Microcode	The lowest specified level of processor and machine instruction sets. It is a layer comprised of small instruction sets, which are derived from machine language. Microcode performs short, control-level register operations, including multiple microinstructions, each of which performs one or more microoperations.
Modernized e-File	An IRS system that receives and processes tax returns in an Internet environment.
Petabyte	A unit of computer memory or data storage capacity equal to 1,024 terabytes.
Priority 1 Incident	Priority is based on impact and urgency and is used to identify required times for actions to be taken. Priority 1 is a critical ranked incident with an immediate target response time and four-hour target resolution time.
Priority 2 Incident	Priority is based on impact and urgency and is used to identify required times for actions to be taken. Priority 2 is a high-ranked incident with a one-hour target response time and eight-hour target resolution time.
Storage Array	A data storage system that is used for block-based, file-based, or object storage.
Terabytes	A unit of measure used to describe memory and disk capacity that is equal to approximately 1 trillion bytes or 1,024 gigabytes. It is also equivalent to approximately 500,000,000 pages of text.
Tier 1	Computing infrastructure consisting of mainframe computers that handle a high volume of critical operational data.
Toolkit Suite With Command Centre	IRS enterprise-level repository and incident management decision support tool and plan repository for Business Continuity and Disaster Recovery.
Warmstart	Synonymous with warmboot. Reloading the operating system by performing a restart operation from the computer's main menu while it is still turned on. The warm boot does not turn the power off and back on, and it does not clear memory.

Appendix VI

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF INFORMATION OFFICER

SEP 0 4 2018

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report – Review of the System Failure that Led to the Tax Day Outage (#201820027) (e-trak # 2018-05474)

Thank you for the opportunity to review your draft audit report and to discuss the report observations with the audit team. The IRS is committed to delivering a complete and timely filing season, while ensuring the security and availability of our information technology systems.

We are encouraged the report recognizes how we effectively responded to the Tax Day outage and timely resumed individual tax return and payment processing. While any service disruption is not ideal, we believe the Tax Day outage demonstrated our improved ability to rapidly and successfully respond to major incidents. The quick response to this incident and subsequent processing of almost 4 million individual returns by midnight the same day is a testament to the talented and dedicated staff IRS employs. It should also be noted that we reduced downtime from a similar event in 2016 that had a 30 hour recovery time to 11 hours. This is significant and demonstrates our commitment to process improvements.

We continue to develop and implement new technologies, refine our processes and conduct robust testing. Since the outage:

- We have established a process to collect and consolidate all documents pertaining to a major outage and updated the Major Outage SOP accordingly.
- We formalized the monthly microcode bundle meetings with the vendor to include documenting meeting participants, meeting minutes, decisions and discussions of risks identified in the Release Notes for the current microcode.
- We are receiving all "call home" notifications simultaneously with IBM.
- We are taking steps to strengthen our site resilience to further reduce downtime.

Over the course of the audit period, the IRS and TIGTA teams engaged in multiple review sessions and conversations. The report is an accurate reflection of those conversations.

We are committed to continuously improving our information technology strategies, systems, and processes. The continued support, assistance, and guidance your team provides is very valuable to us in this regard. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Karen Mayr at (202) 368-8396.

Attachment

Recommendation 1: Ensure that the Director, Security Operations and Standards Division, collects and formally documents in one consolidated action plan any lessons learned for all major outages and implements the approved corrective action plan per the Major Outage SOP.

CORRECTIVE ACTION #1: We agree with this recommendation. Enterprise Operations has created a process that will be used to collect and document a consolidated action plan in accordance with the updated Major Outage SOP.

IMPLEMENTATION DATE: February 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

Recommendation 2: Formalize the monthly microcode bundle meetings with IBM and Unisys to include documenting meeting participants, detailed meeting minutes, and discussions of risks identified in the release notes for the current microcode updates.

CORRECTIVE ACTION #2: We agree with this recommendation. We formalized the monthly microcode bundle meetings which includes documenting meeting participants, meeting minutes, decisions and discussions of risks identified in the Release Notes for the current microcode upgrades.

IMPLEMENTATION DATE: August 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: N/A

Recommendation 3: Ensure that all decisions to not install the latest microcode bundle updates are documented and approved by the system Authorizing Official.

CORRECTIVE ACTION #3: We agree with this recommendation. We will implement a process to ensure that the Authorizing Official and responsible directors are aware of the content of the microcode bundles updates and approve decisions to not install.

IMPLEMENTATION DATE: February 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

Recommendation 4: Seek liquidated damages from the contractor per the ESS contract.

CORRECTIVE ACTION #4: We agree with this recommendation. We have sought liquidated damages from Unisys in accordance with ESS contract provisions.

IMPLEMENTATION DATE: August 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: N/A

Recommendation 5: Modify the ESS contract to require the contractor to provide the IRS with timely notifications of all alerts, to include "call home" events regardless of severity level.

CORRECTIVE ACTION #5: We agree with this recommendation. Enterprise Operations will modify the ESS contract to require the contractor to provide the IRS with notifications of all alert events regardless of severity level.

IMPLEMENTATION DATE: February 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.

Recommendation 6: Modify the ESS contract to address specific risks affecting IRS systems related to ESS performance monitoring and incident management, including 24-hour system monitoring and detailed incident response processes.

CORRECTIVE ACTION #6: We agree with this recommendation. Enterprise Operation will modify the ESS contract to address specific risks affecting IRS systems related to ESS performance monitoring and incident management, to include 24-hour system monitoring and detailed incident response processes.

IMPLEMENTATION DATE: February 15, 2019

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them monthly until completion.