EFFECTIVE DATE

(03-18-2022)

PURPOSE

(1) This transmits revised IRM 10.6.4 Incident Management Program, catalogue number 71634U.

MATERIAL CHANGES

(1) New restrictions for LCRs working in an IMT.

(2) Separation of IT Section Chief from Logistics Team in General Staff of an IMT.

(3) Clarification of duties.

(4) Sections added to conform to Publishing requirements.

(5) Editorial changes for consistency.

EFFECT ON OTHER DOCUMENTS

This updates IRM 10.6.4 *Incident Management Program*, dated March 11, 2020.

AUDIENCE

RM 10.6.4 applies to all organizations and individuals involved in preparing for or implementing any Incident Management program.

Pablo F. Meléndez
Chief, Business Continuity Operations Officer, Deputy Chief of Staff Office C:CoS:DCoS;
Continuity Coordinator

10.6.4
Incident Management Program

Table of Contents

10.6.4.1
(03-18-2022)
Program Scope and Objectives

(1) **Purpose:**

a. This IRM covers policy for the IRS' overall approach to Incident Management and applies to all IRS business units (BUs), all IRS locations, and all types of incidents.
b. This IRM establishes the minimum baseline requirements for the Incident Management Program and the Incident Management Plan in order to: Provide a consistent enterprise approach to incident management; Ensure personnel safety and accountability; Prioritize allocation of resources based on IRS prioritized essential functions; Provide an orderly reconstitution of IRS operations; Monitor and track all incident related activities; and Provide consistent, accurate, and timely information to IRS Senior Executives.
c. Incident Response Contingency Plans (Cybersecurity, Privacy, and Information Systems) are implemented by the BU Program Owner and are outside the scope of this IRM.

(2) **Audience.** These procedures apply to IRS employees who are responsible for developing, implementing, and using the Incident Management Plan including:

- Members of SCR Continuity Operations and Field Operations;
- Members of Headquarters Continuity Operations (COOP) Teams;
- National Continuity Points of Contact (NCPOCs);
- Local Continuity Representatives (LCRs);
- Partner organizations including, but not limited to Facilities Management and Security Services (FMSS), Human Capital Office (HCO), and Information Technology (IT).

(3) **Policy Owner.** The IRS Continuity Coordinator is the Business Continuity Operations Officer of the Deputy Chief of Staff Office of the Commissioner's Complex.

(4) **Program Owner.** The Program Manager of Continuity of Operations of the Senior Commissioner's Representatives within the Deputy Chief of Staff Office.

(5) **Stakeholders.** All audience listed above.

10.6.4.1.1
(03-11-2020)
Background

(1) This IRM lays the foundation to implement and manage the Incident Management Program and Plan within the IRS to ensure an efficient and effective response and recovery following incidents that impact IRS personnel, facilities, and/or business operations.

10.6.4.1.2
(03-11-2020)
Authority

(1) IRM 10.6.1, *Continuity Operations Program, Continuity Planning Requirements*, March 2014, establishes the continuity program and the policy framework for the IRS.

(2) *Presidential Policy Directive 8/PPD-8: National Preparedness*, April 11, 2011.

(3) *Homeland Security Presidential Directive (HSPD) 5 - Management of Domestic Incidents,* December 2003.

(4) *Presidential Policy Directive 40, National Continuity Policy*, July 15, 2016.

(5) *Federal Continuity Directive 1 (FCD-1), Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017.

(6) National Incident Management System (NIMS), October, 2017.

10.6.4.1.3
(03-11-2020)
Responsibilities

(1) The IRS Incident Management Program is owned by SCR Continuity Operations (SCR-CO:CO) and Implemented by SCR Field Operations (SCR-CO:FO) and Campus SCRs as appropriate. See IRM 10.6.4.2 of this IRM for details.

(2) The IRS Incident Management Team (IMT) is cross functional and set up in response to a specific incident. SCR-CO:FO or Campus SCR will activate the IMT. See IRM 10.6.4.3 of this IRM for details.

10.6.4.1.4
(03-11-2020)
Program Reports

(1) There are no periodic reports specifically on the Incident Management Program.

(2) When the Incident Management Plan is implemented and an IMT is activated, reports will be sent to the Senior Executive Team on a frequency determined by the scope of the incident. Usually this is daily, but may be more or less frequent as needed.

(3) The Treasury Operations Center (TOC) will be provided a copy of the Incident Status Report.

(4) All Corrective Actions generated from an Incident are tracked in the SCR-CO:CO Monthly Measures.

10.6.4.1.5
(03-18-2022)
Terms

(1) **Incident** - An occurrence or event, natural or man-made, that requires a response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, civil unrest, wildland and urban fires, floods, hazardous materials, spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, tsunamis, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

(2) **Incident Management** - The broad spectrum of activities and organizations providing effective and efficient operations, coordination, and support applied at all levels of government, utilizing both governmental resources to plan for, respond to, and recover from an incident regardless of cause, size, or complexity.

10.6.4.1.6
(03-11-2020)
Acronyms

(1) CP - Continuity Plan;

(2) EOC - Emergency Operations Center;

(3) IC - Incident Commander;

(4) IMP - Incident Management Plan;

(5) IMT - Incident Management Team;

(6) LCR - Local Continuity Representative;

(7) NCPOC - National Continuity Point of Contact;

(8) OEP - Occupant Emergency Plan;

(9) SCR-CO - Senior Commissioner's Representative-Continuity Operations;

(10) SCR-CO:FO - SCR Field Operations;

(11) SCR-CO:CO - SCR Continuity Operations.

10.6.4.1.7
(03-11-2020)
Related Resources

(1) Incident Management Planning involves coordination with other IRS emergency plans that are referred to as the IRS Business Continuity Suite of Plans. The suite of plans include:

a. Incident Management Plan;
b. Occupant Emergency Plan;
c. Continuity Plan (Headquarters and Business Units);
d. Disaster Recovery/ Information Systems Contingency Plan.

(2) The following IRMs provide the plan requirements:

a. This IRM provides the requirements for the Incident Management Plan;
b. IRM 10.2.9 *Occupant Emergency Planning*, October 5, 2017 provides requirements related to Occupant Emergency Plans;
c. IRM 10.8.60 *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*, September 4, 2015 provides requirements for Information Systems Contingency Plans and Disaster Recovery Plans;
d. IRM 10.6.1 *Continuity Operations Program, Introduction to Continuity Planning*, March 2014 and current update provides requirements for the IRS Continuity Plans.

10.6.4.2
(03-11-2020)
IRS Incident Management Program

(1) The components of the IRS Incident Management Program are:

a. Develop Incident Management Policy and Guidance;
b. Develop and maintain Incident Management Plan;
c. Test and Exercise the Incident Management Plan (see IRM 10.6.3 *Test and Exercise*);
d. Track Corrective Actions and Improvement Plans from the Tests and Exercises (see IRM 10.6.3 *Test and Exercise*);
e. Track Corrective Actions and Improvement Plans resulting from incidents;
f. Coordinate with Treasury Office of Emergency Preparedness;
g. Coordinate with Occupant Emergency and IT Services Continuity Management Programs;
h. Support the IRS Commissioner, Headquarters COOP Teams and Local and/or Area Incident Commanders (ICs) during exercises and actual events.

10.6.4.2.1
(03-11-2020)
Incident Management Plan

(1) The IRS Incident Management Plan (IMP) provides a standardized, yet flexible, framework to managing incidents that impact its personnel, facilities, and/or IRS operations, regardless of incident type, location, and/or severity.

(2) The IMP is implemented by the activation of an IMT, led by an IC, who takes command and control, coordinates and communicates response and recovery activities for all impacted personnel and business units, regardless of to whom they normally report. This includes prioritization and coordination of the resources needed to continue, devolve, and/or reconstitute IRS Mission Essential Functions (MEFs), Essential Support Activities (ESAs), and Critical Business Processes (CBPs).

(3) The IRS Business Unit Continuity Plans (CPs) are implemented and coordinated through the IMP. Each business unit at the impacted site should have a Local Continuity Representative (LCR) who represents their business unit on the IMT's Operations Section.

(4) All IRS locations with assigned personnel are covered by the IRS IMP.

(5) IRS will designate a sufficient number of IMP Owners and Local and/or Area IC(s) to cover all locations with assigned personnel.

(6) The Plan Owner may be responsible for multiple location(s) based on type of office and/or geographical location.

(7) The standardized IMP, as developed by SCR-CO:CO with input from Plan Owners, is required for use to ensure consistency across the enterprise. The Plan incorporates features of the Incident Command System.

(8) The IMP will be reviewed and updated on an annual basis or when critical changes are required due to lessons learned and/or best practices following exercises or real-world incidents.

(9) The IMP will be exercised as required by the IRS Test and Exercise Program requirements.

10.6.4.2.2
(03-11-2020)
Incident Management Plan Components

(1) The Incident Management Plan (IMP) consists of three components:

a. Incident Management Plan;
b. IMT Contact List;
c. Incident Management Plan Toolkit.

10.6.4.2.2.1
(03-11-2020)
Contents of the Incident Management Plan

(1) The IMT must follow the Incident Command System (ICS) organizational structure of an Incident Commander (IC), Command Staff (CS), and General Staff (GS).

(2) The IMP must consist of:

a. Composition of the IMT including roles and responsibilities;
b. Quick Response Checklists (QRC) for each role. The QRC provides an outline of tasks that should be considered;
c. Procedures to cover the incident life cycle (Response, Stabilize, Recover, Restore, Resume, Normalize);
d. Triggers for plan implementation;
e. Notification and Activation Procedures of IMT members;
f. Establishment of an Emergency Operations Center (EOC);
g. Transfer of Command, Escalation of Command, and Associated Briefings;
h. Personnel Accountability Procedures;
i. Development of an Incident Action Plan with common goals and objectives;
j. Internal Contacts;
k. Test and Exercise Requirements;
l. Plan Maintenance;
m. Revision Record.

(3) The Incident Management Plan is to be designated as **Sensitive but Unclassified.**

10.6.4.2.2.2
(03-18-2022)
Contents of the Incident Management Team Contact List

(1) Information required is:

a. The location(s) of team responsibility;
b. The location(s) of the EOC where the team will meet.

Note: These locations may be virtual.

(2) Identification of a primary and two alternates for each of the team roles, at a minimum.

(3) Contacts for personnel assigned to the GS sub-teams may be named but are not mandatory.

(4) The format for maintaining the team contact listing(s) is at the discretion of the plan owner.

10.6.4.2.2.3
(03-11-2020)
Contents of the Incident Management Plan Toolkit

(1) The Toolkit is a collection of forms and procedures that may be needed during an incident based upon past real-world experiences.

(2) The forms and procedures may be used as provided, modified to meet the incident needs, or not used at all.

10.6.4.2.3
(03-18-2022)
Incident Management Plan Owners

(1) IRS has the designated the following as IMP owners:

a. SCR-CO:FO SCRs are responsible for all field posts of duty and the Enterprise Computing Center - Martinsburg;
b. Wage and Investment Campus Directors are responsible for all campus locations and the Tennessee Enterprise Computing Center. Wage and Investment Campus Directors will work with the SCR-CO:FO SCR if the incident is large in scope or covers multiple geographic areas.

(2) Incident Management Plan Owners are responsible for:

a. Maintaining the IMP;
b. Identifying a sufficient number of IMT(s) for their geographical area of responsibility;
c. Identifying a primary and two alternates for key positions on each IMT. Key Positions include the IC, CS (Officers), and GS (Chiefs);
d. Maintaining a list(s) of their IMT members, with current contact information;
e. Coordinating with Continuity Operations to maintain a list(s) of the Operation's Section Local Continuity Representatives (LCRs), as designated by the BUs with current contact information,;
f. Identifying and maintaining a list of primary and alternate EOCs;
g. Ensuring that key positions on the IMT, both primary and alternates, understand their team role and responsibilities;
h. Coordinating and/or conducting, and documenting completion of all required tests and exercises and report status/completion to SCR-CO:CO, as required;
i. Coordinating and/or conducting a hot wash and complete the after-action report/improvement plan following exercises and/or real-world incidents and provide documentation to SCR-CO:CO;
j. Monitoring corrective actions to ensure all are completed and report status/completion to SCR-CO:CO as required;
k. Assist in updating the IMP.

10.6.4.3
(03-11-2020)
Incident Command System

(1) The Incident Command System (ICS) is a standardized, well-proven incident management methodology that establishes a coordinated response, common planning processes, and management of resources. It allows for the integration of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure.

(2) The use of ICS is mandated by the National Incident Management System (NIMS), and is a part of the National Response Framework. The NIMS provides a consistent framework for incident management at all jurisdictional levels regardless of the cause, size, or complexity of the incident. ICS is a key component of the NIMS.

(3) The IRS IMP is based upon features of the ICS.

(4) The IMT will expand or contract based on the size and scope of the incident and as determined by the IC.

10.6.4.3.1
(03-11-2020)
Emergency Operations Center (EOC)

(1) An EOC is the central command and control facility where the IMT meets to manage and/or coordinate response and recovery operations.

(2) The EOC may be a physical fixed location or a virtual location or a combination of both.

(3) At a minimum, IRS must identify a primary and an alternate EOC for the IRS Senior Executive Team / Headquarters Commissioner's Core COOP Team.

10.6.4.3.2
(03-18-2022)
Incident Management Team Members

(1) The lead of the IMT is the IC.

(2) The Command Staff consists of:

a. HCO Representative;
b. Campus Liaison;
c. Information Officer;
d. Liaison Officer;
e. Government Liaison Officer;
f. Safety Officer;
g. Security Officer;
h. Criminal Investigations Special Agent;
i. Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations Special Agent;
j. National Treasury Employees Union (NTEU).

(3) The General Staff consists of:

a. Operation Section Chief, with LCRs reporting to Operations Section Chief;
b. Planning Section Chief;
c. Logistics Section Chief;
d. IT Section Chief;
e. Finance/Administrative Section Chief.

(4) To prevent any potential mishandling or confusion during an emergency, LCR selections should not include individuals who perform other roles within an IMT.

10.6.4.3.3
(03-11-2020)
Roles and Responsibilities of the Team Members

(1) IMT roles and responsibilities are defined in the IMP.

(2) The plan includes a quick response checklist for each role.

10.6.4.3.3.1
(03-18-2022)
Local and Area Incident Commanders

(1) The Associate Director SCR-CO will serve as the Area Incident Commander (AIC) if the incident scope or geographic area warrants it. The Associate Director may delegate this responsibility for specific incidents.

(2) The Field Operations Manager (FOM) for SCR-CO provides guidance and direction to the SCRs as Incident Commanders (IC) during the planning and activating of an EOC and ensures resources are allocated to the ICs.

(3) Local and/or AICs implement the IMP based on the impact to IRS personnel, facilities, and/or impact to IRS operations.

(4) Local Area Commanders handle incidents that impact location(s) within their geographical area of responsibility.

(5) All Local and Area IMT Commanders MUST follow guidelines established in IRM 10.6.1 *Continuity Operations Program, Overview of Continuity Planning* and in this IRM for emergency response procedures, team participants, and required recordation and documentation.

(6) An AIC coordinates incidents having two or more local incident commanders and/or incidents with no Local IC but impacts a large geographical area (such as a hurricane).

10.6.4.3.3.2
(03-18-2022)
Incident Management Team Members

(1) The overall role of the IMT is to provide the command and control infrastructure that is required to manage the logistical, fiscal, planning, operational, safety, and human capital issues related to the incident.

(2) The role, responsibility and Quick Response Checklist (QRC) for each member of the IMT is contained in the IMP.

(3) Team members are to ensure they are familiar with their role and responsibility, maintain current team contact information, and participate in all required training, tests and exercises, and hot washes.

(4) All IMT Members MUST follow guidelines established in IRM 10.6.1 *Continuity Operations Program, Overview of Continuity Planning* and in this IRM for emergency response procedures, team participants, and required recordation and documentation.

(5) Team members are to keep the plan owner apprised of changes to their contact information.

(6) Team members are to inform the plan owner immediately if they are not available for team activation (health, relocation, or retirement).

(7) Each member of any Continuity Team should have sufficient knowledge of personnel and processes to ensure timely completion of responsibilities. Each should also have sufficient authority to be able to represent their BU in all continuity matters.

(8) No IMT member may have a dual role as an LCR.

10.6.4.3.3.3
(03-11-2020)
National Continuity Points of Contact (NCPOCs)

(1) Serves as a member of the Area IMT (Operations Section) and will initiate accountability of personnel during an event which spans multiple SCR areas upon request from an AIC.

(2) Coordinates with the LCRs.

10.6.4.3.3.4
(03-18-2022)
Local Continuity Representatives

(1) Designated by the BU to implement their CP and represent their BU on the IMT under the Operations Section.

(2) Serves as a member of the IMT (Operations Section) with the primary role of conducting employee accountability

(3) Communicates with the NCPOC, their business unit's Senior Leadership and their business unit's managers who have employees who were impacted to provide status updates and convey leadership decisions to and from the IMT.

(4) No LCRs may have any other role in the IMT.

10.6.4.4
(03-18-2022)
Senior Commissioner's Representatives - Continuity Operations (SCR-CO:CO) Responsibilities

(1) SCR-CO:CO is responsible for the IRS IMP and as such, will:

a. Establish and maintain the IRS enterprise-wide incident management policy, standards, templates, and procedures;
b. Oversee plan development, tests and exercises, corrective actions and improvement plan activities;
c. Provide support and guidance to the IMP owners;
d. Maintain a master list of all NCPOCs and LCRs, as designated by their BU and share the appropriate LCRs with the appropriate IMP Owners;
e. Support the Treasury Office of Emergency Preparedness and Treasury Operations Center;
f. Serve as HQ COOP Advance Team (CAT) members and support the IRS Commissioner, HQ COOP Teams, and IRS Local and/or Area ICs during tests, exercises and real-world incidents;
g. Serve as IC Liaison for the HQCOOP Teams;
h. Serve as LCR Liaisons/Coordinators on IMTs;
i. Maintain the Incident Management Toolkit (Forms and Procedures) which must be accessible and available to all IMTs (both field and campus).

(2) Process requests for copies of the IMP. All requests are to be in writing and include sufficient information to determine type of document(s) requested, purpose/need and requestor's information/position.

10.6.4.5
(03-11-2020)
Access to Incident Management Plans

(1) Only employees, or non-IRS individuals, with an authorized need to know shall view or receive documentation relating to the IMP.

10.6.4.6
(03-11-2020)
Conclusion of an Incident

(1) Documentation must be maintained, organized, and available at the conclusion of any incident in which either appropriated funds were used to mitigate the incident or an IMT was formed.

(2) Every participant in the IMT should assume that TIGTA will examine the Service's response after the close of the incident.

10.6.4.6.1
(03-11-2020)
Responsibilities and Procedures for Corrective Actions Generated by Incidents and Events

(1) Because each incident or event differs from all others in scope and impact, both Lessons Learned and Corrective Actions must be scaled appropriately.

(2) IC Responsibilities include, but are not limited to:

a. Identifying weaknesses in preparation, response, and reconstitution;
b. Developing improvement plans to address these weaknesses;
c. Tracking all BU specific resources used.

(3) SCR-CO:CO:

a. General Responsibilities are similar to BU responsibilities but also include all necessary supporting activities such as Procurement, Real Estate, and Physical Security;
b. Specific Responsibilities focus on issues related to program continuity and recovery, especially relating to the Service's Mission Essential Functions (see IRM 10.6.1 *Introduction to Continuity Planning*).

(4) SCR-CO:FO Specific Responsibilities include issues identified as Incident Management (see IRM 1.4.12 *Resource Guide for Managers, Senior Commissioner's Representatives Roles in Management of IRS Field and Headquarters Offices,*), employee accountability, and overall coordination.

(5) Agency Responsibilities:

a. The Service will assume responsibility for issues that will or may become public information, such as integrity of tax information;
b. The Service will provide coordinated response and tracking for all issues and questions raised by the oversight agencies;
c. Until delegated, the Service will be the primary contact for any audits or investigations;
d. SCR-CO:CO will assume responsibility for monitoring status of Corrective Actions resulting from an incident or event, and will provide reports, as appropriate.

10.6.4.6.2
(03-11-2020)
Reporting

(1) The purpose of the reporting is to ensure all critical processes of the Service are able to resume critical operations.

(2) All Corrective Actions must be submitted to Continuity Operations for tracking.

(3) It is the responsibility of each IC to close all Corrective Actions timely.

(4) Based on the Corrective Action Tracking Report, CO will identify any delinquent, incomplete, or unclosed issues and provide to the Continuity Operations Program Manager, SCR-CO:CO, for follow-up with SCR-CO:FO, or the individual BUs as needed.

(5) A summary of Corrective Actions status (not identified by any individual BU) will be included in a quarterly report to the Continuity Operations Program Manager, SCR-CO:CO. This will include type of Corrective Actions, and if appropriate, a listing of incomplete or unclosed recommendations with aging information.