EFFECTIVE DATE

(09-04-2015)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*.

BACKGROUND

(1) This IRM defines test, training, and exercise processes to ensure that:

a. Internal Revenue Service (IRS) information systems (IS) resources can be fully recovered in the event that IS contingency or disaster recovery plans must be activated.
b. Systems and their associated Information Systems Contingency Plans (ISCPs) or disaster recovery (DR) plans and procedures are exercised and/or tested to determine the capability of the IRS to recover and restore its systems in the event of a disruption, disaster, or catastrophe.

(2) FIPS 200 mandates the use of Special Publication 800-53 as baseline for the creation of agency IT security policy.

(3) IRM 10.8.62 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

MATERIAL CHANGES

(1) The following sections have been updated/clarified with this version of policy:

a. IRM 10.8.62.1, Overview: Updated the title of IRM 10.8.60.
b. IRM 10.8.62.1.2, Authority: Updated the title of IRM 10.8.60.
c. IRM 10.8.62.1.3, Scope: Updated the title of IRM 10.8.60, and defined FISMA, and ISCP,
d. IRM 10.8.62.1.4, Risk Acceptance and Risk-Based Decisions: Updated Hyperlink.
e. IRM 10.8.62.2.1, Security Risk Management (SRM) Organization: Removed DR Test, Exercise, and Evaluation (DRTEE) and changed to new group name DR Testing and Business Analysis (DRTBA).
f. IRM 10.8.62.2.1, Security Risk Management (SRM) Organization: Updated the time frame for updating the ISCP and added additional control in regards to functional exercises/test for FISMA reportable assets.
g. IRM 10.8.62.2.1, Security Risk Management (SRM) Organization: Removed Trusted Agent FISMA (TAF) and changed to new system Treasury FISMA Inventory Management System (TFIMS).
h. IRM 10.8.62.2.2, IRS Information Technology (IRS IT) Services Operations: Defined KISAM.
i. IRM 10.8.62.3.1.1., ISCP and DR Test, Training, and Exercises (TT&E) Requirement: Updated control in regards to annual tabletop exercises.
j. IRM 10.8.62.3.1.1.1, Test, Training, and Exercises (TT&E) Program: Added new control in regards to functional exercises.
k. IRM 10.8.62.3.1.1.3, Keystroke Procedures: Updated title from Disaster Recovery Keystroke Procedures to Keystroke Procedures.
l. IRM 10.8.62.3.1.1.5, Tabletop Exercises: Added new control in regards to ISCP and DR Testing Checklist.
m. IRM 10.8.62.3.1.1.8, Training: Added new control in regards to ISCP and DR Testing Checklist.

n. IRM 10.8.62.3.1.3.1, Tabletop Exercises: Updated the conference call invitation time period.
o. IRM 10.8.62.3..1.4.1, Scorecard: Updated control.
p. IRM 10.8.62.3.1.4.2, Treasury FISMA Inventory Management System (TFIMS): Updated subsection title from Trusted Agent FISMA (TAF) to Treasury FISMA Inventory Management System (TFIMS), and added additional control.
q. IRM 10.8.62: Updated all instances of DRTEE to DRTBA.
r. IRM 10.8.62: Updated all instances of TAF with TFIMS.
s. Exhibit 10.8.62-1, ISCP & DR Testing Checklist: Updated link and added and added link to the checklist.
t. Exhibit 10.8.62-2, ISCP Functional Exercise Methodology and Procedures: Updated link.
u. Exhibit 10.8.62-3, BOD ISCP & DR Testing Job Aid: Updated link.
v. Exhibit 10.8.62-4, Glossary and Acronyms: Added acronyms and definitions
w. Exhibit 10.8.62-5, References: Updated references.

(2) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.62 dated July 24, 2013, is superseded. This IRM supersedes all prior versions of IRM 10.8.62. This IRM supplements IRM 10.8.1, Information Technology (IT) Security Policy and Guidance; IRM 10.8.2, Information Technology Security Roles and Responsibilities; and IRM 10.8.3, Information Technology Audit Logging Security Standards. Also, this IRM supplements IRM 10.8.60.

AUDIENCE

IRM 10.8.62 shall be distributed to all personnel responsible for ensuring that ISCPs or DR plans and procedures are exercised and/or tested to determine the capability of the IRS to recover and restore its systems in the event of a disruption, disaster, or catastrophe. This policy applies to all employees, contractors, and vendors of the IRS.

Terence V. Milholland
Chief Technology Officer

10.8.62
Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process

Table of Contents

10.8.62.1
(09-04-2015)
Overview

(1) This IRM augments the security controls as defined in IRM 10.8.60, IT Service Continuity Management (ITSCM) Policy and Guidance (formerly Information Technology (IT) Disaster Recovery Policy and Guidance), to ensure Internal Revenue Service (IRS) information technology (IT) resources and business processes can be recovered.

10.8.62.1.1
(07-24-2013)
Purpose

(1) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets in order to:

a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
b. Prevent unauthorized access to IRS assets.
c. Enable IRS IT computing environments that meet the security requirements of this policy and support the business needs of the organization.

(2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.

(3) To configure less restrictive controls requires a risk-based decision. See the Risk Acceptance and Risk-Based Decisions (RBD) section within this IRM for additional guidance.

10.8.62.1.2
(09-04-2015)
Authority

(1) IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, establishes the security program and the policy framework for the IRS.

(2) This IRM augments the security controls as defined in IRM 10.8.60, IT Service Continuity Management (ITSCM) Policy and Guidance (formerly Information Technology (IT) Disaster Recovery Policy and Guidance) to ensure Internal Revenue Service (IRS) information technology (IT) resources and business processes can be recovered.

10.8.62.1.3
(09-04-2015)
Scope

(1) This IRM covers the methodology that can be applied to tabletop exercise events built around any type of information system-related plan, including, but not limited to, contingency and disaster recovery plans.

a. Per IRM 10.8.60, IT Service Continuity Management (ITSCM) Policy and Guidance and the guidance listed in the References section, the IRS shall exercise or test Information System Contingency Plans (ISCPs) and Disaster Recovery (DR) planning documents at least annually, for information systems prescribed by Public Law and the IRS.
b. Each Federal Information Security Management (FISMA) year (as defined in E-Government Act of 2002 (P.L. 107-347), *Title III, Federal Information Security Management Act (FISMA) of 2002),* the Director of Security Risk Management (SRM) shall issue a program memorandum specific to Information System Contingency Plan (ISCP) and DR testing for that FISMA year. The memorandum shall include any changes in regulations and testing requirements/guidance.

(2) The provisions in this manual apply to:

a. All offices and business, operating, and functional units within the IRS.
b. When IT is used to accomplish the IRS mission.
c. Individuals and organizations having contractual arrangements with the

IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate information systems that store, process, or transmit IRS Information or connect to an IRS network or system.

d. All IRS information and information systems. For information systems that store, process, or transmit classified information, please refer to IRM 10.9.1, *National Security Information*, for additional procedures for protecting classified information.

(3) The IRS shall ensure that the product and version selected is in accordance with IRS Enterprise Architecture (EA) Enterprise Standards Profile (ESP) that dictates the official products and versions of software within the IRS.

(4) The IRS shall ensure the application or system version is a version for which the vendor still offers standardized technical support.

(5) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive.

10.8.62.1.4
(09-04-2015)
Risk Acceptance and Risk-Based Decisions

(1) Any exception to this policy requires that the Authorizing Official (AO) make a Risk-Based Decision (RBD).

(2) Risk-Based Decision requests shall be submitted in accordance with IRM 10.8.1 and use Form 14201, as described in Request for Risk Acceptance and Risk-Based Decision Standard Operating Procedures (SOPs), available on the Enterprise FISMA Compliance SharePoint site via the Risk Acceptance Requests link at: *https://portal.ds.irsnet.gov/sites/CyberSRM/Public/SitePages/RiskAcceptance.aspx*.

(3) Refer to IRM 10.8.1 for additional guidance about risk acceptance.

10.8.62.2
(07-24-2013)
Roles and Responsibilities

(1) IRM 10.8.2, *Information Technology Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and computer security, and is the authoritative source for such information.

(2) The supplemental requirements provided below are specific to the implementation of Test, Training, and Exercise (TT&E) processes.

10.8.62.2.1
(09-04-2015)
Security Risk Management (SRM) Organization

(1) Refer to IRM 10.8.60 for additional guidance on Security Risk Management (SRM) program roles and responsibilities.

(2) SRM DR Testing and Business Anlaysis (DRTBA) personnel are responsible for:

a. Implementing an effective TT&E program on behalf of SRM. The program shall include at a minimum the following components:
i. Developing and preparing processes, templates, schedules, and procedures for exercises and tests.
ii. Coordinating with appropriate organizations, all ISCP and DR exercises and tests for FISMA-reportable assets in the FISMA master inventory.
iii. Documenting ISCP and DR exercise and test results and lessons learned.
iv. Monitoring ISCP reviews and updates, including ensuring that the plan is updated within 30 days or June 1 of the FISMA cycle, whichever comes

first, after the AO signs the ISCP Testing Checklist validating the performance of the annual tabletop, functional exercise, and/or DR test, or as major changes are made to the application/system.

b. Training Business Operating Division (BOD) and IRS IT personnel annually in their responsibilities related to ISCP and DR tests and familiarizing them with the ISCP and DR test processes.
c. Developing and maintaining a master ISCP and DR testing schedule for all FISMA-reportable assets in the FISMA master inventory.
d. Coordinating with BODs and IRS IT to identify recovery and support personnel needed to participate in planned tests and exercises.
e. Facilitating tabletop exercises of the ISCP to familiarize contingency personnel with the plan and recovery procedures within the plan and to identify inconsistencies and outdated information within the plan that could affect capabilities to support contingency operations.
f. Ensuring that all contingency and recovery tests performed by the IRS meet all Federal requirements and follow the standard guidelines set forth by the Director of SRM.
g. Coordinating with IRS IT personnel and BOD information system staffs to ensure that they perform the following tests for all FISMA-reportable applications and systems in the FISMA master inventory, or as directed in the annual SRM program memorandum:
   i. A functional exercise/test of the ISCP for a FISMA-reportable asset with a LOW or MODERATE availability rating.
   ii. DR test of the ISCP/DR plan for a FISMA-reportable asset with a high availability rating or an asset deemed as a Critical Infrastructure Protection (CIP) asset.
h. Validating that previous ISCP and DR related findings are reviewed prior to performance of tests and exercises to ensure that testing activities address corrective actions taken for resolution of the findings.
i. Collaborating with BOD and IRS IT personnel to create DR test cases, scenarios, milestones, and summarize all in the DR test plan.
j. Validating that a documented process is in place for creating system and application backup files.
k. Validating that a documented process is in place for storing backup files in an alternate offsite location by either electronically transferring them to that designated location or by creating tapes to ship to the alternate offsite storage facility.
l. Developing and maintaining scorecard/metrics to keep BOD personnel, Security Program Management Offices (PMOs), and Associate Chief Information Officers (ACIOs) informed about the status of ISCP exercising/testing progress.
m. Collaborating with IT representatives to define and document the evidence and artifacts needed to validate test activities.
n. Uploading completed exercise/test documents to Treasury FISMA Inventory Management System (TFIMS) system, uploading the updated ISCPs to TFIMS and to the Toolkit Suite Command Center (TSCC), and recording the completed test dates and ISCP completion dates into TFIMS.
o. Maintaining and updating ISCP and DR test processes, templates, and procedures.

10.8.62.2.2
(09-04-2015)
IRS Information Technology (IRS IT) Services Operations

(1) IRS IT operations provides support for all IRS information technology with only documented exceptions. During the ISCP tabletop exercises, DR exercises and DR tests, IRS IT shall:

a. Support the activities that relate to exercises and tests of the ISCP and procedures.
b. Perform system backup, rebuild, recovery, reconstitution, cutover, relocation, etc., for systems supported and/or owned by IRS IT.
c. Provide documented backup procedures to include information about the backup frequency, encryption of backup media, offsite storage, and timelines for receipt of backup media from offsite storage during normal working hours and after hours.
d. Perform ISCP exercises and DR tests annually for applications and systems supported and/or owned by IRS IT.
e. Provide resources for ISCP and DR exercises and tests annually for applications and systems supported and/or owned by IRS IT, including staffing and procuring funded backup solutions and equipment for DR tests.
f. Complete the ISCP & DR Testing Checklist (TFIMS artifact) (see Exhibit 10.8.62-1) to report the results of all functional exercises, recovery tests, and operational recoveries of production servers that host applications in the FISMA master inventory.
g. Provide annual recommendations for updates to the ISCP Functional Exercise Methodology and Procedures (see Exhibit 10.8.62-2).
h. Facilitate planning meetings between various IRS IT and BOD areas in preparation for scheduled DR tests.
i. Create the schedule of daily exercise activities and milestones chart in preparation for scheduled DR tests.
j. Coordinate with appropriate areas in creation of DR test scenario and scope.
k. Coordinate with Knowledge Incident/Problem Service Asset Management (KISAM) project office and Enterprise Service Desk for support and use of KISAM test system during DR tests.
l. Coordinate with appropriate areas (Cybersecurity, BODs, AD, etc.) to develop a DR test schedule to include necessary FISMA assets.
m. Facilitate post DR test meetings with test participants to review issues and resolutions to determine if any followup actions are required by appropriate areas.
n. Work with appropriate areas to close action items that appear on the Vulnerabilities Matrix.

(2) The appropriate IRS IT organizations responsible for supporting the ISCP shall review, update, exercise, and/or test the ISCP at least annually (or as significant changes occur).

(3) Information system resources owned by Contractors or Vendors on behalf of the IRS and by BODs shall also be compliant with the IRS IT requirements identified within this IRM.

10.8.62.2.3
(07-24-2013)
Business Operating Division (BOD) Information System Owners

(1) The BOD/Information System Owner is responsible for:

a. Ensuring that applications' ISCP is exercised and tested annually. (For step-by-step procedures see the BOD ISCP & DR Testing Job Aid, Exhibit 10.8.62-3.)

b. Ensuring that the most current version of the ISCP is kept in the TFIMS authoritative repository for FISMA documentation, and that the current plan is used during all ISCP exercises and tests.
c. Reviewing the most current version of the Plan of Action and Milestones (POA&M) prior to performing exercises or tests to identify ISCP- and DR-related issues, both open and recently closed, for inclusion in the current exercise or test to determine if the annual ISCP tests could provide a closing action for the finding.
d. Completing the ISCP & DR Testing Checklist (see Exhibit 10.8.62-1) prior to tabletop exercises and ensuring that tabletop participants each receive a copy of the completed Checklist for use during the exercise.
e. Participating in tabletop exercises using the ISCP & DR Testing Checklist (the Checklist) to ensure that applications' ISCPs are kept current and accurate and participants validate roles and procedures documented in the plans.
f. Providing annual recommendations for updates to the ISCP test methodology and templates.
g. Ensuring that the application's/system's AO receives and reviews the results, summary findings, and ISCP changes after tabletop and functional exercises. The AO shall validate that tabletop and functional exercises are completed by signing and dating the ISCP & DR Testing Checklist. The BOD shall then ensure that the changes from the Checklist are incorporated into the ISCP within 90 calendar days from the date the AO signed the Checklist, or June 1, whichever comes first.
h. Forwarding the completed exercise documentation for uploading into TFIMS.
i. Performing the IRS IT activities during ISCP exercises and tests for BOD-owned applications that are not supported by IRS IT.

(2) Information system resources owned by Contractors or Vendors on behalf of the IRS shall also be compliant with the IRS IT requirements identified within the IRS IT Operations section in this IRM.

10.8.62.2.4
(07-24-2013)
Information System Contingency Plan (ISCP) Coordinator

(1) The ISCP Coordinator, having selected and implemented the backup and system recovery strategies, must designate appropriate teams to implement the strategy.

10.8.62.3
(07-24-2013)
IT Security Controls

(1) Refer to IRM 10.8.1 for the other security control families other than Contingency Planning.

(2) The Contingency Planning controls in IRM 10.8.60 supplement the Contingency Planning requirements defined in IRM 10.8.1.

(3) In addition to the Contingency Planning requirements defined in IRM 10.8.1 and IRM 10.8.60, the following sections for contingency planning and disaster recovery test, training, and exercising requirements shall be applied.

10.8.62.3.1
(07-24-2013)
CP – Contingency Planning (CP)

(1) IRM 10.8.62 satisfies the requirements of this security control with regard to policy.

10.8.62.3.1.1
(09-04-2015)
ISCP and DR Test, Training, and Exercises (TT&E) Requirement

(1) All IRS applications and systems listed in the FISMA master inventory are required to undergo a tabletop exercise of the ISCP annually for all categories of potential impact on availability.

(2) In addition to an annual tabletop exercise, applications, and systems with a LOW and MODERATE potential impact on availability also require that a functional exercise (described in the Functional Exercises section) be performed annually.

(3) Applications and systems that are CIP assets or that have HIGH potential impact on availability, in addition to the annual tabletop exercise, must also undergo testing (described in DR Tests section) which is equivalent to a DR activity such as a cutover test or complete restoration of the system.

(4) All annual testing and exercises must be completed during the July 1 through June 30 timeframe each year in order to meet IRS FISMA reporting requirements.

(5) For each tabletop exercise activity conducted, the results shall be documented in the ISCP & DR Testing Checklist testing artifact with all changes identified in the exercise.

10.8.62.3.1.1.1
(09-04-2015)
Test, Training, and Exercises (TT&E) Program

(1) A testing program in non-disaster so that IRS leadership and personnel have familiarity with contingency plans and procedures and validates the IRS' contingency capabilities through regular tests, training, and exercises. It can also identify issues or deficiencies for remediation.

(2) Exercises and tests offer different ways of ensuring that ISCPs provide viable and actionable procedures to recover or restore IRS systems and applications to their original state in the event of a disruption.

(3) Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-84, **Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities**, for guidance on establishing an effective ISCP testing program and the various methods and approaches for conducting tabletop exercise activities.

(4) All tests and exercises shall include some kind of determination of the effects on the organization's operations and provide for a mechanism to update and improve the plan as a result.

(5) The depth and rigor of ISCP testing activities increases with the FIPS 199 availability security objective. Refer to the ISCP templates (FIPS 199 low, moderate, high) in NIST SP 800-34 for details for conducting testing activities appropriate to their respective impact level.

- **For LOW and MODERATE-impact systems, a tabletop and functional exercise shall be conducted annually to ensure that a basic level of recovery capability is available for all IRS FISMA assets.** The tabletop should follow a scenario that simulates a disruption, include points of contact whose roles appear in the ISCP, be attended by the business and system owners or responsible authority, and be facilitated by DRTBA personnel. The functional exercise should include an element of system recovery from backup media and is performed by IRS IT or BOD IT personnel on behalf of the BODs.

- **For HIGH-impact systems or Critical Infrastructure Protection assets, a tabletop exercise and a full-scale end-to-end or DR test shall be conducted annually to ensure that a full recovery capability is available for all the most critical IRS FISMA assets.** The tabletop should follow a scenario that simulates a disruption, include points of contact whose roles appear in the ISCP, be attended by the business and system owners or responsible authority, and be facilitated by DRTBA personnel. The full-scale test should include a system restoration at the alternate location. This could include additional activities such as full notification and activation of key personnel to the recovery location, recovery of a server or database from backup media or setup, and processing from a server at an alternate location. The test shall also include a full recovery and reconstitution of the information system to a known state.

10.8.62.3.1.1.2
(10-04-2012)
Information System Contingency Plan (ISCP)

(1) The ISCP shall provide procedures and capabilities for recovering a system or application in the event of an information system disruption. The plan shall address the resources, roles, responsibilities, and procedures for restoration of information systems and recovery of business applications and processes after a disruption.

10.8.62.3.1.1.3
(09-04-2015)
Keystroke Procedures

(1) The keystroke procedures located within the ISCP are an information system-focused part of the plan that applies to major, usually catastrophic, events that deny access to the normal facility or information system for an extended period of time. The plan is designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.

(2) The purpose of the keystroke procedures is to provide detailed step-by-step procedures to facilitate recovery of capabilities at an alternate site; the scope is information system-focused and limited to major disruptions with long-term effects.

10.8.62.3.1.1.4
(07-24-2013)
Exercises

(1) As defined in NIST SP 800-84:

a. An exercise is a simulation of an emergency designed to validate the viability of one or more aspects of an ISCP.
b. Personnel with roles and responsibilities in a particular ISCP meet to validate the content of a plan through discussion of their roles and responses to emergency situations, execution of responses in a simulated operational environment, or other means of validating responses that do not include using the actual operational environment.
c. Exercises are scenario-driven, such as a power failure in one of the organization's computing centers or a fire causing certain systems to be damaged, with additional situations often being presented during the course of an exercise.
d. Exercises help to identify gaps and inconsistencies within ISCPs and procedures, as well as cases where personnel need additional training or when training needs to be changed. The deficiencies identified in exercises are documented as part of the exercise process.

10.8.62.3.1.1.5
(09-04-2015)
Tabletop Exercises

(1) Tabletop exercises are discussion-based exercises only and do not involve deploying or recovering systems, equipment, or other resources. Personnel meet to discuss their roles during an emergency and their responses to a particular emergency situation. During the tabletop exercise, participants also identify information or procedures in the plan to identify outdated information or procedures in the plan that need to be updated and corrected.

(2) The objectives of any tabletop exercise are to validate the content of the ISCP and related policies and procedures, validate participants' roles and responsibilities as documented in the plan, and validate the interdependencies documented in the plan.

(3) The ISCP and DR Testing Checklist is an IRS internal document designed to assist BODs and support staffs in navigating through tabletop exercise events. See Exhibit 10.8.62-1 for the Checklist Template at the end of this document.

10.8.62.3.1.1.6
(10-04-2012)
Functional Exercises

(1) Functional exercises allow personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment. A functional exercise is designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., backup procedures, communications, emergency notifications, information system equipment setup).

(2) Functional exercises vary in complexity and scope, from validating specific aspects of a plan (e.g., backup retrieval, reading backup data, and validation of offsite storage) to exercising all plan elements in a simulation.

(3) Functional exercises allow staff to execute their roles and responsibilities as they would in an actual emergency situation, but in a simulated manner.

10.8.62.3.1.1.7
(07-24-2013)
DR Tests

(1) In the context of DR, a test is the method used to evaluate the organization's readiness and ability to recover a system from varying degrees of non-functioning to its original functional state by following authorized keystroke procedures. Components of tests are listed in these sections, such as using quantifiable metrics to validate the operability of an information system or system component in an operational environment specified in an ISCP.

Note: The term *test* is reserved for testing system hardware/software/OS recovery capability or system components; it is not used to describe *exercising* plans.

(2) Tests are used to measure the effectiveness and suitability of the processes and procedures contained in ISCPs related to the systems being tested and to evaluate compliance with an information system contingency. In the event of a disaster or disruption the goal is to be able to use tested ISCPs to ensure that following documented operational procedures and plans will result in successful recovery of business applications and systems.

(3) The scope of tests can range from individual system components or systems to comprehensive tests of all systems and components that support an ISCP. Examples of tests are:

a. Component tests - Restoring a system by retrieving backup data from offsite storage and loading the data to test the usability of the data.
b. System tests - Restoring multiple components such as the operating system, database, and system software by using data stored offsite.

(4) A test is conducted in as close to an operational environment as possible, testing components, or systems used to conduct daily operations.

(5) If feasible, an actual test of the components or systems used to conduct daily operations for the organization can be used to comply with the ISCP testing program's annual requirements.

(6) Tests that result in components or systems malfunctioning or becoming inoperable could indicate problems in personnel training or in DR plans and procedures.

(7) Each information system component shall be tested to confirm the accuracy of individual recovery procedures.

(8) Each information system shall have a contingency plan that addresses the following areas, as applicable:

- Notification procedures
- System recovery on an alternate platform from backup media
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations
- Other planned tests (where coordination is identified, i.e., Continuity of Operations Plan (COOP), Business Continuity Plan (BCP))

(9) Additional test plan requirements:

a. The test plan shall include a schedule detailing the timeframes for each test and test participants.
b. The test plan shall clearly delineate scope, scenario, and logistics.
c. The scenario chosen may be a worst-case incident or an incident most likely to occur.
d. It should mimic reality as closely as possible.

10.8.62.3.1.1.8
(09-04-2015)
Training

(1) Training refers to informing personnel of their roles and responsibilities within a particular information system plan and teaching them skills related to those roles and responsibilities, thereby preparing them for participation in exercises, tests, and actual emergency situations related to the information system plan.

(2) The scheduling of training sessions will be coordinated closely with the schedules for ISCP tabletop exercises, functional exercises, and DR tests.

(3) Training sessions will emphasize studying and understanding the following documents in preparation for participating in each test or exercise:

a. ISCP – Participants will be able to answer questions about the purpose of the plan, system recovery procedures, specific application processes, recovery roles and responsibilities, notification procedures, and all appendices included in the plan.
b. ISCP & DR Testing Checklist (see Exhibit 10.8.62-1) – The ISCP Testing Checklist shall be included in the training sessions scheduled prior to all testing and exercise events. Participants will gain knowledge of the purpose of the Checklist, how to complete it, and the procedures for its use during the scheduled exercises and tests of the ISCP.

c. ISCP and DR Exercise/Testing Schedule – Participants will gain knowledge of the contents of the schedule, how and why it is created, and how it is vetted. The schedule ensures that every application and system in the FISMA master inventory is included in exercise and testing activities required under FISMA and that the dates are acceptable.
d. FISMA Contingency Plan Computer Controls – Participants will gain knowledge of the Contingency Plan family of security controls (NIST 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*) and how exercising and testing of plans will address deficiencies in compliance with those controls.

(4) Recovery personnel shall be trained on the following plan elements:

- Purpose of the plan
- Cross-team coordination and communication
- Reporting procedures
- Security requirements
- Team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases)
- Individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases)

10.8.62.3.1.2
(07-24-2013)
ISCP & DR Exercise and Testing

(1) Two weeks before each new FISMA reporting cycle begins (July 1), the DRTBA Staff shall solicit comments from BOD and IRS IT Point-of-Contacts (POCs) to evaluate the lessons learned from the previous ISCP and DR test period to ensure that the test process continues to be viable, cost-effective, resource efficient, and compliant with new regulations. The ISCP & DR Testing Checklist template and ISCP template will be reviewed and revised as necessary.

(2) DRTBA Staff will work with appropriate Organizations to develop a testing schedule each year to exercise or test the ISCP, for all the applications and systems found in the FISMA master inventory.

(3) The DRTBA Staff will facilitate all tabletop exercises for each FISMA reporting cycle. During the Security Assessment and Authorization (SA&A) process, DRTBA personnel will collaborate with the FISMA Certification Program Office (CPO) to ensure that the ISCP testing schedule is in sync with the SA&A process and the Security Control Assessment schedule.

(4) The schedule will be reviewed by IRS IT and BOD personnel to ensure that ISCP tabletop exercises, functional exercises, and DR tests are scheduled to coordinate each application, or more than one application if requested on a case-by-case basis, using the following keys:

a. Platform
b. System
c. BOD
d. Site

(5) DRTBA will present the revised ISCP & DR Testing Checklist template, ISCP template, the previous POC lists, and the new ISCP and DR Exercise/Testing Schedule to the Security PMO to initiate the annual exercise and testing activities. The PMO will vet the schedule and the POC list with their respective organizations and will coordinate errors, questions, and changes with the DRTBA Staff through the *IT IT DR Mailbox. When the information is finalized

and approved by the Council, DRTBA will use the approved schedule and POC lists to begin the new testing cycle.

(6) The approved schedule is published, distributed, and followed to perform ISCP and DR exercises and tests. The schedule includes:

a. A designated DRTBA Staff member as the Facilitator for each tabletop exercise.
b. Changes as submitted by BOD and IRS IT authorized personnel, documented by DRTBA, and distributed when updated.
c. Modifications as needed during the annual FISMA reporting cycle.

(7) DRTBA will enter the completed testing and updated ISCP dates in TFIMS for every application and system listed in the FISMA master inventory.

(8) Changes in dates of scheduled exercises or tests will be coordinated through the IRS IT and BOD Security PMOs who will coordinate with DRTBA to establish a new date. DRTBA will update the schedule with the new exercise/test date. However, no tests will be scheduled after April 30 of each FISMA reporting cycle and all tests will be completed by June 1 to facilitate loading of all completed test packages in TFIMS by the FISMA reporting deadline of June 30.

(9) DRTBA will schedule and present training for all BOD and IRS IT participants to ensure that they are ready to participate in the exercise. DRTBA will answer any questions the POCs may have about the exercise/test process or the Checklist.

10.8.62.3.1.2.1
(07-24-2013)
ISCP & DR Testing Checklist

(1) The Checklist is a three part form that allows BODs and Support Organizations to document multiple exercise/test activities on one form to create one authoritative source to standardize and simplify the archival process.

(2) Part A of the Checklist is the Tabletop Exercise, Part B is the Functional Exercise, and Part C is the ASPE Test or Production Operational Recovery which documents DR Testing activities. See Exhibit 10.8.62-1 for a copy of the Checklist.

(3) The ISCP & DR Testing Checklist provides a step-by-step process to guide participants through the most pertinent sections of the ISCP. The Checklist provides an area to document changes for each section in the ISCP and changes to procedures that might be needed. The Checklist also provides areas to document the results of functional exercises and DR tests, if applicable.

(4) The Checklist standardizes the walkthrough process for all applications and systems, and documents all testing activities and ISCP changes. The Checklist serves as the validated artifact for the tabletop exercise events and ISCP update activities. The Checklist and supporting documentation is uploaded to TFIMS after it has been reviewed and signed by the AO.

(5) The Checklist is used to train personnel in their contingency roles and responsibilities with respect to their application or system.

(6) Completion of the Checklist documenting performance of the required exercises and/or tests provides the artifact in TFIMS to validate that the

following family of controls, if appropriate, are met (Reference NIST 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems*):

a. CP-2 Contingency Plan – The ISCP is pulled from TFIMS and distributed to each participant for the tabletop exercise validating that the plan exists.
b. CP-3 Contingency Training – The requirements, roles and responsibilities, and recovery procedures are discussed as the ISCP is exercised during the tabletop exercise.
c. CP-4 Contingency Plan Testing and Exercises – Use of the ISCP & DR Testing Checklist to annotate the results of the exercise/test, including entering the completed test date and the AO's signature and date, provides evidentiary documentation that the plan was exercised and tested.
d. CP-6 Alternate Storage Site – As the tabletop exercise is performed, the ISCP is reviewed and discussed to ensure that information about backup procedures and an alternate storage site is identified and included in the plan. If backup procedures or alternate storage sites are not in place, a summary finding is annotated on the Checklist to document this issue.
e. CP-7 Alternate Processing Site – During tabletop exercises, the Application Test Plan shall be reviewed to determine if an alternate processing site, based on the criticality of the application, is a viable option. In the event the infrastructure does not recover at a site where a disruption has occurred, the application Business Owner would have to plan accordingly. Establishment of an alternate processing site could provide a DR solution.
f. CP-8 Telecommunication Services – Tabletop exercises for IRS IT systems and business applications not supported by IRS IT will include discussions about the telecommunication infrastructure and its DR capabilities, backup procedures, and validation that a DR plan exists for its recovery.
g. CP-9 Information System Backup – Discussions during tabletop exercises will focus on the ISCP to ensure that backup procedures are documented and implemented. The procedures will include information about the backup frequency, encryption of backup media, offsite storage, and timelines for receipt of backup media from offsite storage during normal working hours and after hours. If backup procedures have not been implemented, a summary finding is annotated on the checklist to document this issue.
h. CP-10 Information System Recovery and Reconstitution – Tabletop discussions for this control will focus on the information in Section 5 of the ISCP to validate that procedures are in place to recover and reconstitute IRS IT systems and applications.

(7) Each BOD will be responsible for identifying a Data Collector who will be responsible for documenting the exercise and/or testing activities as they occur and populating the appropriate parts of the Checklist with the description of the activities.

(8) The ISCP & DR Testing Checklist will be used as an artifact in TFIMS to document all tabletop exercises, functional exercises, and DR tests that are scheduled.

10.8.62.3.1.3
(07-24-2013)
Conducting Exercises and Tests

(1) The following sections provide procedures and guidance for performance of the activities for the testing and exercising portions of the TT&E Program.

(2) When a production program is being tested in the disaster recovery environment (on IRS computer systems in an IRS facility), live data from the production backup media, including entire file(s) and database(s) involved, may be used to test the backup recovery capability of that production data. IRS employees and their contractors with approved access are not required to submit a Live Data Waiver in order to test the restoration/recovery of the live data on the production backup media.

10.8.62.3.1.3.1
(09-04-2015)
Tabletop Exercises

(1) DRTBA will schedule and present training for all BOD and IRS IT participants to prepare them for the current FISMA Cycle ISCP exercises and tests. DRTBA will answer any questions the POCs may have about the test process or the Checklist.

(2) Based on the approved testing schedule and IRS IT/BOD POC list, the assigned DRTBA Facilitator will send the standard conference call invitation to all participating POCs **30 days** prior to the day of the exercise. The assigned DRTBA Facilitator shall provide the ISCP and DR Testing Checklist with items 1-4 of the checklist pre-populated by the DRTBA to the Data Collector (who is assigned by the BOD Security PMO or AO POC as delegated by the AO).

(3) Using the most current version of the ISCP and POA&M stored in TFIMS the Data Collector populates items 1 through 7 and Part A on the Checklist, and if necessary meets with appropriate BOD or IRS IT personnel to complete this task. When exercising and discussing the ISCP, the Data Collector and BOD or IRS IT personnel shall capture noteworthy changes prior to the tabletop. This promotes a more efficient exercise and discussion regarding how to recover the application/system.

(4) After the Checklist is populated, and at least **5 work days** prior to the tabletop, the Data Collector shall forward the checklist and the current ISCP to all recipients, including the DRTBA Facilitator. If assistance is needed, the Data Collector shall notify the Facilitator or the designated DRTBA Contacts noted in the invitation.

(5) During the tabletop exercise, the Data Collector is responsible for capturing on the Checklist all changes, observations, lessons learned, and summary findings that result from the tabletop discussions. **The Date Exercise Completed** block must be entered with the date the tabletop was performed.

(6) The Data Collector then has **7 work days** to update the Checklist with the result of the exercise. The Facilitator will coordinate with the Data Collector as needed to provide guidance and to compare notes taken during the exercise.

(7) After the Checklist update is completed, the Data Collector shall send it to the *IT IT DR Mailbox with a copy to the BOD Security PMO. DRTBA shall enter the date the checklist was received in the test tracking log and forward it to the assigned DRTBA Facilitator, who shall review the Checklist to ensure that all information has been recorded. If Checklist corrections are needed, the Facilitator will coordinate with the Data Collector to ensure that the modifications are made.

(8) Depending on the required exercises or tests, the DRTBA Facilitator can hold the Checklist until all other testing has been completed and can be documented in Part B or Part C of the Checklist. If no other testing is required, the

DRTBA Facilitator shall send the Checklist back to the Data Collector and the BOD Security PMO within **7 work days** for final signature (digital signature is acceptable) by the AO or the AO Designee.

(9) The AO or AO Designee has a **30 calendar day** maximum timeframe for signing the Checklist unless the June 1 deadline is less than 30 days, then the checklist is due on June 1. The AO or Designee shall return the signed Checklists to DRTBA as soon as possible to avoid delays in uploading the completed test packages into TFIMS prior to the end of the FISMA reporting cycle.

(10) After the AO has signed the Checklist, the Data Collector or BOD Security PMO shall submit it to the *IT IT DR Mailbox, and the designated DRTBA Staff member shall load the Checklist and all supporting documentation into TFIMS.

(11) BOD and IRS IT organizations have **90 calendar days** from the signature date of the AO on the Checklist, or June 1, whichever comes first, to revise the ISCP with the changes identified in the tabletop exercise. After changes are made, the BOD/IRS IT designated POC shall send the revised ISCP to the *IT IT DR Mailbox for upload into TFIMS by the designated DRTBA Staff member. If no changes were noted, the existing version of the ISCP will remain in TFIMS unchanged.

10.8.62.3.1.3.2
(07-24-2013)
Functional Exercises

(1) Functional exercises are performed by IRS IT personnel or by the BOD's information system personnel when the application is not supported by IRS IT. During the performance of the functional exercises, IRS IT personnel or BOD information system personnel will complete the ISCP & DR Testing Checklist Part B as they go through the exercise. (See Exhibit 10.8.62-1.)

(2) See Exhibit 10.8.62-2, ISCP Functional Exercise Methodology and Procedures. This exhibit provides step-by-step procedures for a backup retrieval and sampling pull for functional exercise activities. All functional exercises will be conducted using the approved procedures in Exhibit 10.8.62-2.

(3) As the production environment implements new technologies, strategies, and procedures, IRS IT and SRM shall assess when to modify Exhibit 10.8.62-2 procedures to ensure that functional exercises can be performed to accommodate the updated production environment.

(4) During the functional exercise, the IRS IT or BOD information system personnel will take screen prints of the backup tool index header and tape or server listing to validate the method used to backup system files and/or application data files. Take additional screen prints to validate that the data on the backup media is readable. The IRS IT or BOD information system personnel will also provide evidence in the form of routing sheets, logs, or e-mail requests proving the length of time needed between the request for backup data from offsite storage and the receipt of that data at the test site.

(5) IRS IT or BOD information system personnel shall also provide evidence to validate that documented backup procedures are in place including information about the backup frequency, encryption of backup media, offsite storage site, and timelines for receipt of backup media from offsite storage during normal working hours and after hours.

(6) If no documented procedures describe the backup process, annotate the Summary Findings section in Part B of the Checklist to document this issue.

Annotate the Summary Findings section if the backup tapes are corrupted or if evidence cannot captured for the exercise.

(7) At the end of the functional exercise, the IRS IT or BOD information system personnel shall update the Checklist with results from the exercise. The IT personnel performing the exercise will submit the populated Checklist and supporting evidentiary documentation to DRTBA at *IT IT DR Mailbox within 10 work days from the completion of the exercise.

(8) DRTBA will ensure that the populated Checklist received from the IT personnel who performed the functional exercise is consolidated with the Tabletop Exercise Checklist. DRTBA will review the evidence submitted for the functional test to ensure it supports the testing was completed. DRTBA wil then create the evidence package and finalize the results of the completed exercises in preparation for the AO signature.

(9) The AO POC will present the completed test package to the AO for review of the exercise results, the summary findings, and final validation. The AO shall sign and date the Checklist and the AO POC shall return the signed Checklist to DRTBA at *IT IT DR Mailbox for final action.

(10) Upon receipt of the signed Checklist and supporting documentation from the AO POC, DRTBA shall upload the Checklist into TFIMS as the validated artifact along with all supporting documentation.

10.8.62.3.1.3.3
(10-04-2012)
DR Tests

(1) IRS is required to perform DR tests on all applications with a High Availability Impact and for CIP assets. These tests are designed to evaluate IRS readiness to cutover, relocate, restore, or rebuild IRS systems/applications.

(2) DR tests involve activities such as performing cutovers from one platform or system to another, relocation of systems/applications, or recovery of platforms and their hosted applications. As DR tests are performed on systems, sites, or platforms, hosted applications can benefit from these tests through coordination of the application ISCP review and the DR test activities.

(3) IRS IT personnel perform DR tests unless IRS IT does not support the application. The BOD's information system personnel perform DR tests when the application is not supported by IRS IT. During the performance of the DR Test IRS IT personnel or BOD information system personnel shall complete the ISCP & DR Testing Checklist Part C, and Test Case templates as they go through the test. (See Exhibit 10.8.62-1.)

(4) The DRTBA Staff will coordinate with IRS IT organizations to identify components, systems, and/or comprehensive tests to be planned based on FISMA, Treasury, and NIST requirements, and IRS executive-level priorities.

(5) Production operational recoveries can also be considered in meeting FISMA and DRTBA program requirements. The Service may also consider combining tests with planned operational activities, such as restoring a backup, moving a server from one room to another, upgrading or patching operating systems or applications, or changing hardware components (e.g., swapping hard drives, replacing a failed power supply). The results of this collaboration will define the scope and objectives for the tests.

(6) The DRTBA Staff will collaborate with designated BOD POCs to determine if the tests identified in collaboration with IRS IT are compatible with the priorities and processing timeframes of the Business Unit. DRTBA will coordinate with BODs to determine the level of involvement required from the BOD POCs.

(7) The DRTBA Staff shall create a test schedule based on IRS and FISMA requirements, FISMA timeframes, and business processing priorities.

(8) The DRTBA Staff will coordinate the following activities with IRS IT and BOD POCs to ensure that the Test Case Template, Test Activities Worksheet, ISCP & DR Testing Checklist, Summary Report, and all testing documentation is completed before, during, and after testing. DRTBA will:

a. Coordinate with the designated IRS IT organization to ensure that population of the Test Case Template by the IRS IT and BOD POCs with pertinent information about the test such as scope detail, objectives, recovery personnel, support personnel, and test activities is performed.
b. Ensure that IRS IT POCs identify the files needed to be transmitted in preparation for the tests and determine the date for transmission of data via IRS approved protocols.
c. Coordinate with Enterprise Computing Center (ECC) Security Management Office (SMO) personnel to reserve a conference room to hold meetings before, during, and after planned test activities as needed.
d. Coordinate with stakeholders to ensure that pre-test activities are completed.
e. Facilitate the creation of procedures to terminate the test in case operational issues necessitate it.
f. Coordinate with IRS IT and BOD POCs to ensure that all test participants including end users are familiar with the test termination procedures.
g. Coordinate with IRS IT POCs to ensure that BOD end users are not adversely affected during planned test activities.
h. Coordinate with IRS IT POCs at the end of the test to ensure that test deactivation procedures are completed.
i. Review and evaluate the completed Test Case Template, worksheets, findings, corrective actions, and all test evidentiary documentation.
j. Populate a test Summary Report to include findings, corrective actions, lessons learned, and summarize test worksheet results.
k. Facilitate post test meetings as needed to go over Summary Report, lessons learned, and corrective actions.

10.8.62.3.1.4
(07-24-2013)
Annual FISMA Reporting Cycle Activities

(1) The following sections describe the activities needed to capture the results of the ISCP testing program. Reporting and testing artifact control are critical to the successful completion of the exercise and testing process each year and are performed on a regular basis throughout the FISMA Reporting Cycle.

10.8.62.3.1.4.1
(09-04-2015)
Scorecard

(1) For the purposes of reporting on the progress of exercises and testing, DRTBA shall maintain a scorecard to document the progress of the ISCP tabletop and functional exercises and the status of the DR tests.

10.8.62.3.1.4.2
(09-04-2015)
Treasury FISMA Inventory Management System (TFIMS)

(1) DRTBA shall input all activities and documentation into TFIMS in a timely manner. All changes to the application or system must be recorded in TFIMS. DRTBA shall document changes identified during the testing process in the ISCP & DR Testing Checklist artifact or in the ISCP. As these artifacts are created and/or updated, update the Contingency Planning (CP) fields in TFIMS with completion dates.

(2) Documentation for all activities and all actions performed must be completed in a timely manner. The results of each exercise/test must be fully documented using the ISCP & DR Testing Checklist and then uploaded into TFIMS.

Note: Also coordinate with SA staff and/or inventory staff and/or Help Desk to update the asset inventory recordation, which includes the GSS designation and supported applications and environments.

(3) The following TFIMS documentation and TFIMS CP fields are uploaded and updated after exercise/testing is completed:

- Revised Contingency Plan Artifact (ISCP).
- Tested Contingency Plan (Checklist).
- Evidence (year).
- Last CP Test Date (date test/all tests were completed).
- Next CP Test Date (one year from last CP Test Date).

This Page Intentionally Left Blank

Exhibit 10.8.62-1 (09-04-2015)
ISCP & DR Testing Checklist

The ISCP & DR Testing Checklist as an artifact for Treasury FISMA Inventory Management System (TFIMS) to record changes to the content of the ISCP based on information gathered during Test, Training, & Exercise (TT&E) activities documented in Parts A, B, and C of this Checklist, which are provided on the Cybersecurity's Security Risk Management SharePoint at: *https://portal.ds.irsnet.gov/sites/CyberSRM/Public/SitePages/TestingISCP.aspx*. Completion and documentation of these activities also provide evidence that the requirements in the NIST 800-53 family of controls for Contingency Planning Class are met: CP-2 Contingency Plan, CP-3 Contingency Training, and CP-4 Contingency Plan Testing and Exercise. For the latest information, refer to the Security Risk Management's training calendar and information: *https://portal.ds.irsnet.gov/sites/CyberSRM/Public/SitePages/Home.aspx*

Exhibit 10.8.62-2 (09-04-2015)
ISCP Functional Exercise Methodology and Procedures

This ISCP Exercise and Testing job aid has been prepared for use by all Business Operating Divisions (BODs) to inform BOD participants about the activities required to perform ISCP tabletop and functional exercises and DR testing during the current FISMA reporting cycle. For the latest information, refer to *https://portal.ds.irsnet.gov/sites/CyberSRM/Public/SitePages/Forms/AllPages.aspx*

Exhibit 10.8.62-3 (09-04-2015)
BOD ISCP & DR Testing Job Aid

This ISCP Exercise and Testing job aid has been prepared for use by all Business Operating Divisions (BODs) to inform BOD participants about the activities required to perform ISCP tabletop and functional exercises and DR testing during the current FISMA reporting cycle. For the latest information, refer to:
https://portal.ds.irsnet.gov/sites/CyberSRM/Public/SitePages/Forms/AllPages.aspx

Exhibit 10.8.62-4 (09-04-2015)
Glossary and Acronyms

Term	Definition or description
ACIO	Associate Chief Information Officer
After Action Report	A document containing findings and recommendations from an exercise or a test.
AO	Authorizing Official
Alternate Processing Site (APS)	Establishes an alternate processing site including necessary agreements to permit the transfer and resumption of [Bureau-defined information system operations] for essential missions/business functions within [Bureau-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable
BCP	Business Continuity Plan
BOD	Business Operating Division
Critical Business Process (CBP)/Critical Functions	IRS business processes defined by the IRS Business Units that are the most critical to the tax administration mission of the IRS and the Federal Government.
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
Comprehensive Test	A test of all systems and components that support a particular IT plan, such as a contingency plan or computer security incident response plan.
COOP	Continuity of Operations Plan
CP	Contingency Planning
CPO	Certification Program Office
DR	Disaster Recovery
DRTBA	DR Testing and Business Analysis
DRTEE	DR Test, Exercise, and Evaluation; now DRTBA
EA	Enterprise Architecture
ESA	Essential Supporting Activity
ESP	Enterprise Standards Profile
ECC	Enterprise Computing Center
Event	The suite of test or exercise activities.
Exercise	A simulation of an emergency designed to validate the viability of one or more aspects of an IT plan.
FIPS	Federal Information Processing Standard

Exhibit 10.8.62-4 (Cont. 1) (09-04-2015)
Glossary and Acronyms

Term	Definition or description
FISMA	Federal Information Security Management Act
Functional Exercise	A functional exercise is designed to exercise the roles and responsibilities of specific team members, procedures, and assets involved in one or more functional aspects of a plan (e.g., backup procedures, communications, emergency notifications, IS equipment setup).
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IS	Information System
ISCP	Information System Contingency Plan
IT	Information Technology
MITS	Modernization Information Technology Services; changed to IRS IT July 1, 2012.
NIST	National Institute of Standards and Technology
Plan	In the context of this policy, the capitalized term, “Plan”, refers to any of the various IT plans, including Technical Contingency Plan Documents, Continuity of Operations Plans, and any equivalent planning documents.
POA&M	Plan of Actions and Milestones
POC	Point of Contact
PMO	Program Management Office
SA&A	Security Assessment and Authorization
SOP	Standard Operating Procecedure
Scenario	A sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and thus allow demonstration of the exercise objectives.
SP	Special Publication
SRM	Security Risk Management
Tabletop Exercise	A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.

Exhibit 10.8.62-4 (Cont. 2) (09-04-2015)
Glossary and Acronyms

Term	Definition or description
Test	In the context of DR, a test is the method used to evaluate the organization's readiness and ability to recover a system from varying degrees of non-functioning to its original functional state by following authorized ISCP/DR keystroke procedures.
TFIMS	Treasury FISMA Inventory Management System
TSCC	Tool Suite Command Center
TT&E	Test, Training, and Exercise
TT&E Event	An event used to support the maintenance of an IT plan by allowing organizations to identify problems related to an IS plan and implement solutions before an adverse situation occurs.

Exhibit 10.8.62-5 (09-04-2015)
References

- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance*.
- IRM 10.8.2 – *Information Technology (IT) Security, Roles and Responsibilities*.
- IRM 10.8.3 – *Information Technology (IT) Security, Audit Logging Security Standards*.

Treasury

- TD P 85–01, *Treasury Information Technology (IT) Security Program*, March 10, 2008.

National Institute of Standards and Technology (NIST)

- NIST FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*.
- NIST FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*.
- NIST SP 800-34, Rev 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (Errata page - Nov. 11, 2010).
- NIST SP 800-35, *Guide to Information Technology Security Services*, October 2003.
- NIST SP 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, February 2010.
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, May 2010.
- NIST SP 800-53A Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2010.
- NIST SP 800-60 Rev. 1, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes)*, August 2008.
- NIST SP 800-84, *Guide to Test, Training, and Exercise Program for IT Plans and Capabilities*, September 2006.

Department of Homeland Security

- Homeland Security Presidential Directive/HSPD-20, National Continuity Policy, May 2007.
- Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection, December 2003.
- Department of Homeland Security (DHS), National Response Plan, May 2006.

Other

- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002 (FISMA).
- Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources, November 2000.
- Public Law 100-235, Computer Security Act of 1987.