TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement

May 8, 2023

Report Number: 2023-20-023

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta

HIGHLIGHTS: Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement

Final Audit Report issued on May 8, 2023 **Report Number 2023-20-023**

Why TIGTA Did This Audit

To carry out its mission, the IRS relies on three mission essential functions (MEF): Processing Tax Remittances, Processing Tax Returns, and Processing Tax Refunds. MEFs are a limited set of IRS functions that must be continued throughout, or rapidly resumed after, a service outage or disaster. Supported by 50 information systems (hereafter referred to as systems), these functions enable the IRS to meet its mission and provide vital services to taxpayers.

This audit was initiated to assess the effectiveness of software and data recovery processes after a service outage or disaster for systems that support MEFs.

Impact on Tax Administration

In Fiscal Year 2022, the IRS collected nearly $5 trillion in Federal tax payments and processed 260 million tax returns and forms. The IRS's Federal tax refund and outlay activities were over $640 billion. Without testing all systems that support MEFs and meeting its recovery time objectives (RTO), the IRS risks its ability to rapidly resume operations after a service outage or disaster.

What TIGTA Found

The IRS equipped its enterprise computing centers with dual power supplies which are now equipped to provide continuous operations during a service outage. As a result, the enterprise computing centers no longer require three planned power outages annually to test backup capabilities and perform electrical maintenance.

The IRS uses a disaster recovery planning tool to create a dynamic disaster recovery plan during a service outage or disaster; however, the tool does not reflect MEF recovery priorities. A review of the disaster recovery planning tool reports identified that only 21 of the 50 systems that support MEFs are listed. In addition, seven systems in the tool are incorrectly identified as systems that support MEFs.

Disaster recovery testing needs improvement. A review of the 50 systems determined that the RTO (a measure of system downtime before negative effects occur to other systems) for 45 systems was more than the maximum tolerable downtime (MTD) of 12 hours (the maximum time system owners can tolerate a MEF outage). In addition, the RTO was only tested for 40 of the 50 systems. Of the 40 systems tested, eight systems' recovery time actuals (actual system recovery time when tested) were greater than the MTD and did not meet MEF requirements. The remaining 32 systems' recovery time actuals met MEF requirements. Further, the recovery time actuals for general support systems are not documented clearly.

Finally, the 50 systems are not rated as high impact for availability, even though they are essential to accomplishing the IRS's mission. Systems are assigned a high-impact value if the loss of availability is expected to have a severe or catastrophic adverse effect to an extent and duration that the organization is unable to perform one or more of its primary functions.

What TIGTA Recommended

TIGTA made seven recommendations to the Chief Information Officer that include ensuring that: 1) a process to create and maintain an approved consolidated list mapping systems to MEFs is implemented; 2) systems listed in the disaster recovery planning tool are periodically validated; 3) RTOs are updated; 4) disaster recovery testing is performed for systems that were not tested; 5) a Plan of Action and Milestones is prepared for systems unable to meet the MTD; 6) disaster recovery testing is performed annually on systems supporting MEFs; and 7) the impact value of availability for systems supporting MEFs is reassessed.

The IRS agreed with all seven recommendations and plans to maintain an approved list mapping systems to MEFs; periodically validate systems in the disaster recovery planning tool; update the RTOs; perform disaster recovery testing for systems not tested; develop a Plan of Action and Milestones for systems unable to meet the MTD; perform disaster recovery testing annually; and reassess the impact value of availability for systems supporting MEFs.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

May 8, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement (Audit # 202220015)

This report presents the results of our review to assess the effectiveness of software and data recovery processes after a service outage or disaster for systems that support mission essential functions. This review is part of our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS [Internal Revenue Service] Resources*.

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

Appendices

Background

Federal agencies are dependent on information systems and electronic data to carry out operations and to process, maintain, and report essential information. Information systems and electronic data support virtually all Federal activities. Agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information technology assets.

The Internal Revenue Service (IRS) mission is to provide America's taxpayers top-quality service by helping them understand and meet their tax responsibilities and enforce the law with integrity and fairness to all. During Fiscal Year 2022, the IRS collected approximately $4.9 trillion in Federal tax payments and processed 260 million tax returns and forms.[1] The IRS's Federal tax refund and outlay activities were over $640 billion.[2] To carry out its mission, the IRS has identified three mission essential functions (MEF).

- MEF 1 – Processing Tax Remittances: the process of receiving payments, fees, and other monies through submission processing, and includes the deposit of funds and all accompanying payment data.
- MEF 2 – Processing Tax Returns: the process of receiving, sorting, coding, and archiving all tax returns.
- MEF 3 – Processing Tax Refunds: the process of performing final calculations and verifications to settle an account, including exception reports, posting offsets, and sending refund information for issuance.

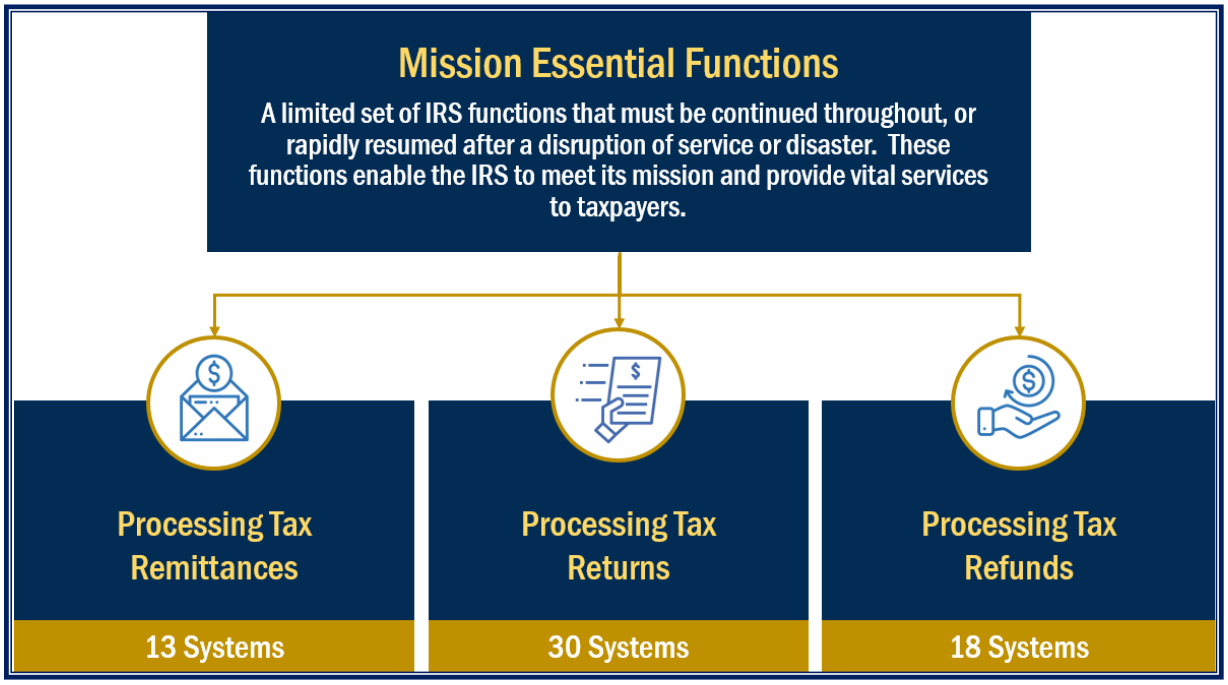
MEFs are a limited set of IRS functions that must be continued throughout, or rapidly resumed after, a service outage or disaster. These functions enable the IRS to meet its mission and provide vital services to taxpayers. MEFs serve as key continuity planning factors to determine appropriate staffing, communications, information, facilities, training, and other requirements. As of February 2022, IRS business operating divisions have identified 50 information systems (hereafter referred to as systems) that support the MEFs.[3] Systems within each respective MEF must all be operational in order to fully provide the vital service to taxpayers. Figure 1 illustrates the three MEFs and the number of systems that support them.

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

[2] Federal tax refund and outlay activities include refunds of tax overpayments, payments for interest, and disbursements for refundable tax credits, such as the Earned Income Tax Credit.

[3] See Appendix III for a list of the 50 systems and MEFs they support.

Figure 1: Number of Systems Supporting Each MEF

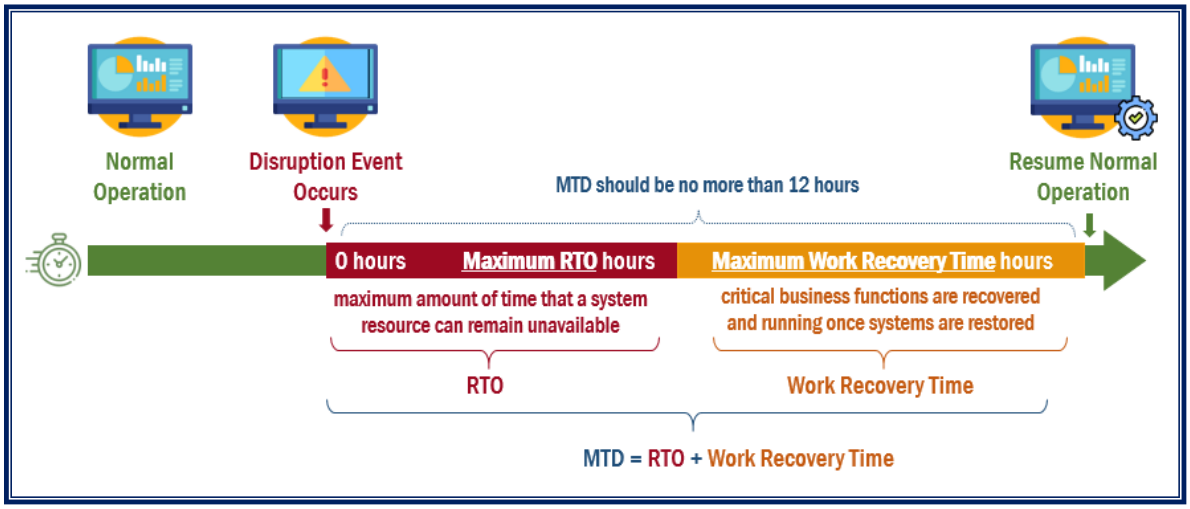


Source: Treasury Inspector General for Tax Administration's analysis of Internal Revenue Manual (IRM) 10.8.60, Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance (July 2021), and the systems' business impact analysis. Note: A system can support more than one MEF.

The execution of MEFs requires a coordinated effort between the Information Technology organization's Cybersecurity and Enterprise Operations functions as well as IRS business operating divisions. The Cybersecurity function is responsible for ensuring that the IRS complies with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of its systems and data. The Enterprise Operations function operates and maintains the computing infrastructure at the enterprise computing centers (ECC) located in [redacted]. The Cybersecurity and Enterprise Operations functions, in conjunction with the business operating divisions, are responsible for performing disaster recovery tests annually of their systems. In addition, the Cybersecurity function and the business operating divisions are jointly responsible for developing and maintaining the business impact analyses and disaster recovery plans (DRP). A business impact analysis determines the system recovery priorities, and the results are incorporated into the development of a DRP.

A DRP defines the resources, roles, responsibilities, actions, tasks, and steps required to restore a system to its full operational status at the current or an alternate facility, after a service outage or disaster. A DRP should contain the processes to attain MEF capabilities as soon as possible but no later than 12 hours, referred to as the maximum tolerable downtime (MTD), following a planned activation. The MTD represents the maximum acceptable amount of time system owners can tolerate an outage of a MEF, while the recovery time objective (RTO) is a measure of system downtime before negative effects occur to other systems. The work recovery time represents the time needed to restore functions back to operation once the underlying systems have been restored. Figure 2 presents the relationship between the MTD, the RTO, and work recovery time.

Figure 2: MTD, RTO, and Work Recovery Time Relationship for MEFs



Source: Treasury Inspector General for Tax Administration's analysis of IRM 10.8.60.

Results of Review

Dual Power Supplies Have Been Implemented at the Enterprise Computing Centers

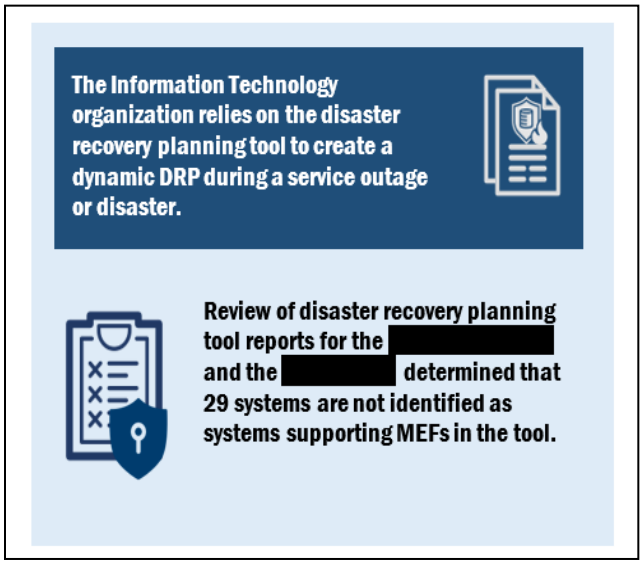
Effective in Fiscal Year 2020, the [redacted] were both configured to deliver dual power supplies and are now equipped to provide continuous operations during a service outage, *e.g.*, electrical maintenance or interrupted utility power leading to a disaster. According to the *EOPS [Enterprise Operations] Dual Power Concurrent Maintenance DME [Development/Modernization/Enhancement] #228578, #203969, Request for Close-out* (Apr. 2021), the [redacted] were physically and logically configured for dual power redundancy from two separate uninterrupted power sources. In addition, a Supervisory Control and Data Acquisition system was installed to monitor and provide the capability to balance electrical power loads between the power sources. Enterprise Operations function management also provided test reports completed in April 2021 after the implementation of the dual power supplies at the ECCs. Our review of the test reports determined that each of the 1,745 and 1,546 pieces of information technology equipment at the [redacted], respectively, received a "passed" status and are equipped to provide dual power supplies. As a result, the Enterprise Operations Governance Board approved closing out the project in April 2021.

Prior to Fiscal Year 2019, the ECCs required three planned power outages annually to test backup capabilities and perform electrical maintenance. The Facilities Management and Security Services office planned power outages caused mainframe computing processes and tax processing operations to be unavailable, affecting MEFs. It also required extensive planning to ensure that systems are available and operational at an alternate facility. According to the [redacted] *IT Equipment Dual Cording Capability Analysis to Support Shutdown Aversion, Project No: 2032H5-18-P-00327, Technical Analysis/Corrective Action Plan*, a

contractor analysis performed during Fiscal Years 2018 and 2019 determined that 15 percent and 10 percent (or a total of 1,015 pieces) of the information technology equipment at the [redacted], respectively, were not capable of providing dual power supplies.

Moving forward, the [redacted] will need to be shut down only once every five years and the [redacted] shut down only once every three years for general facilities maintenance. As a result, the IRS calculated an estimated annual cost savings of approximately $750,000 in labor costs based on hours employees spent on electrical maintenance activities.

The Disaster Recovery Planning Tool Does Not Reflect Mission Essential Function Recovery Priorities



Our review of the June 7, 2022, disaster recovery planning tool reports for the [redacted] determined that 29 (58 percent) of the 50 systems identified by the Cybersecurity function as supporting MEFs, *e.g.*, the [redacted], are not listed in the tool. The remaining 21 (42 percent) systems are appropriately identified and listed in the disaster recovery planning tool. In addition, seven systems in the disaster recovery planning tool were incorrectly identified as systems supporting MEFs, *e.g.*, the [redacted] and the [redacted].

The IRS does not create individual DRPs for each of its ECCs and campuses.[4] Instead, the Information Technology organization relies upon the disaster recovery planning tool as its disaster recovery planning and execution solution. The tool is designed to create a dynamic DRP during a service outage or disaster and takes into account which systems or services are experiencing a disruption in service. The tool maintains system priority and dependency information, which allows for the creation of a DRP tailored to the specific system(s) experiencing the disruption in service. The disaster recovery planning tool restoration of systems is based on MEF order, *i.e.*, MEF 1 (Processing Tax Remittances), followed by MEF 2 (Processing Tax Returns), and then followed by MEF 3 (Processing Tax Refunds). If multiple systems within a MEF require restoration, the systems are restored based on system priorities and dependencies.

According to IRM 10.8.60, system owners are responsible for the analysis to determine their needs in a disaster recovery. They should determine the impact to business processes, recovery requirements, and recovery time frames. Additional recovery needs and system priorities should also be identified. This information should be communicated to the Cybersecurity function and

[4] The campuses that host systems supporting MEFs are located in [redacted]; [redacted]; and [redacted].

used to complete a business impact analysis to evaluate business and system requirements as well as to determine contingency planning requirements and priorities. In addition, IRM 10.8.62, *Information Technology Security (IT), Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program* (Nov. 2019), requires the Cybersecurity function to update the DRP (or disaster recovery planning tool) within 30 calendar days after performing a disaster recovery exercise.

The IRS does not have a formalized process to generate an approved consolidated list mapping systems to MEFs. The data are compiled on an as-needed basis by reviewing information contained in various documents, *i.e.*, business impact analysis and the ISCP, for each system. In addition, the Enterprise Operations function and system owners did not ensure that the disaster recovery planning tool was updated with the current systems supporting MEFs following the completion of disaster recovery exercises. As a result, systems critical to meeting the IRS's mission that are not prioritized for restoration may be impacted and be unable to rapidly resume within 12 hours after a service outage or disaster.

The Chief Information Officer (CIO) should:

Recommendation 1: Implement a process to create and maintain an approved consolidated list mapping systems to MEFs.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will implement a process to create and maintain an approved consolidated list mapping systems to MEFs.

Recommendation 2: Ensure that the disaster recovery planning tool is updated with the current systems supporting MEFs and periodically validated to ensure accuracy.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will update the disaster recovery planning tool with the current systems supporting MEF and will periodically validate the tool to ensure accuracy.

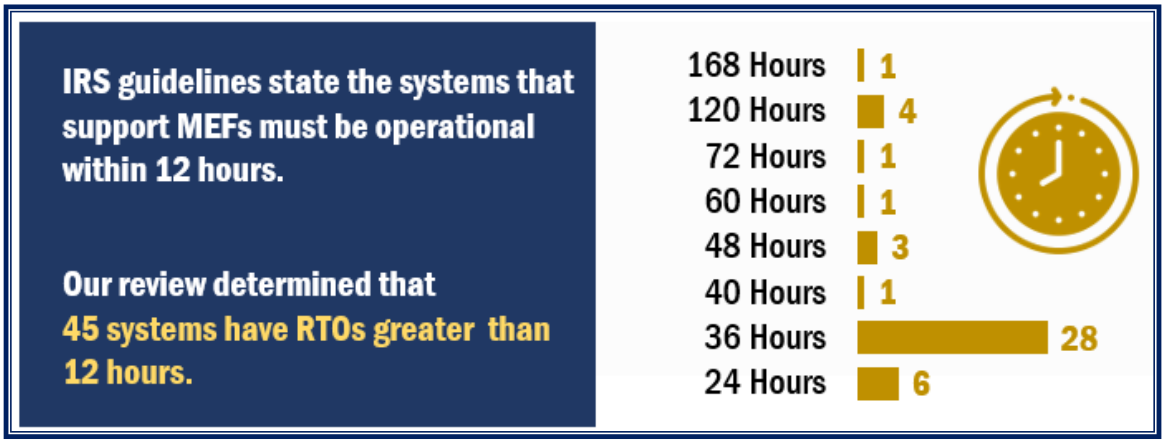
Disaster Recovery Testing Needs Improvement

A majority of systems have a RTO greater than the MTD

To determine whether the RTOs are less than the MTD of 12 hours for MEFs, we reviewed a list of systems' RTOs as of February 2022. Because some systems are dependent on other systems to be operational, the recovery time of a MEF is limited by the system with the longest RTO. The IRS provided a list of systems' RTOs as part of the mapping of systems to MEFs. Our review of the RTO for each of the 50 systems determined that only five (10 percent) systems, *e.g.*, the [redacted] and the [redacted], have a RTO less than 12 hours. However, 45 (90 percent) systems, *e.g.*, the [redacted] and the [redacted], are assigned a RTO greater than 12 hours.[5] Figure 3 depicts the number of systems and their RTOs exceeding 12 hours.

[5] See Appendix IV for a list of the 45 systems with the RTOs greater than 12 hours.

Figure 3: Number of Systems With a RTO Greater Than the MTD



Source: Treasury Inspector General for Tax Administration's analysis of a list of systems' RTOs as of February 2022 provided by the Cybersecurity function.

IRM 10.6.1, *Continuity Operations Program, Overview of Continuity Planning* (Mar. 2020), states that MEFs must be operational within 12 hours, which establishes the RTO for systems. Cybersecurity function personnel stated that they were not informed when IRM 10.6.1 was updated in March 2020 with the new requirement. As a result, Cybersecurity function personnel did not work in conjunction with system owners to update their respective system's RTO nor apply the new criteria when performing disaster recovery testing. Prior to the update, IRM 10.6.1 did not directly specify a time frame for when MEFs must be operational. When systems are tested against overstated RTOs, systems may be unable to meet the MTD and potentially not resume operations timely after a service outage or disaster.

Recommendation 3: The CIO should coordinate with system owners to ensure that they update their respective system's RTO.

Management's Response: The IRS agreed with this recommendation. The CIO will coordinate with system owners to ensure that they update their respective system's RTO.

While most systems' RTO have been tested, several have recovery time actuals (RTA) greater than the MTD

To determine whether the IRS tested the RTO and met RTA requirements, we reviewed the *Application ISCP Testing Checklist* and the *ISCP Testing Observation Report* completed during disaster recovery testing. The *Application ISCP Testing Checklist* is used to validate the system's performance and reports the results of the disaster recovery testing. The *ISCP Testing Observation Report* includes additional disaster recovery testing information, such as scope, observations, and results. During the disaster recovery testing for Federal Information Security Modernization Act of 2014 (FISMA) Year 2021, *i.e.*, July 1, 2020, through June 30, 2021, we found that the IRS tested the RTOs for only 20 of the 50 systems.[6] The RTOs for the remaining 30 systems were not tested. Because the IRS tested less than 50 percent of the systems and was more than half way through FISMA Year 2022, we gave the IRS an opportunity to complete the disaster recovery testing of the RTOs for the remaining 30 systems. Our review of the disaster recovery testing documents for FISMA Year 2022 found that the IRS tested the RTOs for 20 of

[6] Pub. L. No. 113-283.

the 30 remaining systems. Collectively, the IRS tested the RTOs for 40 (80 percent) and did not test the RTOs for 10 (20 percent) systems during FISMA Years 2021 and 2022. Figure 4 identifies the 10 systems for which the RTOs have not been tested.

Figure 4: Systems for Which the RTO Has Not Been Tested

Source: Treasury Inspector General for Tax Administration's analysis of the Application ISCP Testing Checklists and the ISCP Testing Observation Reports for FISMA Years 2021 and 2022.

Of the 40 systems' RTOs tested, our review further found that the RTAs for 32 systems were less than 12 hours, meeting MTD requirements for MEFs. However, the RTAs for the remaining eight systems were greater than 12 hours, not meeting MTD requirements for MEFs. Figure 5 provides the eight systems not meeting the MTD for FISMA Years 2021 and 2022 disaster recovery testing.

Figure 5: Systems Not Meeting the MTD for FISMA Years 2021 and 2022

Source: Treasury Inspector General for Tax Administration's analysis of the Application ISCP Testing Checklists and the ISCP Testing Observation Reports for FISMA Years 2021 and 2022.

IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Sept. 2021), states that MEFs are part of the critical infrastructure. IRM 10.8.62 also states that full-scale disaster recovery testing should be performed annually on critical infrastructure protection assets and high-impact systems to ensure that a full recovery capability is available for all of the most critical FISMA assets. The full-scale testing should include a system restoration at an alternate facility. All annual disaster recovery testing should be completed during each FISMA year from July 1 through June 30. In addition, IRM 10.6.1 states that MEFs must be continued under all circumstances and be operational within 12 hours.

Cybersecurity function management stated that they did not test the RTOs for nine systems because the systems do not have disaster recovery environments or the environments have not yet been configured to allow them to be restored at an alternate facility. In addition, Cybersecurity function management stated that the remaining system, the [redacted], was not tested because they are in the process of removing it from the list of systems supporting MEFs because it is not on the IRS's network. Cybersecurity function management further stated that the eight systems unable to meet the MTD were due to technical limitations. For example, the [redacted] and the [redacted] are legacy systems and can only be restored in 48 hours and 75 hours, respectively.

When the IRS does not test all systems for disaster recovery annually as required, it will be unable to assure system owners that their systems can be recovered within the RTOs. In addition, when the IRS is unable to recover its systems within 12 hours during disaster recovery testing, it will be unable to recover systems in a service outage or real disaster and meet its mission to provide taxpayers top-quality service.

Management Action: Cybersecurity function management stated that they have entered into a managed service agreement with a new replication vendor to provide disaster recovery environments for six of the nine systems which were not tested during FISMA Years 2021 and 2022 and have received assurances that these systems will be recoverable within the allowable RTOs. For the remaining three systems, they plan to move recovery capabilities to a virtualized environment. In addition, Cybersecurity function management provided documentation to support that the RTOs for six of the nine systems were tested in FISMA Year 2023 and met RTA requirements.

The CIO should:

Recommendation 4: Ensure that the Cybersecurity and Enterprise Operations functions, in conjunction with the business operating divisions and, as needed, with the new replication vendor, perform disaster recovery testing of the three systems that were not yet tested in FISMA Year 2023.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will perform disaster recovery testing of the three systems that were not tested in FISMA Year 2023.

Recommendation 5: Develop Plan of Action and Milestones to document the planned remediation actions to ensure that systems are recovered within the MTD for MEFs.

> **Management's Response:** The IRS agreed with this recommendation. The CIO will develop a Plan of Action and Milestones to document the planned remediation actions to ensure that systems are recovered within the MTD for MEFs.

Recommendation 6: Ensure disaster recovery testing is performed annually on systems supporting MEFs.

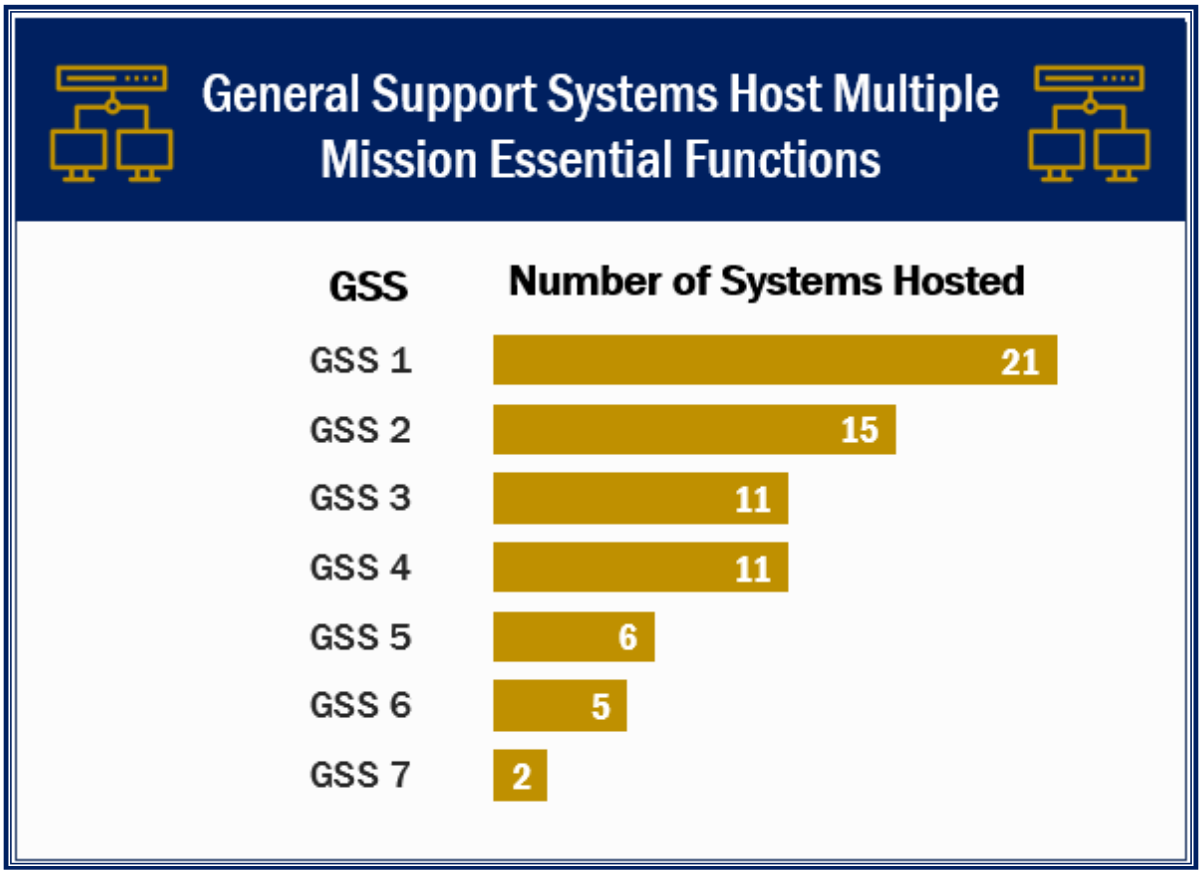
> **Management's Response:** The IRS agreed with this recommendation. The CIO will ensure disaster recovery testing is performed annually on systems supporting MEFs.

General support systems' (GSS) RTAs are not clearly documented

Our review of the *Application ISCP Testing Checklists* completed during FISMA Years 2021 and 2022 disaster recovery testing found that the checklist does not clearly document whether the hosting GSS is included as part of the system's RTA. The *Application ISCP Testing Checklist* has only one field to document the RTA. Specifically, the *System Restoration* section of the *Application ISCP Testing Checklist* does not provide separate fields to document the RTAs for the hosting GSS and the system and does not contain instructions or comments to indicate that the RTA includes both.

A GSS is an interconnected set of information resources that are under the same direct management control and share common functionalities that must be restored prior to restoring the system. A GSS normally includes hardware, software, information, data, applications, communications, and staff. Seven GSSs host the 50 systems supporting MEFs. Figure 6 presents the GSSs and the number of systems they host.

Figure 6: The GSSs and the Number of Systems that Support MEFs They Host (in Descending Number of Systems Hosted Order)



Source: Treasury Inspector General for Tax Administration's analysis of the systems' ISCPs and system security plans. Note: A system that supports the MEFs can be hosted by more than one GSS.

According to the Government Accountability Office's *Standards for Internal Control in the Federal Government* (Sept. 2014), documentation is a necessary part of an effective internal control system, and is required for the effective design, implementation, and operating effectiveness of an organization's internal control system. In addition, IRM 10.8.60 requires the Cybersecurity function to facilitate the testing of the ISCPs and the DRPs and to document the test results.

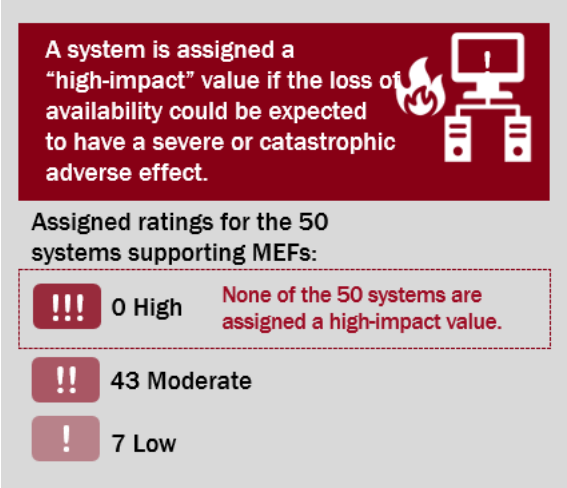
Cybersecurity function management stated that the RTA on the *Application ISCP Testing Checklist* does include the recovery times for both the hosting GSS and the system. However, Cybersecurity function management also agreed that the RTA is not clearly documented in the checklist. Without clearly documenting the GSS's RTA, subsequent comparisons of the system's RTA to the MTD may be inaccurate or misleading.

Management Action: At the end of our review, a statement was added to the *Application ISCP Testing Checklist* that clarifies the RTA includes the recovery times for both the hosting GSS and the system.

Systems Are Not Rated as High Impact for Availability

Federal standards require agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The impact values (high, moderate, and low) measure the impact on a system if its security would be compromised. A loss of availability is the disruption of access to or use of information or an information system.

To determine whether the impact value for the security objective of availability was appropriate, we applied the Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), criteria to the impact value assigned to each of the 50 systems. These standards state that a system is assigned a high-impact value if the loss of availability is expected to have a severe or catastrophic adverse effect on an organization's operations, assets, or staff. A severe or catastrophic adverse effect is defined as the loss of availability that may cause a severe degradation in or loss of mission capability to an extent and duration that the organization is unable to perform one or more of its primary functions. According to Cybersecurity function management, if an information system is assigned a high-impact value for either confidentiality, integrity, or availability, then the overall categorization of the system is rated as a high impact.



The IRS provided a March 2022 list of systems' impact values for the security objective of availability. The IRS assigned a moderate impact rating to 43 systems and a low impact rating to seven systems. None of the 50 systems were assigned a high-impact value for availability, even though they are essential to accomplishing the IRS's mission. We surveyed five system owners to determine whether the loss of availability of their systems would have a severe degradation in their ability to achieve their respective MEF. All five system owners or their delegates confirmed that the loss of availability of their system would cause a severe degradation.

As part of the Enterprise Life Cycle software development process, the Cybersecurity function requires system owners to submit a *Security Categorization Worksheet*. This process determines the system's impact value based on the Federal Information Processing Standards Publication 199. The *Security Categorization Worksheet* states that it is necessary to consider special factors, such as agency's mission, critical system functionality, and time-criticality, when assigning the impact value. Thereafter, during the annual security controls assessment process, the Cybersecurity function and the system owners discuss and reassess their systems' impact values for confidentiality, integrity, and availability.

The 50 systems were not categorized as a high-impact value for availability because the IRS did not fully consider all special factors, *e.g.*, critical system functionality and time-criticality, which are inherent to its mission. As a result, the systems' overall categorizations were not rated as high-impact and are not subject to additional security controls in the areas of audit and accountability, configuration management, contingency planning, and identification and

authentication. Consequently, the IRS cannot ensure that these additional security controls are in place and implemented.

Recommendation 7: The CIO should ensure that the Cybersecurity function and system owners jointly reassess the impact value of availability for all systems supporting the MEFs based on all factors as stated in Federal Information Processing Standards Publication 199 and the *Security Categorization Worksheet*.

Management's Response: The IRS agreed with this recommendation. The CIO will reassess the impact value of availability for all systems supporting the MEFs based on all factors as stated in Federal Information Processing Standards Publication 199 and the *Security Categorization Worksheet*.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective for this review was to assess the effectiveness of software and data recovery processes after a service outage or disaster for systems that support MEFs. To accomplish our objective, we:

- Reviewed Federal and IRS policies, procedures, and guidance for identifying, testing, and prioritizing the recovery of systems.
- Determined whether the Information Technology organization properly identified systems and incorporated system recovery priorities into the disaster recovery planning tool by reviewing business impact analyses and the ISCPs, and interviewing Cybersecurity and Enterprise Operations functions' personnel.
- Determined whether RTOs for the 50 systems were tested during FISMA Years 2021 or 2022, and whether the systems successfully recovered and were operational within the 12 hours MTD by reviewing disaster recovery testing documents and interviewing Cybersecurity and Enterprise Operations functions' personnel.
- Determined whether systems were appropriately assigned an availability security rating by applying the Federal Information Processing Standards Publication 199 criteria to the impact value assigned to each of the 50 MEF systems. We also surveyed five system owners to determine whether the loss of availability of their systems would have a severe degradation in their ability to achieve their respective MEF.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity and Enterprise Operations functions, located at the New Carrollton Federal Building in Lanham, Maryland, during the period January through December 2022. 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.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Carol Taylor, Audit Manager; Kanika Kals, Acting Audit Manager; Daniel Preko, Acting Audit Manager; Denis Danilin, Lead Auditor; and William Varnadore, Auditor.

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: the Government Accountability

Office's *Standards for Internal Control in the Federal Government*; Federal Information Processing Standards Publication 199; and various IRS policies, procedures, and guidance for disaster recovery planning and disaster recovery testing. We evaluated these controls by interviewing Cybersecurity and Enterprise Operations functions' personnel, surveying system owners, and reviewing relevant MEF and disaster recovery documentation.

Appendix II

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 36 systems not identified or incorrectly identified as systems that support MEFs in the disaster recovery planning tool (see Recommendation 2).

Methodology Used to Measure the Reported Benefit:

We reviewed the disaster recovery planning tool reports, dated June 7, 2022, for the [redacted] and determined that 29 of the 50 systems identified by the Cybersecurity function as supporting MEFs are not listed in the tool. In addition, we found seven systems in the disaster recovery planning tool incorrectly identified as systems supporting MEFs.

Appendix III

Map of Systems to Mission Essential Functions

	System Name	MEF 1 Processing Tax Remittances	MEF 2 Processing Tax Returns	MEF 3 Processing Tax Refunds
1	[redacted]	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]	[redacted]
5	[redacted]	[redacted]	[redacted]	[redacted]
6	[redacted]	[redacted]	[redacted]	[redacted]
7	[redacted]	[redacted]	[redacted]	[redacted]
8	[redacted]	[redacted]	[redacted]	[redacted]
9	[redacted]	[redacted]	[redacted]	[redacted]
10	[redacted]	[redacted]	[redacted]	[redacted]
11	[redacted]	[redacted]	[redacted]	[redacted]
12	[redacted]	[redacted]	[redacted]	[redacted]
13	[redacted]	[redacted]	[redacted]	[redacted]
14	[redacted]	[redacted]	[redacted]	[redacted]
15	[redacted]	[redacted]	[redacted]	[redacted]
16	[redacted]	[redacted]	[redacted]	[redacted]
17	[redacted]	[redacted]	[redacted]	[redacted]
18	[redacted]	[redacted]	[redacted]	[redacted]
19	[redacted]	[redacted]	[redacted]	[redacted]
20	[redacted]	[redacted]	[redacted]	[redacted]
21	[redacted]	[redacted]	[redacted]	[redacted]
22	[redacted]	[redacted]	[redacted]	[redacted]
23	[redacted]	[redacted]	[redacted]	[redacted]

[1] [redacted].

	System Name	MEF 1 Processing Tax Remittances	MEF 2 Processing Tax Returns	MEF 3 Processing Tax Refunds
24	[redacted]	[redacted]	[redacted]	[redacted]
25	[redacted]	[redacted]	[redacted]	[redacted]
26	[redacted]	[redacted]	[redacted]	[redacted]
27	[redacted]	[redacted]	[redacted]	[redacted]
28	[redacted]	[redacted]	[redacted]	[redacted]
29	[redacted]	[redacted]	[redacted]	[redacted]
30	[redacted]	[redacted]	[redacted]	[redacted]
31	[redacted]	[redacted]	[redacted]	[redacted]
32	[redacted]	[redacted]	[redacted]	[redacted]
33	[redacted]	[redacted]	[redacted]	[redacted]
34	[redacted]	[redacted]	[redacted]	[redacted]
35	[redacted]	[redacted]	[redacted]	[redacted]
36	[redacted]	[redacted]	[redacted]	[redacted]
37	[redacted]	[redacted]	[redacted]	[redacted]
38	[redacted]	[redacted]	[redacted]	[redacted]
39	[redacted]	[redacted]	[redacted]	[redacted]
40	[redacted]	[redacted]	[redacted]	[redacted]
41	[redacted]	[redacted]	[redacted]	[redacted]
42	[redacted]	[redacted]	[redacted]	[redacted]
43	[redacted]	[redacted]	[redacted]	[redacted]
44	[redacted]	[redacted]	[redacted]	[redacted]
45	[redacted]	[redacted]	[redacted]	[redacted]
46	[redacted]	[redacted]	[redacted]	[redacted]
47	[redacted]	[redacted]	[redacted]	[redacted]
48	[redacted]	[redacted]	[redacted]	[redacted]
49	[redacted]	[redacted]	[redacted]	[redacted]
50	[redacted]	[redacted]	[redacted]	[redacted]

Appendix IV

Systems With a Recovery Time Objective Greater Than 12 Hours
(in Descending Recovery Time Objective Order)

	System Name	Recovery Time Objective
1	[redacted]	[redacted]
2	[redacted]	[redacted]
3	[redacted]	[redacted]
4	[redacted]	[redacted]
5	[redacted]	[redacted]
6	[redacted]	[redacted]
7	[redacted]	[redacted]
8	[redacted]	[redacted]
9	[redacted]	[redacted]
10	[redacted]	[redacted]
11	[redacted]	[redacted]
12	[redacted]	[redacted]
13	[redacted]	[redacted]
14	[redacted]	[redacted]
15	[redacted]	[redacted]
16	[redacted]	[redacted]
17	[redacted]	[redacted]
18	[redacted]	[redacted]
19	[redacted]	[redacted]
20	[redacted]	[redacted]
21	[redacted]	[redacted]
22	[redacted]	[redacted]
23	[redacted]	[redacted]
24	[redacted]	[redacted]
25	[redacted]	[redacted]
26	[redacted]	[redacted]

[1] [redacted].

	System Name	Recovery Time Objective
27	[redacted]	[redacted]
28	[redacted]	[redacted]
29	[redacted]	[redacted]
30	[redacted]	[redacted]
31	[redacted]	[redacted]
32	[redacted]	[redacted]
33	[redacted]	[redacted]
34	[redacted]	[redacted]
35	[redacted]	[redacted]
36	[redacted]	[redacted]
37	[redacted]	[redacted]
38	[redacted]	[redacted]
39	[redacted]	[redacted]
40	[redacted]	[redacted]
41	[redacted]	[redacted]
42	[redacted]	[redacted]
43	[redacted]	[redacted]
44	[redacted]	[redacted]
45	[redacted]	[redacted]

Appendix V

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

April 26, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Jeffrey W. King,
Acting Chief Information Officer

Jeffrey King
Digitally signed by Jeffrey King
Date: 2023.04.26
14:25:19 -04'00'

SUBJECT: Draft Audit Report – Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement (Audit # 202220015)

Thank you for the opportunity to review and comment on the subject draft audit report. The IRS has robust disaster recovery plans in place to ensure continuous service during an outage. Your review of the agency's policies, procedures and guidance for identifying, testing and prioritizing the recovery of systems will help us further strengthen mission essential functions (MEFs) and the resiliency of the supporting systems.

We are pleased that the Treasury Inspector General for Tax Administration acknowledged the IRS enterprise Computing Center dual cording and power redundancy enhancements, which enable continuous service during an outage. We are actively working to implement the process improvements recommended in the draft report. As of November 2022, we have established disaster recovery environments for the remaining information systems supporting MEFs, and we tested the recovery time objective for all MEFs in preparation for the start of filing season. In addition, we have taken actions to ensure a maximum tolerable downtime of 12 hours for all MEFs and implemented procedures that provide an authoritative mapping of systems to MEFs.

The audit team identified opportunities to further strengthen our policies, procedures and guidance, and we remain committed to remediating issues timely. We agree with the recommendations and outcome measure in this report and have included a corrective action plan.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at 202-317-5000, or a member of your staff may contact Anthony Gillespie, acting director, Cybersecurity, Security Risk Management, at 240-613-2834.

Attachment

Attachment

TIGTA Audit 202220015 – Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement

Recommendations

RECOMMENDATION 1: The Chief Information Officer should implement a process to create and maintain an approved consolidated list mapping systems to mission essential functions (MEFs).

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief Information Officer will implement a process to create and maintain an approved consolidated list mapping systems to MEFs.

IMPLEMENTATION DATE: September 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should ensure that the disaster recovery planning tool is updated with the current systems supporting MEFs and periodically validated to ensure accuracy.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief Information Officer will update the disaster recovery planning tool with the current systems supporting the MEF and will periodically validate the tool to ensure accuracy.

IMPLEMENTATION DATE: September 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Operations

RECOMMENDATION 3: The Chief Information Officer should coordinate with system owners to ensure that they update their respective system's recovery time objective.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief Information Officer will coordinate with system owners to ensure that they update their respective system's recovery time objective.

IMPLEMENTATION DATE: October 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Attachment

TIGTA Audit 202220015 – Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement

RECOMMENDATION 4: The Chief Information Officer should ensure that the Cybersecurity and Enterprise Operations functions, in conjunction with the business operating divisions and as needed, with the new replication vendor, perform disaster recovery testing of the three systems that were not tested in Federal Information Security Management Act (FISMA) Year 2023.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief Information Officer will perform disaster recovery testing of the three systems that were not tested in FISMA Year 2023.

IMPLEMENTATION DATE: August 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 5: The Chief Information Officer should develop Plan of Action and Milestones to document the planned remediation actions to ensure that systems are recovered within the maximum tolerable downtime for MEFs.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief Information Officer will develop a Plan of Action and Milestones to document the planned remediation actions to ensure that systems are recovered within the maximum tolerable downtime for MEFs.

IMPLEMENTATION DATE: October 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 6: The Chief Information Officer should ensure disaster recovery testing is performed annually on systems supporting MEFs.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief Information Officer will ensure disaster recovery testing is performed annually on systems supporting MEFs.

IMPLEMENTATION DATE: March 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Attachment

TIGTA Audit 202220015 – Disaster Recovery of Information Systems That Support Mission Essential Functions Needs Improvement

RECOMMENDATION 7: The Chief Information Officer should ensure that the Cybersecurity function and system owners jointly reassess the impact value of availability for all systems supporting the MEFs based on all factors as stated in Federal Information Processing Standards Publication 199 and the Security Categorization Worksheet.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The Chief Information Officer will reassess the impact value of availability for all systems supporting the MEFs based on all factors as stated in Federal Information Processing Standards Publication 199 and the Security Categorization Worksheet.

IMPLEMENTATION DATE: April 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Appendix VI

Glossary of Terms

Term	Definition
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 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.
Campus	The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.
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.
Disaster Recovery	The ability of an organization to respond to a disaster or an interruption in services by implementing a DRP to stabilize and restore the organization's critical functions.
Disaster Recovery Plan	A plan created and maintained by the IRS Information Technology organization or any information technology service provider that defines the resources, roles, responsibilities, actions, tasks, and steps required to restore an information system to its full operational status at the current or alternate facility after a disruption.
Disaster Recovery Test	Full-scale functional exercise that involves recovering the information system and/or application on nonproduction equipment, in a simulated environment, or at the recovery location.
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.

Term	Definition
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and staff.
Information System Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate facility, in the event of emergencies, system failures, or disasters.
Plan of Action and Milestones	A management process that outlines weaknesses and delineates the tasks necessary to mitigate them.
Supervisory Control and Data Acquisition	A computer-based system for gathering and analyzing real-time data to monitor and control equipment that deals with critical and time-sensitive materials or events. It was first used in the 1960s and is now an integral component in virtually all industrial plant and production facilities.

Appendix VII

Abbreviations

CIO	Chief Information Officer
DRP	Disaster Recovery Plan
ECC	Enterprise Computing Center
FISMA	Federal Information Security Modernization Act of 2014
GSS	General Support System
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISCP	Information System Contingency Plan
MEF	Mission Essential Function
MTD	Maximum Tolerable Downtime
RTA	Recovery Time Actual
RTO	Recovery Time Objective

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

(800) 366-4484

By Web:

www.tigta.gov

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 23291

Washington, D.C. 20026

Information you provide is confidential, and you may remain anonymous.