TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Information Technology: Improvements Are Needed in Enterprise-Wide Disaster Recovery Planning and Testing

June 1, 2017

Reference Number: 2017-20-024

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.treas.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.

INFORMATION TECHNOLOGY: IMPROVEMENTS ARE NEEDED IN ENTERPRISE-WIDE DISASTER RECOVERY PLANNING AND TESTING

Highlights

Final Report issued on June 1, 2017

Highlights of Reference Number: 2017-20-024 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

Disaster recovery is the ability of an organization to respond to a disaster or an interruption in computing services. During Fiscal Year 2015, the IRS reported that it processed more than 244 million tax returns and collected more than $3.3 trillion in taxes. Because the IRS depends heavily on computer systems to carry out its mission, the IRS is required to continue mission-essential functions in the event of an emergency or resume them rapidly after a disruption of normal activities.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS has a complete and adequate disaster recovery planning and testing capability that allows the IRS to recover major computer systems and applications from its Enterprise Computing Centers in a time frame that satisfies established business needs and priorities.

WHAT TIGTA FOUND

The IRS has identified three mission-essential functions: Process Remittances, Process Tax Returns, and Process Refunds. To identify disaster recovery priorities for the orderly recovery of systems and applications supporting mission-essential functions, an enterprise-wide business impact analysis is needed. Recovery priorities do not exist within the top three critical business processes and by location.

The IRS has identified recovery time objectives for its 140 individual Federal Information Security Modernization Act systems and applications. However, it has not identified maximum tolerable downtimes or recovery time objectives for the agency's mission-essential functions. Further, disaster recovery planning and testing processes have not verified that actual recovery time frames can satisfy business needs. The IRS has determined actual recovery times for only 18 of its 51 identified systems and applications supporting mission-essential functions. Further, while functional exercises of 35 moderate-availability systems and applications supporting mission-essential functions include an element of system recovery, due to the critical nature of these systems, more robust testing is recommended.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer complete the enterprise-wide business impact analysis; collaborate with the IRS business operating divisions to prioritize the recovery of systems and applications within the top three critical business processes and by location and to establish the maximum tolerable downtimes for mission-essential functions; verify that the IRS Information Technology organization is able to recover mission-essential functions within the maximum tolerable downtimes; and implement policy to ensure that functional tests of moderate-availability systems and applications supporting mission-essential functions are designed to test functional aspects of their information system contingency plans that are consistent with the priority of the system and application.

The IRS agreed to ensure authoritative identification mapping is regularly distributed enterprise-wide and to collaborate with IRS business operating divisions on the maximum tolerable downtimes for mission-essential functions. The IRS partially agreed to update its business impact analysis methodology documentation and partially verify its ability to recover mission-essential functions within the maximum tolerable downtimes. The IRS disagreed with three other recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

June 1, 2017

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Information Technology: Improvements Are Needed in Enterprise-Wide Disaster Recovery Planning and Testing (Audit # 201520014)

This report presents the results of the subject audit report. The overall audit objective was to determine whether the Internal Revenue Service (IRS) has a complete and adequate disaster recovery planning and testing capability that allows the IRS to recover major computer systems and applications from its Enterprise Computing Centers in a time frame that satisfies established business needs and priorities. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

FISMA	Federal Information Security Modernization Act
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
NIST	National Institute of Standards and Technology
TIGTA	Treasury Inspector General for Tax Administration
TSCC	Toolkit Suite With Command Centre

Background

Because the Internal Revenue Service (IRS) depends heavily on computer systems to carry out its mission, continuous operation of computing services supporting mission-essential functions is required under all circumstances. During Fiscal Year[1] 2015, the IRS reported that it processed more than 244 million tax returns and collected more than $3.3 trillion in taxes, representing 93 percent of the Federal Government's receipts. In addition, Congress, the Department of the Treasury, tax professionals, taxpayers, and other Government agencies also need data and services provided by IRS systems.

The IRS Information Technology (IT) Cybersecurity organization is responsible for ensuring IRS compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data. Within the Cybersecurity organization, there are the divisions of Security Risk Management and Architecture and Implementation. The Security Risk Management Division is responsible for providing guidance and direction to the IRS enterprise-wide disaster recovery efforts as well as a comprehensive, business-centric Information Technology Service Continuity Management Program designed to protect IRS operations, assets, and information. The Architecture and Implementation Division is responsible for coordinating the efforts of the enterprise-wide Information Technology Service Continuity Management Program.

The IRS IT Enterprise Operations organization functions to deploy and maintain a computing infrastructure capable of supporting the business and administrative needs of the IRS. The Enterprise Operations' Enterprise Computing Centers provide production-processing support for business applications across all production environments and manages the IRS server infrastructure in all environments. The IRS has two Enterprise Computing Centers, which are located in Martinsburg, West Virginia and Memphis, Tennessee. The Enterprise Operations organization performs scheduled information system contingency planning exercises for various IRS applications and systems and two annual disaster recovery tests of its Enterprise Computing Centers' mainframes and associated mainframe applications identified in the related test scenarios.

According to the National Institute of Standards and Technology (NIST),[2] an organization must have the ability to withstand hazards and sustain its mission through environmental changes. These changes can be gradual, such as economic or mission changes, or sudden, as in a disaster event. Rather than just working to identify and mitigate threats, vulnerabilities, and risks,

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

[2] NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).

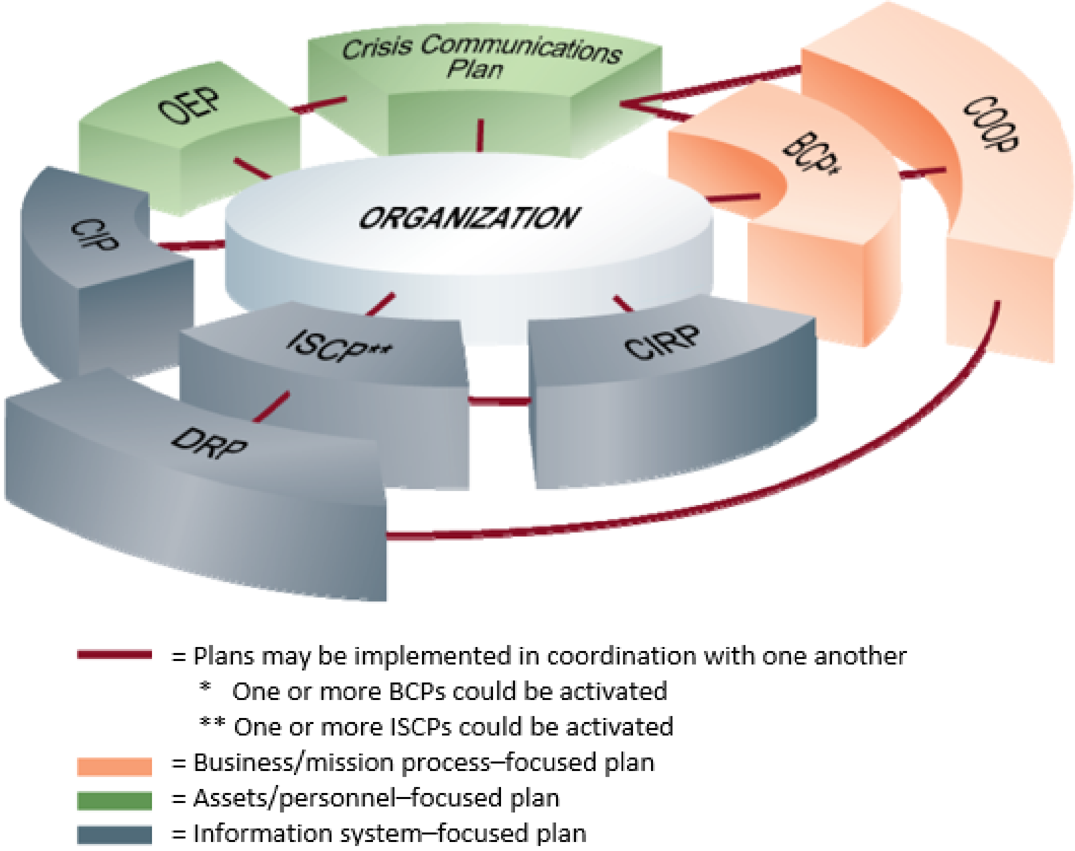
organizations can work toward building a resilient infrastructure, minimizing the impact of any disruption on mission-essential functions. Resilience is the ability to quickly adapt and recover from any known or unknown changes to the environment. The goal of a resilient organization is to continue mission-essential functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions. Risk management, contingency, and continuity planning are individual security and emergency management activities that agencies can implement in a holistic manner across an organization as components of a resiliency program.

Disaster recovery is the ability of an organization to respond to a disaster or an interruption in computing services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions. Disaster recovery is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, computer operations, and data. The goal of the IRS's disaster recovery program is to continually improve the IRS's ability to adapt to changes, risks, and unexpected events that can affect its ability to continue its critical business processes and mission.

The NIST states that a disaster recovery plan applies to major, usually physical, disruptions to service that deny access to the primary facility infrastructure for an extended period. A disaster recovery plan is an information system–focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The disaster recovery plan addresses information system disruptions that require relocation. Multiple information system contingency plans may support the disaster recovery plan to address recovery of affected individual systems once the alternate facility has been established. An information system contingency plan provides established procedures for the assessment and recovery of a system following a system disruption. The information system contingency plan provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system.

Different from a disaster recovery plan, the information system contingency plan's procedures are for recovery of the system regardless of site or location. An agency can activate an information system contingency plan at the system's current location or at an alternate site. In contrast, a disaster recovery plan is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. Once the disaster recovery plan has successfully transferred an information system's processing site to an alternate site, each affected system would then use its respective information system contingency plan to restore, recover, and test systems. Figure 1 shows the relationship of various contingency-related plans that an agency can implement across an organization.

Figure 1: Contingency-Related Plans


Crisis Communications Plan
OEP
COOP
BCP*
CIP
ORGANIZATION
ISCP**
CIRP
DRP
= Plans may be implemented in coordination with one another
* One or more BCPs could be activated
** One or more ISCPs could be activated
🟧 = Business/mission process–focused plan
🟩 = Assets/personnel–focused plan
⬛ = Information system–focused plan

Source: NIST Special Publication 800-34 Rev. 1, BCP – Business Continuity Plan, CIP – Critical Infrastructure Protection, CIRP – Cyber Incident Response Plan, COOP – Continuity of Operations Plan, DRP – Disaster Recovery Plan, ISCP – Information Systems Contingency Plan, OEP – Occupant Emergency Plan.

Backup and recovery strategies are a means to restore system operations quickly and effectively following a disruption in computer operations. The IRS has implemented various backup and recovery strategies such as asynchronous replication, virtual tape replication, and traditional tape backup. Asynchronous replication provides near–real-time remote mirroring for disaster recovery and backup. Virtual tape replication provides the ability for virtual tape datasets to be replicated from one site to the disaster recovery site over IRS networks. Certain applications within the IRS continue to use traditional tape backup solutions.

This review was performed at the New Carrollton Federal Building in Lanham, Maryland, and the IRS Enterprise Computing Center in Martinsburg, West Virginia, during the period August 2015 through July 2016. 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.

Results of Review

An Enterprise-Wide Business Impact Analysis Is Needed to Identify Disaster Recovery Priorities for the Orderly Recovery of Systems and Applications Supporting Mission-Essential Functions

The Treasury Inspector General for Tax Administration (TIGTA) reviewed key disaster recovery controls to determine whether the IRS has a complete and adequate disaster recovery planning capability that allows it to recover major computing systems and applications from its Enterprise Computing Centers in a time frame that satisfies established business needs and priorities. Our review considered whether the IRS has adequately prioritized the recovery of its information systems and if the IRS IT organization is able to recover systems and applications within an acceptable time to satisfy business needs.

Our review found:

- An absence of a current enterprise-wide business impact analysis.
- A need for current and consistent mapping of mission-essential functions to supporting information technology systems and applications.
- The lack of recovery priorities for recovering systems and applications supporting mission-essential functions.

According to the Internal Revenue Manual[3] (IRM), the IRS's mission-essential functions directly relate to accomplishing the mission of the organization. Generally, a mission-essential function is unique to the agency, *i.e.*, most other agencies do not perform this function. An agency's mission-essential functions provide vital services, exercise civil authority, maintain the health and safety of the public, and sustain the economic/industrial base during a disruption of normal operations. The IRS has identified the following three mission-essential functions:

1. Process Remittances – The remittance process involves the receipt of payments, fees, and other monies through submission processing and includes the deposit of funds along with all necessary accompanying payment data to the Department of the Treasury.
2. Process Tax Returns – The tax return process involves the receipt, sorting, coding, and archiving of all tax returns, electronic and paper. For electronic return data, it includes validate, accept/reject, and acknowledge receipt. For paper submissions, it includes receipt, extract and batch/sort, code/edit, and capture as well as archive and manage the paper files.

[3] IRM 10.6.1, *Continuity Operations Program - Continuity Planning Requirements* (March 2014).

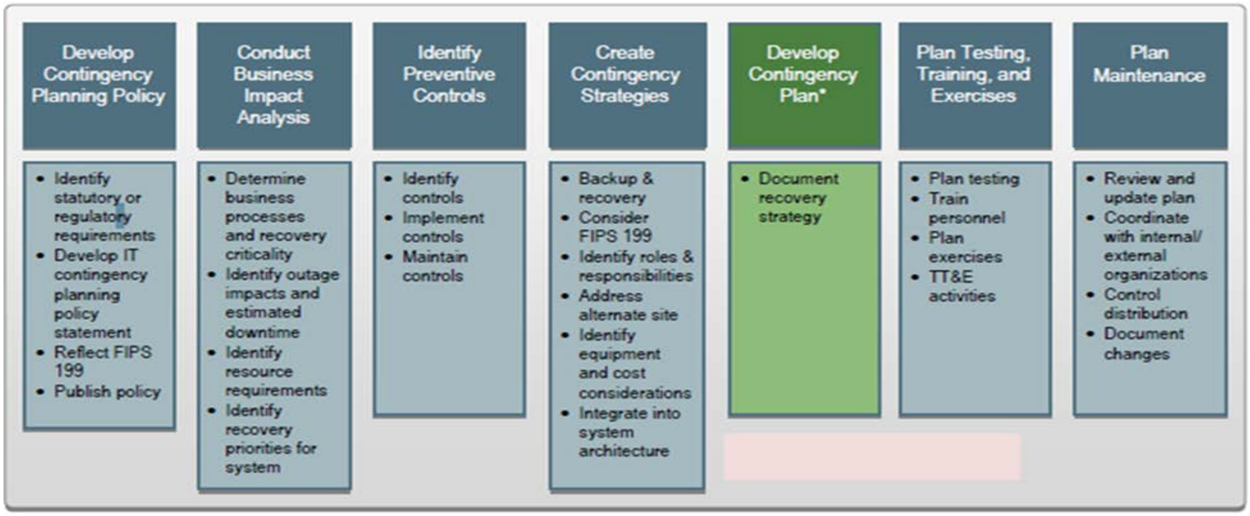
3. Process Refunds – The refund process involves performing the final calculations and verifications to settle taxpayers' accounts, including disposition-based information, exception reports, posting offsets, and sending refund information for issuance.

The three mission-essential functions also comprise three of the IRS's critical business processes. The IRS defines critical business processes as essential or critical operational and/or business support processes or functions that cannot be interrupted or unavailable for more than a mandated or predetermined time frame without significantly jeopardizing the operation of the organization. IRS IT Enterprise Operations personnel explained that the IRS numbers the critical business processes in order of business importance. The three IRS mission-essential functions above are referred to as critical business processes 1, 2, and 3, respectively.

IRS policy[4] requires a comprehensive and effective continuity program. The primary goal of continuity planning is to ensure the continuation of IRS mission-essential functions under all circumstances. Meeting this goal requires the development of comprehensive plans, procedures, and provisions for alternate facilities, personnel, resources, interoperable communications, and vital records.

Figure 2 provides a seven-step contingency planning process for developing and maintaining a viable contingency planning program provided by the NIST.

Figure 2: Contingency Planning Process



Develop Contingency Planning Policy	Conduct Business Impact Analysis	Identify Preventive Controls	Create Contingency Strategies	Develop Contingency Plan*	Plan Testing, Training, and Exercises	Plan Maintenance
• Identify statutory or regulatory requirements • Develop IT contingency planning policy statement • Reflect FIPS 199 • Publish policy	• Determine business processes and recovery criticality • Identify outage impacts and estimated downtime • Identify resource requirements • Identify recovery priorities for system	• Identify controls • Implement controls • Maintain controls	• Backup & recovery • Consider FIPS 199 • Identify roles & responsibilities • Address alternate site • Identify equipment and cost considerations • Integrate into system architecture	• Document recovery strategy	• Plan testing • Train personnel • Plan exercises • TT&E activities	• Review and update plan • Coordinate with internal/ external organizations • Control distribution • Document changes

Source: NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems (May 2010).

[4] IRM 10.6.1, *Continuity Operations, Continuity Planning Requirements* (March 2014).

NIST[5] guidance states that a business impact analysis enables information system contingency plan owners to identify their mission/business processes, related system components, and interdependencies. The purpose of this analysis is to map the critical mission/business processes and services to the related information systems and, based on that information, characterize the consequences of a disruption in computing services. Part of the business impact analysis is the identification of recovery priorities for system resources. Recovery priorities can be effectively established taking into consideration mission/business process criticality, outage impacts, tolerable downtimes, and system resources. An agency could establish priority levels for sequencing recovery activities and resources.

IRM policy[6] further states that the enterprise-wide business impact analysis serves as a core initiative to determine recovery priorities for all IRS applications supporting critical business processes. The IRS should use data gathered during the enterprise-wide business impact analysis to establish recovery priorities within systems, applications, and the enterprise.

To describe its current methodology for completing a business impact analysis, the IRS provided the following document entitled, *IRS Enterprise Business Impact Analysis Methodology, Version 1.1, (not dated)*. This document states that the business impact analysis provides the rationale for prioritizing applications recovery for a given location following a catastrophic disruption. The methodology stated that the IRS should maintain the business impact analysis on an ongoing basis to reflect any major changes in IRS systems, applications, or locations.

The IRS also provided its 2008 Enterprise-Wide Business Impact Analysis document for our review. However, the IRS has not updated this important control document since 2008. This outdated analysis identified the effect that disruptions to computing services could have on the IRS's ability to perform critical business processes and it mapped the critical business processes by:

- Information technology systems and applications covered by the Federal Information Security Management Act of 2002.[7]
- Business unit.
- Host location (Enterprise Computing Center).

The 2008 Enterprise-Wide Business Impact Analysis also provided a numerical recovery prioritization of the 2008 Federal Information Security Management Act of 2002 systems and applications by:

[5] NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).
[6] IRM 10.8.60, *Information Technology (IT) Security - IT Service Continuity Management (ITSCM) Policy and Guidance* (December 2013).
[7] Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899.

1. Critical business process (application priority within each critical business process).
2. Location (Enterprise Computing Center).
3. Enterprise (rank recovery order of all applications and systems).

The Federal Information Security Management Act of 2002 was enacted to strengthen the security of information and information systems within Federal agencies. The Act requires Federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or entity. An amendment to the Federal Information Security Management Act of 2002 was signed into law, called the Federal Information Security Modernization Act of 2014 (FISMA).[8] It provides several modifications to the Federal Information Security Management Act of 2002 that modernize Federal security practices to address current security concerns. The modifications will improve security by transitioning agencies away from paperwork requirements toward a more automated and continuous security posture. The FISMA requires each agency to develop, document, and implement an agency-wide information security program that includes plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. At the time of our review, the IRS identified 140 information technology general support systems and applications within its FISMA Master Inventory.

The IRS explained that it had not completed and thus could not provide a current or complete enterprise-wide business impact analysis due in part to personnel turnover, having to transfer data from a contractor to the IRS, and a subsequent change in database products. The IRS informed us that it was updating its enterprise-wide business impact analysis data. Cybersecurity officials stated that the IRS is streamlining a repeatable process to validate the business impact data annually.

In addition, the IRS initially provided three different lists mapping its mission-essential functions to the supporting information technology systems and applications. Our analysis found inconsistencies between the lists in the detailed mapping of systems and applications to the mission-essential functions, and inconsistencies existed in the total number of systems and applications that were identified as supporting mission-essential functions. Cybersecurity personnel provided lists on August 13, 2015, and September 4, 2015. Enterprise Operations personnel provided a list on October 30, 2015. On January 19, 2016, Cybersecurity and Enterprise Operations personnel provided a fourth list that detailed the systems and applications by critical business process, including the mission-essential functions.

The IRS uses the Information System Contingency Plan Testing Schedule to map IRS systems and applications to critical business processes, business owners of systems and applications, and

[8] Pub. L. No. 113-283, 128 Stat. 3073.

host locations (production/recovery/development). The IRS stated that recovery priorities are reflected in the mapping of the systems and applications to critical business processes, where critical business processes are ranked in sequential order. For example, critical business process 1 is more important than critical business process 2. However, the IRS stated that recovery priorities do not exist by location or within each critical business process.

By not maintaining a current enterprise-wide business impact analysis, the IRS does not have reliable information to guide its disaster recovery restoration priorities. The lack of a current and consistent mapping of the IRS's critical business processes to the supporting information technology systems and applications could result in identifying incorrect and incomplete systems and applications necessary to support the IRS's critical business processes. Lastly, without recovery prioritizations of its current FISMA systems and applications for each location, operational guidance may not be sufficient to allow the IRS IT organization to efficiently recover systems and applications, especially mission-essential functions, in the event of a disruption to computing services.

Recommendations

The Chief Information Officer should:

Recommendation 1: Complete the enterprise-wide business impact analysis in accordance with the IRS business impact analysis methodology.

> **Management's Response:** The IRS partially agreed with this recommendation. Although its business impact analysis processes are current, the documentation is outdated. The IRS will document the methodology appropriately.
>
> **Office of Audit Comment:** IRM policy[9] states that the enterprise-wide business impact analysis serves as a core initiative to determine recovery priorities for all IRS applications supporting critical business processes. The IRS has not completed a current enterprise-wide business impact analysis. As a result, the IRS does not have reliable information to guide its disaster recovery restoration priorities. In addition to documenting its business impact analysis methodology, the IRS needs to use the methodology to complete an enterprise-wide business impact analysis.

Recommendation 2: Enhance the IRS process of identifying the applications and systems that support the mission-essential functions to ensure the authoritative identification mapping is distributed enterprise-wide on a defined and regular basis.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity organization will implement a tool to ensure the authoritative identification mapping is distributed enterprise-wide and on a regular basis.

[9] IRM 10.8.60.4.3(7), *Information Technology Business Impact Analysis* (December 2013).

Recommendation 3: Collaborate with the IRS business operating divisions at least annually to identify the relative recovery priorities of systems and applications and maintain the proper list of applications restoration order for critical business processes 1 through 3 and by location.

> **Management's Response:** The IRS disagreed with this recommendation. The IT organization collaborates with the business operating divisions annually and maintains a list of applications and restoration priorities. The IRS will continue to determine the restoration order of applications as appropriate for the environment.
>
> **Office of Audit Comment:** The IRS has not completed a current enterprise-wide business impact analysis showing recovery priorities of the systems and applications supporting its mission-essential functions. Without recovery prioritizations of its current FISMA systems and applications for each location, operational guidance may not be sufficient to allow the IRS IT organization to efficiently recover systems and applications, especially mission-essential functions, in the event of a disruption to computing services.

Maximum Tolerable Downtimes for Mission-Essential Functions Have Not Been Identified or Verified to Ensure That Business Needs Can Be Met

According to the NIST,[10] an agency needs to establish maximum tolerable downtimes to provide contingency planners with direction on selecting appropriate recovery strategies and methods and provide the detail needed to develop recovery procedures. Maximum tolerable downtime is the total amount of time the system owner or authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations. The maximum tolerable downtime consists of two elements: 1) recovery time objective and 2) work recovery time. The recovery time objective is the maximum amount of time a system resource can remain unavailable before there is an unacceptable impact on other system resources and supported mission/business processes. Work recovery time is the period of time it takes an agency to recover and run critical business functions once the agency restores the systems.

Maximum tolerable downtimes for mission-essential functions have not been identified

For disaster recovery planning purposes, the IRS uses application recovery time objectives, not maximum tolerable downtimes. According to Cybersecurity officials, the IRS system and application owners in the business operating divisions calculate recovery time objectives for each of its 140 FISMA information technology systems and applications. However, the Cybersecurity organization and the IRS business operating divisions have not determined the maximum

[10] NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).

tolerable downtimes or recovery time objectives the business operating divisions are willing to accept for the top three critical business processes, (*i.e.*, remittance processing, tax return processing, and refund processing) that represent the IRS mission-essential functions.

As a result, neither maximum tolerable downtimes nor recovery time objectives have been identified for the IRS's mission-essential functions. Therefore, the IRS IT organization does not know how long the IRS business operating divisions are willing to function without mission-essential functions. Further, due to the IRS's practice of identifying and managing recovery time objectives for each individual system and application, sufficient information is not available to IRS IT management to enable them to manage an enterprise disaster recovery program effectively.

Disaster recovery planning and testing processes have not verified that actual recovery time frames for mission-essential functions satisfy business needs

IRM 10.6.1[11] states that the IRS should continue mission-essential functions in the event of an emergency or resume rapidly after a disruption of normal activities. The IRS has identified three mission-essential functions that it performs—processing tax remittances, processing tax returns, and processing refunds. These three mission-essential functions are also included in the list of the IRS's critical business processes. The IRS defines critical business processes as essential or critical operational and/or business support processes or functions that cannot be interrupted or unavailable for more than a mandated or predetermined time frame without significantly jeopardizing the operation of the organization.

The IRS defines Tier 1 systems to include mainframe hardware, software, maintenance, and data processing services. The IRS defines Tier 2 systems as minicomputer hardware, software, maintenance, and data processing services for computers usually containing multiple microprocessors, capable of executing multiple processes simultaneously, and which may serve multiple users by way of a communications network. The IRS explained that for Tier 2 applications, it only needs to recover the host servers and does not need to recover all Tier 2 servers within the general support system infrastructure.

We analyzed IRS actual recovery times provided on March 8, 2016. At that time, the IRS identified 51 systems and applications that supported mission-essential functions. Our review found that the IRS only had actual recovery times for 18 of 51 systems and applications that supported mission-essential functions. Appendix IV presents the 33 systems and applications for which actual recovery times were not available as of March 8, 2016. The IRS said that some of these systems and applications are replicated; however, supporting documentation was not available during our review.

As of March 2016, the IRS could not identify actual recovery times for all systems and applications supporting its mission-essential functions because, in part, the IRS does not conduct

[11] IRM 10.6.1, *Continuity Operations Program Continuity Planning Requirements* (March 2014).

testing that would identify actual recovery times for all systems and applications supporting mission-essential functions. Furthermore, the Cybersecurity organization manages recovery time objectives for individual systems and applications and does not explicitly plan for and test enterprise-wide recovery times for mission-essential functions. Because actual recovery times are unknown for all systems and applications supporting its mission-essential functions, sufficient information is not available to the IRS IT organization to enable it to verify its ability to recover mission-essential functions within the time frames defined by the business operating divisions.

Recommendations

The Chief Information Officer should:

Recommendation 4: Collaborate with the IRS business operating divisions to reach consensus regarding the maximum tolerable downtime or recovery time objective for each mission-essential function.

> **Management's Response:** The IRS agreed with this recommendation and understands this is a best practice and not required by Federal guidelines or IRM policy. The Cybersecurity organization will collaborate with the business operating divisions to reach consensus on the maximum tolerable downtime for each business process and the recovery time objective for each application/system for each mission-essential function.

Recommendation 5: Verify through testing that the IRS IT organization is able to recover mission-essential functions within the maximum tolerable downtimes or recovery time objectives for mission-essential functions established by the business operating divisions.

> **Management's Response:** The IRS partially agreed with this recommendation. The Enterprise Operations organization will verify through its current documented process that the organization is able to recover mission-essential functions within the maximum tolerable downtimes for only the systems that are identified by the Cybersecurity organization as needing disaster recovery or alternate site processing testing and only to the extent that funding is available.
>
> **Office of Audit Comment:** There are 51 systems and applications supporting the IRS's mission-essential functions. The IRS was able to provide actual recovery times for 18 of these systems and applications. However, the IRS cannot verify that it is able to recover the remaining 33 systems and applications within the time frames defined by the business operating divisions. Timely recovering mission-essential functions is critical to ensure any outage has minimal impact on tax administration. Therefore, the IRS should take the steps necessary to verify systems and applications can be timely recovered within the time frames defined by the business operating divisions.

Improved Testing Practices for Moderate-Availability Systems and Applications Supporting Mission-Essential Functions Could Help Ensure Business Recovery Needs Are Met

TIGTA observed July 2015 disaster recovery testing to determine whether the IRS is able to recover major computing systems and applications within its Enterprise Computing Centers in a time frame that satisfies established business needs and priorities. We considered whether the IRS could fully restore moderate- to high-availability systems/applications in the event of a disruption to computer operations. Our observation of disaster recovery testing determined that the IRS successfully recovered two of its four high-availability general support systems and satisfied the general support systems' stated recovery time objectives. However, we found two areas in which enterprise disaster recovery testing practices can be improved.

Functional exercises of moderate-availability systems and applications supporting mission-essential functions include an element of system recovery; however, more robust testing is recommended

NIST[12] guidance explains that an agency should conduct functional exercises, at an organization-defined frequency, for all moderately available systems. The NIST defines a functional exercise as allowing personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency but in a simulated manner. Functional exercises simulate the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (*e.g.*, communications, emergency notifications, system equipment setup). Further, functional exercise procedures should include an element of system recovery from backup media. Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.

High-availability systems require disaster recovery testing and simulated information system disruptions that require relocation to an alternate processing site. An IRS disaster recovery test includes data recovery from the Martinsburg Enterprise Computing Center to the Memphis Enterprise Computing Center or from the Memphis Enterprise Computing Center to the Martinsburg Enterprise Computing Center. The IRS conducts disaster recovery tests for its five high-availability systems and applications at least once a year.

For low- and moderate-availability systems and applications, the IRS conducts tabletop exercises, which are discussion-based exercises in which personnel meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a

[12] NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).

particular emergency. For moderate-availability systems and applications, the IRS also conducts functional exercises, which involve retrieving data backups from off-site storage and ensuring that a 10 percent sample of data files are readable. Of the 51 systems and applications that support mission-essential functions, 35 were moderate-availability systems and thus are subject to tabletop exercises and sample testing of data files for readability. However, due to the critical nature of these systems and applications and the role mission-essential systems play in processing tax returns, functional tests should test various functional aspects of their information system contingency plans that are consistent with the relative priority of the system and application.

Efficiency of a disaster recovery testing tool can be improved by entering keystroke recovery procedures in order of recovery priorities

IRM 10.8.60[13] states that the enterprise-wide business impact analysis serves as a core initiative to determine recovery priorities for all systems and applications supporting critical business processes. The guidance states that the IRS should use the data gathered during the business impact analysis to establish recovery priorities within systems, applications, and the enterprise.

Our review also considered the IRS's Toolkit Suite With Command Centre (TSCC) disaster recovery testing tool. The TSCC is a commercial off-the-shelf software tool the IRS introduced in 2006. The TSCC system is a decision support tool and plan repository for disaster recovery. The IRS relies on the TSCC as the repository for its 140 FISMA system and application information system contingency plans. The tool is capable of: 1) identifying affected people, processes, and systems; 2) determining the disaster recovery plans that should be activated; and 3) providing critical information during disaster events and exercises. During our review, the Cybersecurity Architecture and Implementation organization explained that the TSCC also provides collaboration, communication, monitoring tools, and the execution of keystroke recovery procedures to recover systems and application in the event of a disruption.

As a part of the IRS's disaster recovery program, Cybersecurity officials stated that they had implemented executable keystroke recovery procedures into TSCC for five systems and 16 applications as of September 2015. As Cybersecurity personnel populate the TSCC with recovery keystrokes for the remaining systems and applications, Cybersecurity personnel focus on entering recovery keystrokes for applications identified on Enterprise Operation's Premium Services List. According to the IRS, the Premium Services List of applications determines the priorities for triaging computer operations incidents during filing season. However, our review found the Premium Services List did not include general support systems, did not include all applications supporting mission-essential functions, and did not consider recovery priority. Due to this lack of important information, the IRS is not entering the recovery keystrokes for systems and applications in order of their recovery priorities as identified in an enterprise-wide business

[13] IRM 10.8.60, *Information Technology (IT) Security - IT Service Continuity Management (ITSCM) Policy and Guidance* (December 2013).

impact analysis. Accordingly, the IRS could use the TSCC tool more efficiently to recover mission-essential function and achieve the aforementioned capabilities of the tool.

Management Action: After our review, the IRS IT organization reported that it is using applications comprising the mission-essential functions as the basis for entering keystroke recovery procedures into the TSCC tool.

Recommendations

The Chief Information Officer should:

Recommendation 6: Revise and implement policy to ensure that functional tests of moderate-availability systems and applications supporting mission-essential functions are designed to test various functional aspects of their information system contingency plans that are consistent with the relative priority of the system and application.

> ***Management's Response:*** The IRS disagreed with this recommendation. The IRS's current processes for conducting tabletop exercises and functional exercises meet the requirements of NIST Special Publication 800-34 and the IRM.
>
> ***Office of Audit Comment:*** NIST guidance recognizes that functional exercises may vary in complexity and scope depending on the applications' criticality. Of the 51 systems and applications that support IRS mission-essential functions, 35 were moderate-availability systems and were subject to tabletop exercises and limited functional testing to ensure that a 10 percent sample of data files were readable. The IRS conducts this same level of functional testing for moderate-availability systems whether the application supports mission-essential functions or not. Because these 35 moderate-availability applications support mission-essential functions, and by definition cannot be unavailable for more than a predetermined time frame without significantly jeopardizing the operation of the organization, the IRS should conduct sufficient functional exercises to ensure that the IRS can recover these applications within the time frames defined by the business.

Recommendation 7: Ensure that the IRS uses the enterprise disaster recovery priorities of systems and applications, derived from an updated enterprise-wide business impact analysis, to identify the order of entering keystroke recovery procedures into the TSCC tool.

> ***Management's Response:*** The IRS disagreed with this recommendation. The IRS stated that the order of entry for existing keystroke recovery plans was modified in 2016; therefore, the mission-essential functions are currently used as the basis for determining that order into the TSCC tool.
>
> ***Office of Audit Comment:*** The actions taken by IRS management address this recommendation.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS has a complete and adequate disaster recovery planning and testing capability that allows the IRS to recover major computer systems and applications from its Enterprise Computing Centers in a time frame that satisfies established business needs and priorities. To accomplish our objective, we:

I. Assessed the completeness and adequacy of the IRS's Disaster Recovery Plans and Information System Contingency Plans.

   A. Reviewed relevant IRM policies that have materially changed since the last TIGTA[1] audit for reasonableness in implementing NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010).

   B. Determined if the IRS has adequately prioritized the recovery of its information systems in the event of a disruption.

   C. Determined if the IRS IT organization is meeting the Recovery Time Objectives for IRS systems/applications.

II. Determined the effectiveness of Disaster Recovery Plan/Information System Contingency Plan testing.

   A. Reviewed relevant IRM policies that have materially changed since the last TIGTA audit for reasonableness in implementing NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* (September 2006).

   B. Evaluated whether the IRS could fully restore in a timely manner moderate- to high-availability systems/applications that support mission-essential functions in the event of a disruption to computer operations.

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 the following internal controls were relevant to our audit objective: IRS policies, procedures, and practices for disaster recovery planning and disaster recovery testing. We evaluated these controls by

[1] TIGTA, Ref. No. 2012-20-041, *Disaster Recovery Testing Is Being Adequately Performed, but Problem Reporting and Tracking Can Be Improved* (May 2012).

interviewing IRS Cybersecurity and Enterprise Operations staff, reviewing disaster recovery and backup documentation, observing a disaster recovery test, and reviewing plans and reports regarding disaster recovery tests.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn McGowan, Director
Carol Taylor, Audit Manager
Richard Pinnock, Lead Auditor
Denis Danilin, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Commissioner for Services and Enforcement
Commissioner, Large Business and International Division
Commissioner, Small Business/Self-Employed Division
Commissioner, Tax Exempt and Government Entities Division
Commissioner, Wage and Investment Division
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Director, Office of Audit Coordination

Appendix IV

Systems and Applications Supporting Mission-Essential Functions Without Known Actual Recovery Times *(as of March 2016)*

<table>
<tr><th colspan="2">General Support Systems</th></tr>
<tr><td colspan="2">Enterprise Systems Domain General Support System 17</td></tr>
<tr><td colspan="2">Infrastructure Shared Services General Support System 18</td></tr>
<tr><td colspan="2">Virtual Host Infrastructure General Support System 39</td></tr>
<tr><td colspan="2">Affordable Care Act Linux Platform General Support System 41</td></tr>
<tr><td colspan="2">Enterprise Linux Platform General Support System 42</td></tr>
<tr><th colspan="2">Applications</th></tr>
<tr><td>Automated 6020(b) Substitute for Returns</td><td>Human Resources Reporting Center</td></tr>
<tr><td>Automated Insolvency System</td><td>Integrated Submission and Remittance Processing</td></tr>
<tr><td>Automated Manual Assessments</td><td>Large Business and International Data Capture System</td></tr>
<tr><td>Automated Non-Master File</td><td>Letter and Information Network User-Fee System</td></tr>
<tr><td>Automated Quarterly Excise Tax Listing</td><td>Photocopy Refunds Program</td></tr>
<tr><td>Bank Discrepancy</td><td>Report Generation Software</td></tr>
<tr><td>Chief Counsel System Domain General Support System</td><td>Redesign Revenue Accounting Control System</td></tr>
</table>

Applications **(continued)**	
Correspondence Examination Automation Support Subsystem – Automated Case Workload Management	Return Review Program
Enterprise Common Services	Remittance Strategy for Paper Check Conversion
Employee Plans-Exempt Organizations Determination System	Service Center Recognition Image Processing System
Electronic Federal Payment Posting System	Standardized Integrated Data Retrieval System Access Tier II
Examination Returns Control System	Taxpayer Advocate Management Information System
Excise Files Information Retrieval System	Title 31 Non-Banking Financial Institution Database
Government Relocation Accounting System	Web-Based Employee Technical Time System

Source: TIGTA analysis of "Mission-Essential Function Recovery Time Objective Actual Recovery-TIGTA Audit Response-030816."

Appendix V

Glossary of Terms

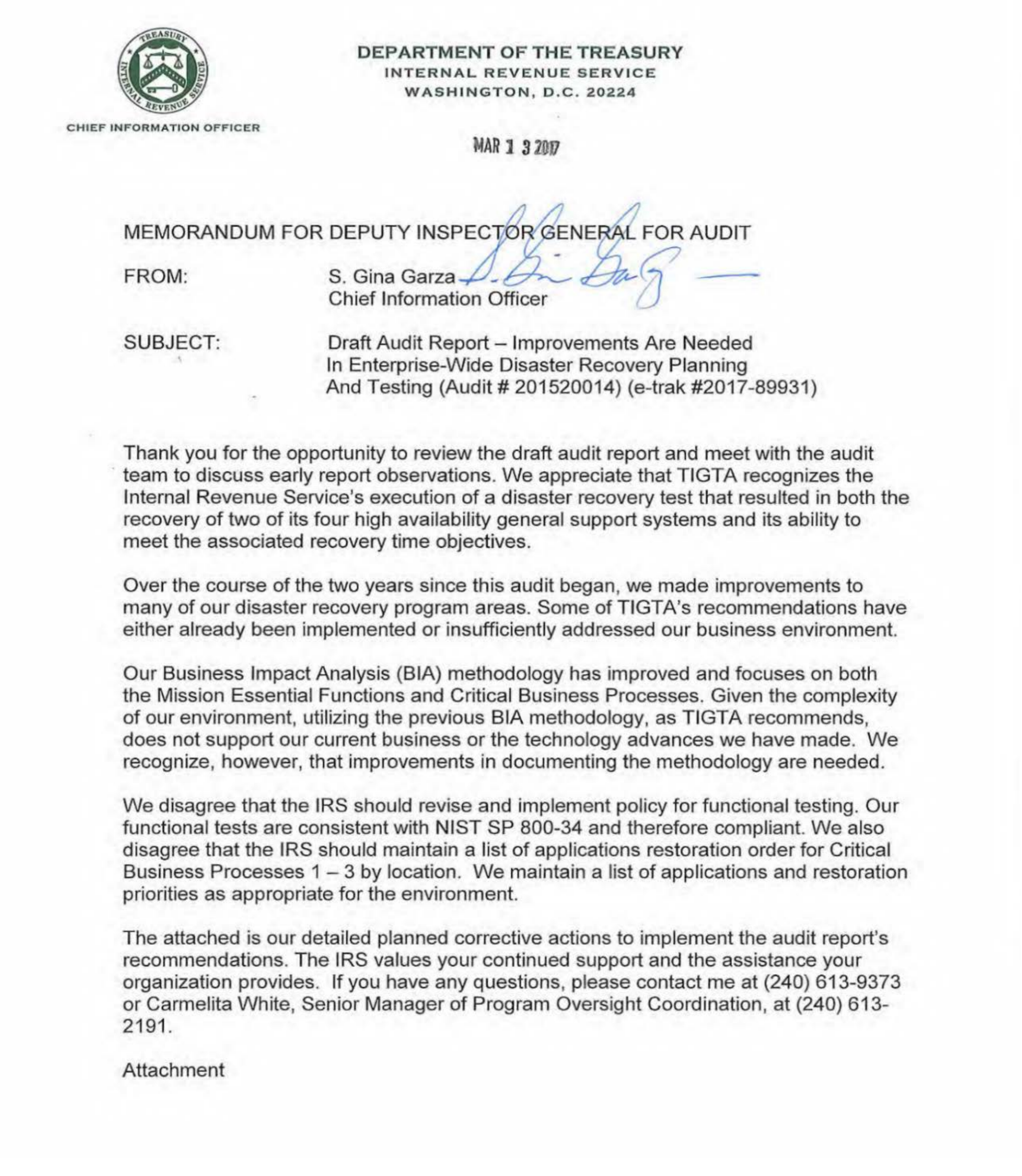
Term	Definition
Alternate Site Processing	Involves moving production processing from one Enterprise Computing Center to the other Enterprise Computing Center using replication and gridding (virtual tape) technologies.
Application	A software program hosted by an information system.
Availability	Ensuring timely and reliable access to and use of information.
Backup	The process of duplicating and storing the files and programs of an information technology system on another medium or device to facilitate complete restoration of the system and its data following a disruption.
Business Impact Analysis	An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Contingency Planning	The process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively affects the organization.
Critical Business Process	Business processes defined by the IRS business operating divisions that are the most critical to the tax administration mission of the IRS and the Federal Government.
Disaster Recovery	The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
Disaster Recovery Plan	A plan created and maintained by the IRS IT organization or any information technology service provider that defines the resources, roles, responsibilities, actions, tasks, and steps required, down to a key step level, to restore an information technology system to its full operational status at the current or alternate facility after a disruption. It can be a part of the Information System Contingency Plan, a standalone document, or separate disaster recovery keystroke procedures.
Disaster Recovery Test	Full-scale functional exercise that involves recovering the system and/or application on nonproduction equipment, in a simulated environment, or at the recovery location.

Term	Definition
Disruption	An unplanned event that causes an information system to be inoperable for a length of time (*e.g.*, minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).
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.
Functional Exercise	Allows personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. Functional exercises exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (*e.g.*, communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or shared information processing service organization.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
Keystroke Recovery	Detailed instructions, including keystroke-by-keystroke details, to restore an information technology system to its full operational status following a disruption.
Maximum Tolerable Downtime	The maximum amount of time a business can tolerate the outage of a critical business function. The Maximum Tolerable Downtime consists of two elements, the systems recovery time objective and the work recovery time.

Term	Definition
Recovery Time Objective	The time it takes to recover a system/application after an outage (*e.g.*, one business day). Recovery time objectives are often used as the basis for the development of recovery strategies and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.
Replication	Copies data from one storage location to one or more other local or remote storage systems.
Tabletop Exercise	A discussion-based exercise in which personnel with roles and responsibilities in a particular plan meet to validate the content of the plan in the context of a particular emergency.
Toolkit Suite With Command Centre	The IRS information technology enterprise-level repository and incident management decision support tool and plan repository for business continuity and disaster recovery, where plans include, but are not limited to: Information System Contingency Plans; Disaster Recovery Plans; Facility Plans; Business Continuity Plans; Occupant Emergency Plans; and Emergency Communication Plans.

Appendix VI

Management's Response to the Draft Report



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

CHIEF INFORMATION OFFICER

MAR 1 3 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report – Improvements Are Needed In Enterprise-Wide Disaster Recovery Planning And Testing (Audit # 201520014) (e-trak #2017-89931)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. We appreciate that TIGTA recognizes the Internal Revenue Service's execution of a disaster recovery test that resulted in both the recovery of two of its four high availability general support systems and its ability to meet the associated recovery time objectives.

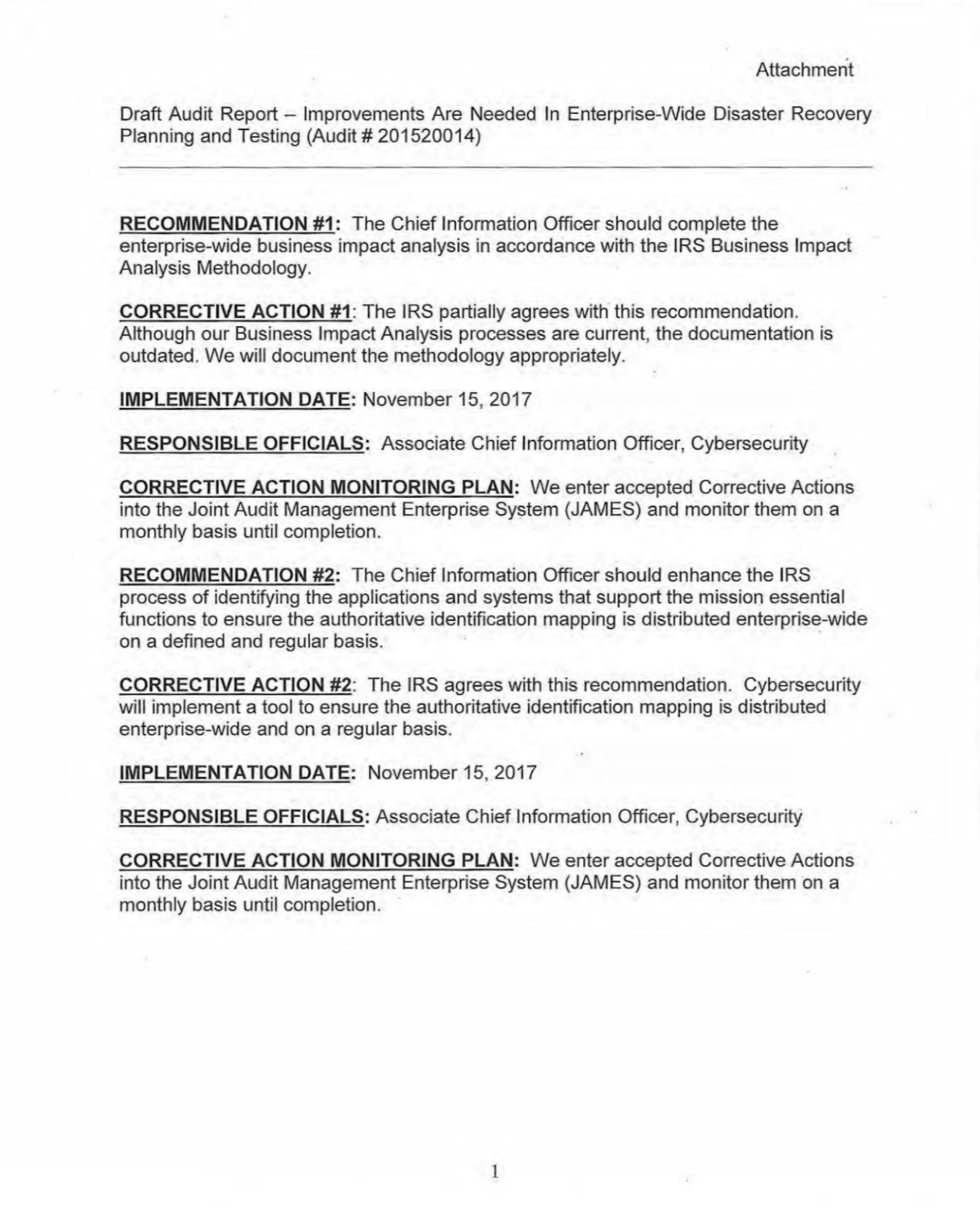
Over the course of the two years since this audit began, we made improvements to many of our disaster recovery program areas. Some of TIGTA's recommendations have either already been implemented or insufficiently addressed our business environment.

Our Business Impact Analysis (BIA) methodology has improved and focuses on both the Mission Essential Functions and Critical Business Processes. Given the complexity of our environment, utilizing the previous BIA methodology, as TIGTA recommends, does not support our current business or the technology advances we have made. We recognize, however, that improvements in documenting the methodology are needed.

We disagree that the IRS should revise and implement policy for functional testing. Our functional tests are consistent with NIST SP 800-34 and therefore compliant. We also disagree that the IRS should maintain a list of applications restoration order for Critical Business Processes 1 – 3 by location. We maintain a list of applications and restoration priorities as appropriate for the environment.

The attached is our detailed planned corrective actions to implement the audit report's recommendations. The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (240) 613-9373 or Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment



Attachment

Draft Audit Report – Improvements Are Needed In Enterprise-Wide Disaster Recovery Planning and Testing (Audit # 201520014)

RECOMMENDATION #1: The Chief Information Officer should complete the enterprise-wide business impact analysis in accordance with the IRS Business Impact Analysis Methodology.

CORRECTIVE ACTION #1: The IRS partially agrees with this recommendation. Although our Business Impact Analysis processes are current, the documentation is outdated. We will document the methodology appropriately.

IMPLEMENTATION DATE: November 15, 2017

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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

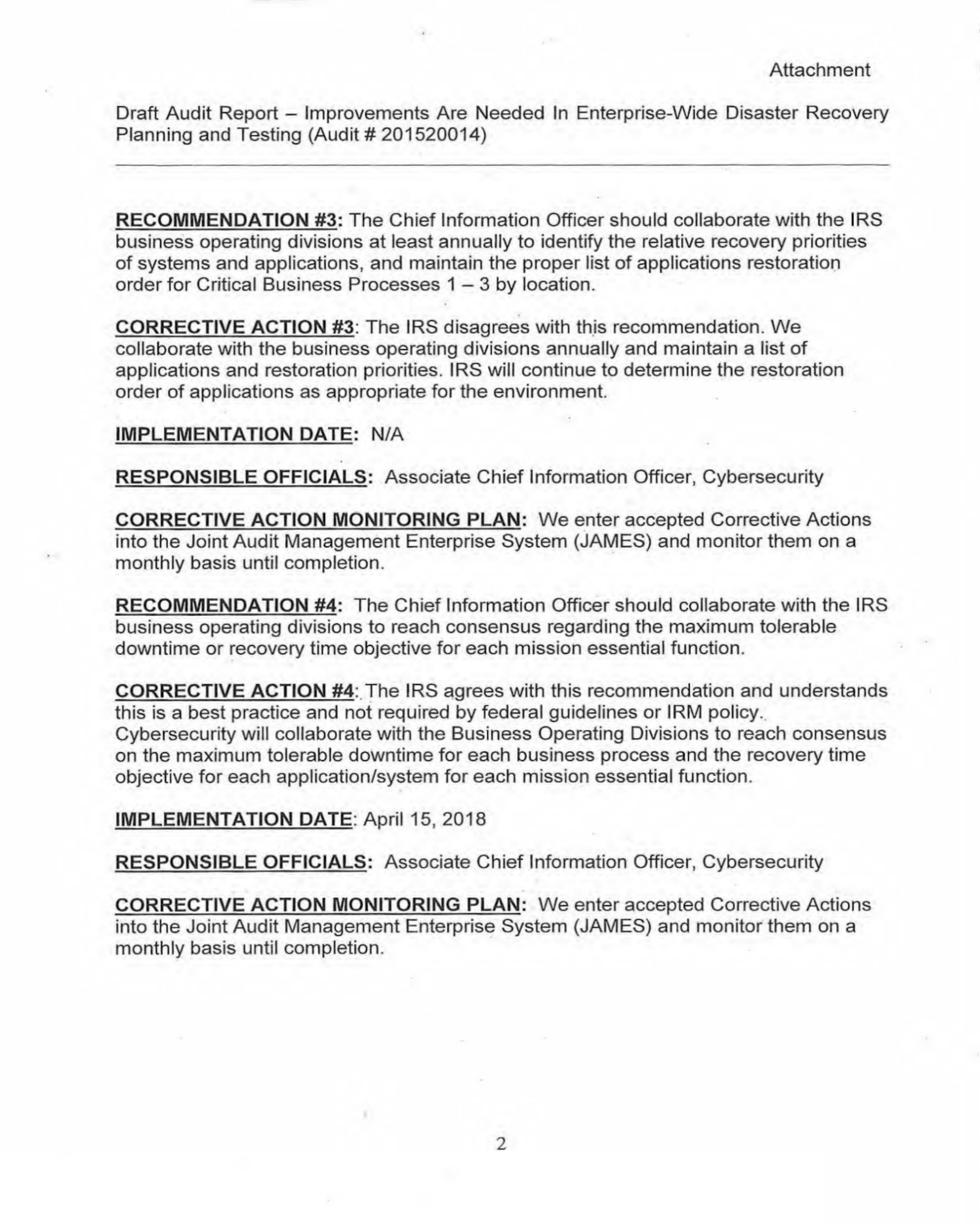
RECOMMENDATION #2: The Chief Information Officer should enhance the IRS process of identifying the applications and systems that support the mission essential functions to ensure the authoritative identification mapping is distributed enterprise-wide on a defined and regular basis.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. Cybersecurity will implement a tool to ensure the authoritative identification mapping is distributed enterprise-wide and on a regular basis.

IMPLEMENTATION DATE: November 15, 2017

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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



Attachment

Draft Audit Report – Improvements Are Needed In Enterprise-Wide Disaster Recovery Planning and Testing (Audit # 201520014)

RECOMMENDATION #3: The Chief Information Officer should collaborate with the IRS business operating divisions at least annually to identify the relative recovery priorities of systems and applications, and maintain the proper list of applications restoration order for Critical Business Processes 1 – 3 by location.

CORRECTIVE ACTION #3: The IRS disagrees with this recommendation. We collaborate with the business operating divisions annually and maintain a list of applications and restoration priorities. IRS will continue to determine the restoration order of applications as appropriate for the environment.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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

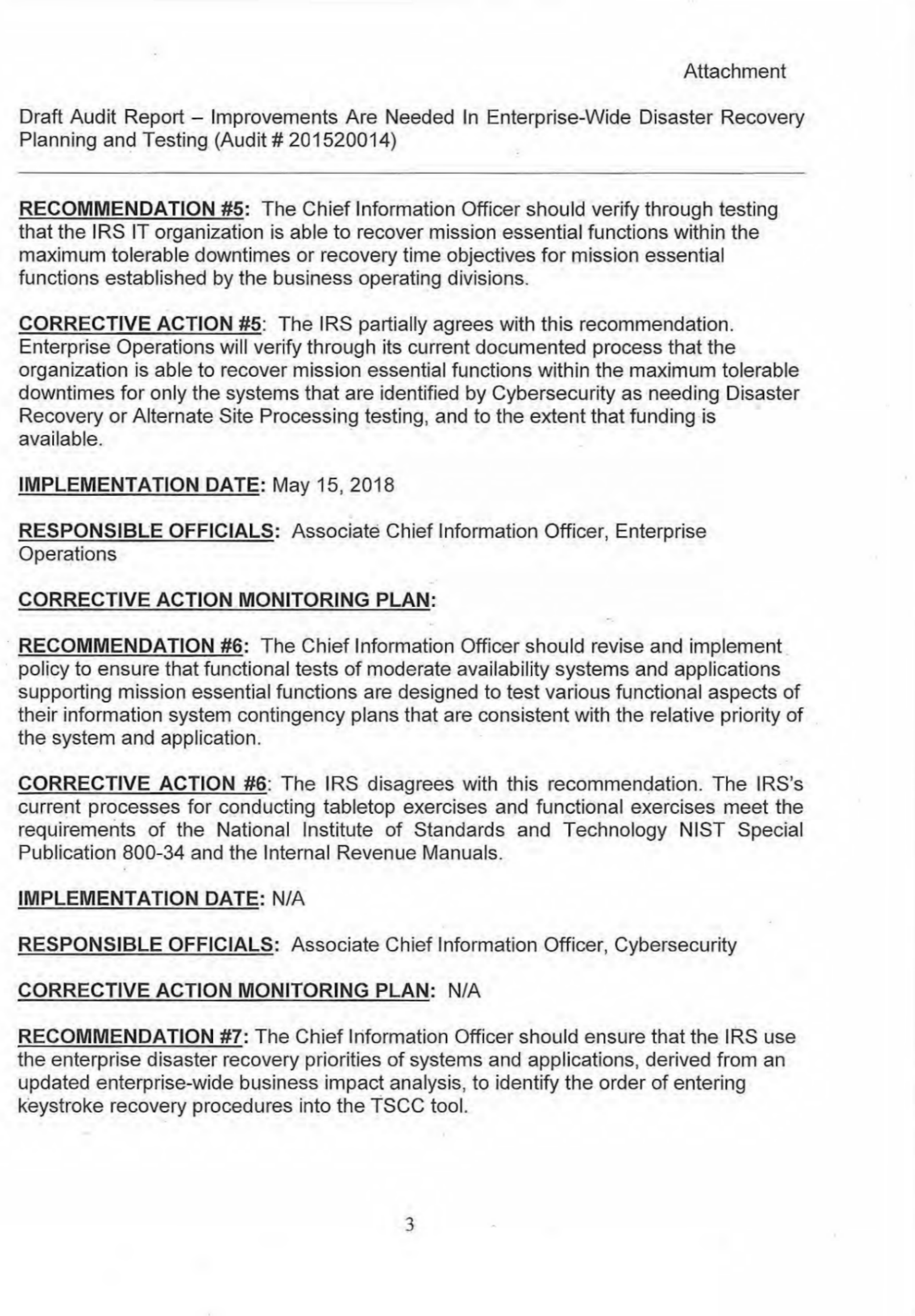
RECOMMENDATION #4: The Chief Information Officer should collaborate with the IRS business operating divisions to reach consensus regarding the maximum tolerable downtime or recovery time objective for each mission essential function.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation and understands this is a best practice and not required by federal guidelines or IRM policy. Cybersecurity will collaborate with the Business Operating Divisions to reach consensus on the maximum tolerable downtime for each business process and the recovery time objective for each application/system for each mission essential function.

IMPLEMENTATION DATE: April 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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



Attachment

Draft Audit Report – Improvements Are Needed In Enterprise-Wide Disaster Recovery Planning and Testing (Audit # 201520014)

RECOMMENDATION #5: The Chief Information Officer should verify through testing that the IRS IT organization is able to recover mission essential functions within the maximum tolerable downtimes or recovery time objectives for mission essential functions established by the business operating divisions.

CORRECTIVE ACTION #5: The IRS partially agrees with this recommendation. Enterprise Operations will verify through its current documented process that the organization is able to recover mission essential functions within the maximum tolerable downtimes for only the systems that are identified by Cybersecurity as needing Disaster Recovery or Alternate Site Processing testing, and to the extent that funding is available.

IMPLEMENTATION DATE: May 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN:

RECOMMENDATION #6: The Chief Information Officer should revise and implement policy to ensure that functional tests of moderate availability systems and applications supporting mission essential functions are designed to test various functional aspects of their information system contingency plans that are consistent with the relative priority of the system and application.

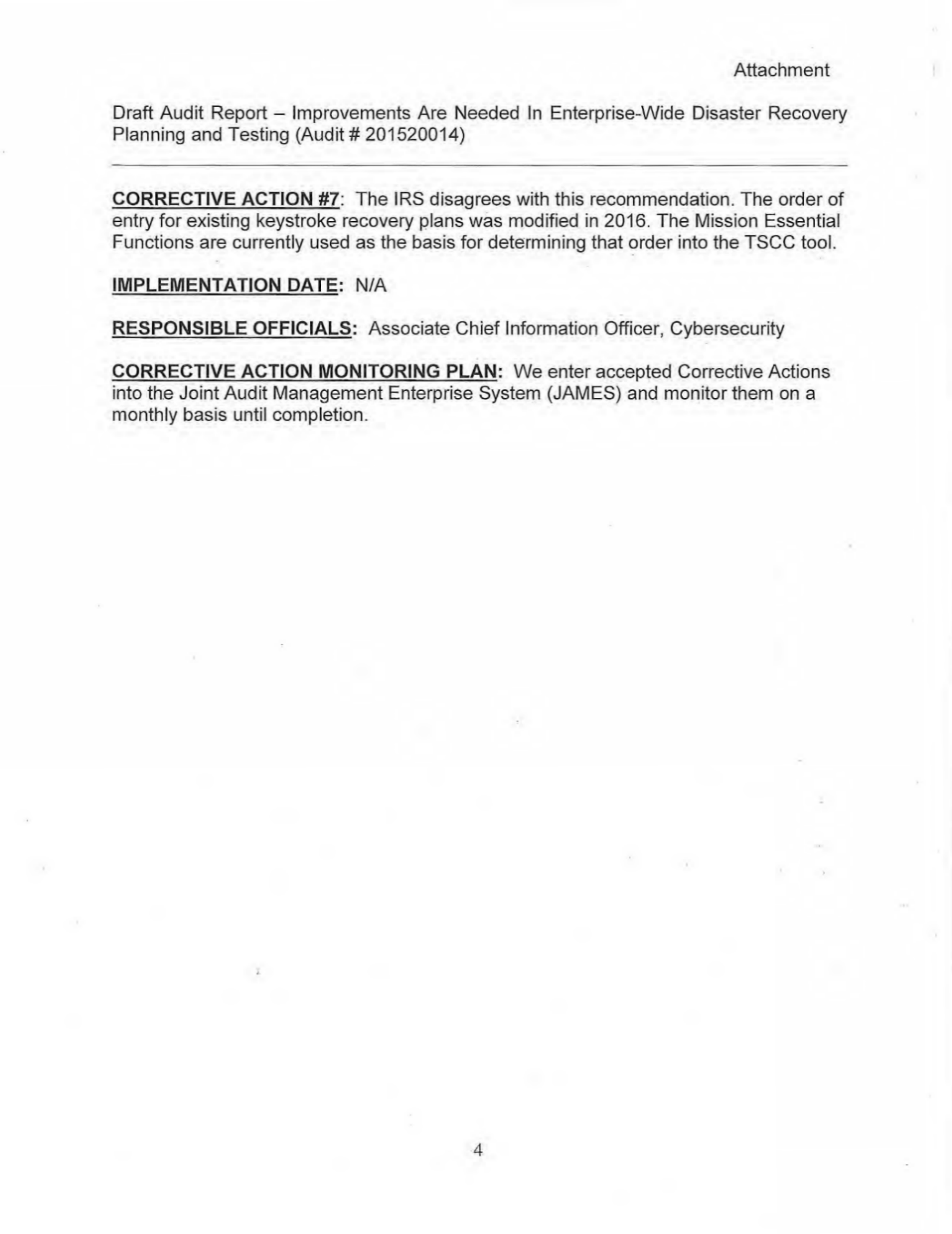
CORRECTIVE ACTION #6: The IRS disagrees with this recommendation. The IRS's current processes for conducting tabletop exercises and functional exercises meet the requirements of the National Institute of Standards and Technology NIST Special Publication 800-34 and the Internal Revenue Manuals.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #7: The Chief Information Officer should ensure that the IRS use the enterprise disaster recovery priorities of systems and applications, derived from an updated enterprise-wide business impact analysis, to identify the order of entering keystroke recovery procedures into the TSCC tool.



Attachment

Draft Audit Report – Improvements Are Needed In Enterprise-Wide Disaster Recovery Planning and Testing (Audit # 201520014)

CORRECTIVE ACTION #7: The IRS disagrees with this recommendation. The order of entry for existing keystroke recovery plans was modified in 2016. The Mission Essential Functions are currently used as the basis for determining that order into the TSCC tool.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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