



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.13

JUNE 3, 2024

EFFECTIVE DATE

(06-03-2024)

PURPOSE

- (1) This transmits the new IRM 10.8.13, Information Technology (IT) Security, *Business Impact Analysis (BIA) Security Policy* to provide guidance and establish security requirements necessary to implement and manage Business Impact Analysis within the IRS.

MATERIAL CHANGES

- (1) The Oversight & Strategic Management Security Policy office is introducing new IT Policy for Business Impact Analysis (BIA) Security Policy.
- (2) This IRM is incorporating Interim Guidance Memo IRM 10.8.60 # IT-10-0123-0001, *Business Impact Analysis (BIA) Policy Update*.

EFFECT ON OTHER DOCUMENTS

This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, and IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*. Also, this IRM supplements IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance* and IRM 10.8.62, *Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*. The IRM incorporates IG Memo IT-10-0123-0001, *Business Impact Analysis (BIA) Policy Update*, dated June 1, 2023.

AUDIENCE

IRM 10.8.13 must be distributed to all personnel responsible for ensuring Business Impact Analysis (BIA) policy is exercised. This policy applies to all employees, contractors, and vendors of the IRS.

Rajiv Uppal
Chief Information Officer

10.8.13

Business Impact Analysis (BIA) Security Policy

Table of Contents

10.8.13.1 Program Scope and Objectives

10.8.13.1.1 Background

10.8.13.1.2 Authority

10.8.13.1.3 Roles and Responsibilities

10.8.13.1.4 Program Management and Review

10.8.13.1.5 Program Controls

10.8.13.1.6 Terms and Acronyms

10.8.13.1.7 Related Resources

10.8.13.2 Risk Acceptance and Risk-Based Decisions

10.8.13.3 IT Roles and Responsibilities

10.8.13.3.1 IRS Executive Sponsors, Program Managers, and Technical Leads

#

#

10.8.13.3.4 Information Technology (IT)

10.8.13.3.5 Business Operating Division (BOD) Information System Owners

10.8.13.3.6 BIA Specialist

10.8.13.4 IT Security Controls

10.8.13.4.1 Business Impact Analysis (BIA)

10.8.13.4.1.1 Business Requirements

10.8.13.4.1.2 Conducting the BIA

10.8.13.4.2 Critical Business Processes (CBPs)/Critical Functions

10.8.13.4.3 Access and Requests for BIA Information

10.8.13.4.4 Internal Information Requests

Exhibits

10.8.13-1 Terms and Acronyms

10.8.13-2 Related Resources

10.8.13.1
(06-03-2024)
**Program Scope and
Objectives**

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of Business Impact Analysis (BIA) within the IRS.
 - a. This policy is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* and augments the existing requirements identified within IRM 10.8.1, as they relate to the IRS BIA program, for on-premise systems, including on-premise cloud deployments.
 - b. This policy is subordinate to IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* and augments the existing requirements identified within IRM 10.8.24, as they relate to IRS BIA program for off-premise cloud deployments.
- (2) **Purpose of the Program:** Develop and publish security policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this policy apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors and outsourcing providers, which use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer.
- (5) **Program Owner:** Cybersecurity, Threat Response and Remediation (an organization within Cybersecurity).
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.13.1.1
(06-03-2024)
Background

- (1) This IRM provides policies and guidance to be used by IRS organizations to carry out their respective responsibilities regarding BIA.
 - a. The Associate Chief Information Officer (ACIO), IT Cybersecurity, is responsible for defining relevant policy requirements for the IRS enterprise-wide BIA program and for ensuring business impact analysis is developed, successfully executed, monitored, and managed.
 - b. This IRM defines the overall requirements to ensure compliance with policy and regulations and to ensure the ability to recover the critical business processes (CBPs) of the IRS, through the systems and applications that support them. CBPs are linked to business processes and are also referred to as critical functions.
 - c. The BIA program:
 - i. Links CBPs to business processes which are identified and aligned to applications/systems to support depiction of interdependencies.
 - ii. Manages the alignment of IRS mission essential functions (MEFs) performed by the business operating divisions (BODs) to the applications/systems used to perform the MEFs.
 - iii. Facilitates the priority order for recovering applications/systems for minimizing loss.
 - iv. Prioritizes the identified risks and risk management strategies, considering associated costs and benefits.
 - v. Assesses the potential risks to the organization, by looking at threats,

vulnerabilities, and consequences.

vi. Enables informed, strategic, and recovery investment decisions.

- (2) IRM 10.8.13 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS IT Cybersecurity.

10.8.13.1.2
(06-03-2024)

Authority

- (1) All IRS systems and applications must be compliant with executive orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.

- (2) This BIA policy provides requirements and guidance to ensure that:

- a. All IRS IT systems and applications must have sufficient BIA capability to recover IRS data with system/application functionality (data is available and usable to the customer) according to confirmed pre-defined Recovery Time Objectives (RTOs)/Recovery Point Objectives (RPOs)/Maximum Tolerable Downtime (MTD) documented in the BIA.
- b. The BOD determines the MTD for each non-MEF business process performed by the business, as the MTD for a MEF is federally mandated to be a 12-hour requirement. This determination directly impacts the disaster recovery solution chosen.

- (3) In accordance with federal laws and regulations, the IRS must:

- a. Establish and manage an Information Security Program within all its offices.
- b. Assign security responsibility to appropriate officials.
- c. Ensure continuity of operations for information systems that support the operations and assets of the agency.
- d. Train appropriate personnel in their roles in accordance with the BIA policy.

10.8.13.1.3
(06-03-2024)

Roles and Responsibilities

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

- (2) The supplemental roles and responsibilities specific to the implementation of the IRS BIA Program are located in IRM 10.8.13.3 IT Roles and Responsibilities subsection of this IRM.

10.8.13.1.4
(06-03-2024)

Program Management and Review

- (1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8 series and the development of technology specific security requirements checklists. Stakeholders are notified when revisions to the security policies and security requirements checklists are made.

- (2) It is the policy of the IRS:

- a. To establish and manage an Information Security Program within all its offices. This policy provides uniform policies and guidance to be used by each office.
- b. To protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
- c. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
- d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), OneSDLC, Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.13.1.5
(06-03-2024)
Program Controls

- (1) Each IRM in the 10.8 series is assigned an author who reviews their IRM to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, Defense Information Systems Agency (DISA)) for potential revisions to security policies and security requirements checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security Policy provides a report identifying security policies and security requirements checklists that have recently been revised or are in the process of being revised.
- (3) This IRM applies to all IRS information and systems, which store, process, or transmit IRS information or connect to an IRS network or system. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance for protecting classified information.
- (4) 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 to meet the security requirements of this policy and support the business needs of the organization.
- (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.

10.8.13.1.6
(06-03-2024)
Terms and Acronyms

- (1) Refer to Exhibit 10.8.13-1, Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.8.13.1.7
(06-03-2024)
Related Resources

- (1) Refer to Exhibit 10.8.13-2, Related Resources, for a list of related resources and references.

page 4

10.8 Information Technology (IT) Security

Risk Acceptance and Risk-Based Decisions

- #

#

IT Roles and Responsibilities

IRS Executive Sponsors, Program Managers, and Technical Leads

- #####

##

**Information Technology
(IT)**

(1) IT is responsible for:

- Ensuring NIST SP 800–34 BIA controls are implemented and documented.
- Completing a BIA on all systems and/or applications.
- Partnering with SRM and BODs to coordinate requirements, priorities, recovery times, and support to critical business process procurement activities to enhance BIA capabilities to meet stated business objectives.

	<ul style="list-style-type: none">• Securing concurrence, in writing, from the Director, SRM and business unit (BU) and BIA manager prior to closing all BIA documents related to POA&M and OneSDLC items.	
10.8.13.3.5 (06-03-2024) Business Operating Division (BOD) Information System Owners	<div><div><div>(1) The BOD/information system owner is the agency official responsible for the overall procurement, development, integration, modification, operation and maintenance of the information system. For applications housed on systems owned by or operated by IT, IRS IT will work with BODs to determine appropriate enterprise priorities and identify funding sources for the procurement of equipment. The information system owner is also known as the business and functional unit owner.</div><div>(2) Each BOD that owns or operates IT resources must comply with the IT requirements.</div><div>(3) Each contractor or vendor that owns or operates IT resources on behalf of the IRS must comply with the BIA requirements.</div></div></div>	# # # # # # #
	<div><div><div>(5) In addition to the information system owner/business and functional unit owner responsibilities defined in IRM 10.8.2, business and functional unit owners must:<ul style="list-style-type: none">• Fully describe and document the information system in the BIA.• Clearly define system and application priorities, subsequent needs, and related risk acceptance or avoidance for recovery.• Determine recovery needs and timeframes needed for business restoration through comprehensive BIA evaluations.• Develop BIA requirements during the development phase of all new systems and throughout any production system upgrades.</div></div></div>	
10.8.13.3.6 (06-03-2024) BIA Specialist	<div><div><div>(1) Roles and responsibilities listed below are specific to the implementation of the IRS BIA Program including:<ul style="list-style-type: none">• Perform extensive research and data collection for all IRS applications, on a priority basis, as part of the BIA and MEF determination working with various groups in IT and the BODs.• Prepare documentation and collaborate with BODs/BUs to direct the completion of a business-focused and a system-focused BIA for all applications and systems in the current production environment (CPE).• Prepare documentation and collaborate with BODs/BUs to direct the completion of a business-focused and a system-focused BIA for any new asset going through the OneSDLC process.• Schedule validation meetings to ensure that the BIAs are current, documented for changes, and updated as needed for each asset and business process performed.</div></div></div>	

- Verify that each BOD/BU follows guidelines, most notably the Federal Continuity Directive-2 (FCD-2) requirements.
- Coordinate with Enterprise Operations (EOps) System Administrators (SAs) to manage the BIA-ISCP Testing Analytics (BITA) Tool Windows servers for the BITA Tool database and ensure vulnerabilities are resolved within the required timeframes.

10.8.13.4
(06-03-2024)
IT Security Controls

- (1) The security controls in this IRM supplement the requirements found in IRM 10.8.1.
 - a. Refer to IRM 10.8.1 for security control families and security controls not addressed within this IRM.
- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.
- (3) To configure less restrictive requirements requires a risk-based decision. Refer to the IRM 10.8.13.2 Risk Acceptance and Risk-Based Decisions subsection within this IRM for additional guidance.

10.8.13.4.1
(06-03-2024)
Business Impact Analysis (BIA)

- (1) The BIA is a critical step in IT business continuity and contingency planning and the Information System Contingency Plan (ISCP). The BIA is used to determine business processes and recovery criticality and priorities, identify outage impacts, identify resource requirements, and identify recovery priorities for systems. (NIST 800-34: Section 3.2)
 - a. For additional guidance about ISCPs, refer to IRM 10.8.60, *IT Service Continuity Management (ITSCM) Policy and Guidance* and IRM 10.8.62, *Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*.
 - (2) BIA is a process to identify the essential function relationships, dependencies, time sensitivities, threats, vulnerabilities, consequences, mitigation strategies, identify potential impacts on the performance of essential functions and the consequences of failure to sustain them, and CBPs. (IRS-defined)
- #

#
- (4) The BIA takes into account business needs and requirements, as well as IT. Refer to the IRM 10.8.13.4.1.2 Conducting the BIA subsection in this IRM for more detail. (NIST 800-34: Section 3.2)
 - (5) For a sub-application or component, a separate BIA will be generated, in addition to the host application BIA, if one of the following is true: (IRS-defined)
 - a. The owning organization of the sub-application or component is different from the host application, or

- b. If the sub-application or component also has sub-application(s) and/or component(s).

Note: Umbrella applications designate a program, boundary or grouping. Independent applications, sub-applications and/or components are linked to an umbrella application, which allows the BITA Tool to create a program-level BIA.

- (6) The BIA evaluates the business and system requirements, processes, and interdependencies to determine contingency requirements and priorities. The BIA correlates system components with the critical services system components provided to quantify the consequences to the business of a disruption to the system components or application. (NIST 800-34: Section 3.2)
- (7) The BIA is evaluated and written in relation to an application and/or system. BIAs are considered stand-alone documents for that particular application or system. BIAs are managed at an enterprise level. (NIST 800-34: Section 3.2)
- (8) The site-based BIA serves to: (IRS-defined)
 - Identify the impact that disruptions to computer applications could have on the ability of a particular site, to perform its critical functions.
 - Determine recovery priorities for site-specific applications that support the critical functions, regardless of security categorization.
 - Identify the risks faced by the site. This helps to evaluate or determine the effectiveness of the site's risk mitigation priorities and associated expenditures.
- (9) The business unit BIA serves as a core initiative to: (IRS-defined)
 - Identify the impact that disruptions to a business process would have on the ability of the IRS to perform its critical functions within a given BOD.
 - Determine recovery priorities for all business unit level applications supporting these processes, regardless of location.
 - Identify the risks faced by the business units and measure the appropriateness of its risk mitigation priorities and expenditures.
- (10) The enterprise-wide BIA serves as a core initiative to: (IRS-defined)
 - Identify the impact that disruptions to computer applications would have on the ability of the IRS to perform its critical functions.
 - Determine recovery priorities for all IRS applications supporting these processes, regardless of location.
 - Identify the risks faced by the enterprise and measure the appropriateness of its risk mitigation priorities and expenditures.
- (11) Continuity of Operations Plan (COOP) functions are subject to a process-focused BIA. Federal information systems are subject to a system-focused BIA. (NIST 800-34: Section 3.2)
 - a. Information systems that support COOP functions will be identified in the process-based BIA.
- (12) FCD-2 contains a Form 2: Business Process Analysis Data Sheet Template and NIST 800-34 provides a template for a system-based BIA, which were both used as guides to create the current BIA Template. Annex D: Business Impact Analysis: A formal review, update, and validation of the organization's

essential functions through a BIA must be conducted at least every two years. As part of biennial continuity assessments conducted by Federal Emergency Management Agency (FEMA), each Department and Agency (D/A) must affirm that risks to the performance of its MEFs and Primary Mission Essential Functions (PMEFs) have been evaluated and documented as part of its BIA. As stated previously, the BIA is conducted annually for the MEF hosted applications/systems. (FCD-2)

- (13) Results from the BIA must be appropriately incorporated into the analysis and strategy development efforts for the IRS' COOP, BCPs, and Disaster Recovery Plan (DRP). (NIST 800-34: Section 3.2)
- (14) Important Terms: (NIST 800-34: Section 3.2)
 - a. **Business Impact Analysis (BIA)** - A structured process to identify the critical functions that are supported by the documented IT resource. The BIA Program incorporates two separate BIA types, the Process-based and the System-based BIA, to support the large volume of data generated for the Enterprise. Both types assist with developing strategies for minimizing risk for the critical work at the IRS. (IRS-defined)
 - The Process-based BIA looks at the processes needed to ensure that the Enterprise maintains a level of service during an incident. Process-based BIA data is collected in the Business Impact Analysis (BIA) Template Form, which incorporates both CPE and newly developed applications (OneSDLC).
 - The System-based BIA is 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.
 - b. **Critical Business Processes (CBP)** - The CBPs were established and categorized based on their relative priority to the execution and support of the overall mission of the IRS. (IRS-defined)
 - c. **Maximum Tolerable Downtime (MTD)** - The maximum amount of time a business process can be disrupted before there is an unacceptable impact on other business processes and/or the mission of the organization. MTD is sometimes referred to as Maximum Tolerable Outage (MTO).
 - d. **Recovery Point Objective (RPO)** - The point in time, prior to a disruption or system outage (e.g., end of previous day's processing) to which data can be recovered (given the most recent backup copy of the data) after an outage. RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that might need to be recreated after the systems or functions have been recovered. RPO factors how much data will be lost based on the date and time of the last backup.
 - e. **Recovery Time Objective (RTO)** - The length of time an information system component can be in the recovery phase before negatively impacting the organization's mission or mission/business functions. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.
 - f. **Service Continuity (SC)** - Supports business continuity management by reducing the risk from events to an acceptable level and planning for the recovery of IT services. SC summarizes information about measures that

serve the purpose of disaster preparation. SC planning addresses business IT risks, processes, data, services, and components.

- g. **Service Levels (SLs)** - The details of IT Service usage: volume, capacity, resource, performance, availability windows, etc.
- h. **Service Level Requirements (SLRs)** - Business requirements supporting service continuity for an IT service. The SLRs belong to the AO who owns the service. The SLR information needs to contain both comprehensible and comprehensive details. The SLRs provide a basis for negotiations linked to the formulation of service level objectives (SLOs) or service level agreements (SLAs).

#

10.8.13.4.1.1
(06-03-2024)

Business Requirements

- (1) All systems and applications listed as assets in the FISMA Master Inventory Spreadsheet (i.e., all Tiers and Cloud Tabs and all titled FISMA System/App & Subsystem(s) in column B) on the Cybersecurity SRM EFC SharePoint site must have an initial BIA conducted as part of the Security Assessment & Authorization (SA&A) process. (IRS-defined)

#

- b. Refer to the Information System Contingency Planning Process subsection within IRM 10.8.60 for additional guidance.

- (2) Conducting and funding of BIA activities must be the responsibility of the business owner. (IRS-defined)
- (3) The BIA is an ongoing, living document that must be evaluated every year for MEF hosting systems or applications, at least every two years for non-MEF hosting systems or applications, or whenever there is a change to business requirements, systems, or applications. (IRS-defined)
- (4) Each system must have a timeframe defined for the MTD for the resumption of objectives from an unscheduled interruption. (IRS-defined)
- (5) All systems must have BIA documentation of potential risks specific to the BOD/BU workflow or the supporting applications/systems. (IRS-defined)
- (6) The owner of the IT assets (applications, sub-applications/components and/or systems) must be responsible for the BIA documentation. Documentation must be maintained/updated by the owner and IT operations responsible for the business impact of the system referenced by the document. (IRS-defined)
- (7) All IT assets, including those that are and are not listed on the FISMA Master Inventory, must have BIA documentation. (IRS-defined)

Note: All new applications and systems must have an initial System-based BIA conducted as part of the OneSDLC process. Refer to IRM 2.16.1, *Enterprise Life Cycle (ELC)*, *ELC Guidance*, for additional guidance on Enterprise Life Cycle (ELC).

10.8.13.4.1.2
(06-03-2024)
Conducting the BIA

(1) Data collection requirements are accomplished through individual/group interviews, workshops, emails, questionnaires, or any combination of these. These four primary steps must be completed as part of an BIA. (IRS-defined)

- a. Identify the business requirements and purpose of the application undergoing the BIA.
- b. Identify outage tolerances:

- | |
|---|
| • Disruption impacts to specific business functions |
| • Maximum Tolerable Downtime (MTD) times |
| • Recovery Time Objectives (RTO) |
| • Recovery Point Objective (RPO) |
| • Interdependencies supporting other IT resources (e.g., systems, internal/external applications) |

- c. Identify outage impacts. Items to consider:

- | |
|---------------------------------|
| • Loss of data/data loss impact |
| • Operational impact |
| • Customer service impact |
| • Damage to reputation |

- d. Identify recovery priorities. Such as:

- | |
|--------------------------------------|
| • Mission Essential Functions (MEFs) |
| • Business Process MTDs |
| • System and Application RTOs |
| • Outage impact (see above) |

10.8.13.4.2
(06-03-2024)
Critical Business Processes (CBPs)/Critical Functions

(1) Critical business processes and functions have been defined by the IRS Senior Executive team and business representatives as those most critical to the tax administration mission of the IRS supporting the overall continuity of the federal government. (IRS-defined)

#

[illegible]

#

- (5) The RTO must ensure that the MTD is not exceeded. The RTO must be shorter than, or at a minimum, equal to the MTD. (NIST 800-34: Section 3.2.1)

Note: For example, a system outage may prevent a particular process from being completed, and because it takes time to reprocess the data, that additional processing time must be added to the RTO to stay within the time limit established by the MTD.

10.8.13.4.3
(06-03-2024)
**Access and Requests
for BIA Information**

- (1) BIA documents contain potentially sensitive operational and personnel information. Its distribution must be marked accordingly and controlled. (NIST 800-34: Section 3.6)

10.8.13.4.4
(06-03-2024)
**Internal Information
Requests**

- (1) Only system administrators, managers, or other individuals with responsibility for BIA may have access to copies of applicable BIA documents. (IRS-defined)
- (2) Requests for copies of or access to system and application BIA documents must be made through the employee’s manager to the system and/or application owner. (IRS-defined)
- (3) All other requests for copies of or access to BIA documents must be requested from the system or application owner. The request must specify what is being requested, purpose, contact person, and where the copy is to be sent. (IRS-defined)

Exhibit 10.8.13-1 (06-03-2024)

Terms and Acronyms

Terms	Definition or Description
ACIO	Associate Chief Information Officer
AO	Authorizing Official
Application	A standalone or host software, such as batch, extract, sub-routines (functions), command codes, and/or reporting jobs.
Backup	The process of duplicating and storing the files and programs of an IT system on another medium or device to facilitate complete restoration of the system and its data following a disruption.
BC	Business Continuity
BIA	Business Impact Analysis
BITA	BIA & ISCP Testing Analytics Tool
BOD	Business Operating Division
BU	Business Unit
Business Continuity	Business Continuity is a collection of strategies and specialized plans that ensures a local IRS site can continue to manage efficiently and operate optimally in response to an impending/actual incident without significant impact to overall IRS client services.
Business Continuity Plan (BCP)	The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption. NIST 800-34, <i>Contingency Planning Guide for Federal Information Systems</i> , Rev 1, Errata Nov 1, 2010. In addition, per IRM 10.6.1, <i>Continuity Operations Program, Overview of Continuity Planning</i> , states the BCP is an ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity operations through personnel training, plan testing, and maintenance.
Business Impact Analysis (BIA)	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.
CBP	Critical Business Process

Exhibit 10.8.13-1 (Cont. 1) (06-03-2024)
Terms and Acronyms

CMMI	Capability Maturity Model Integration
CNSI	Classified National Security Information
Components	Information System components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middle-ware, and applications. Information system components are either purchased commercially off-the-shelf or are custom-developed.
Contingency Planning	The process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively impacts the organization.
Continuity of Operations Plan (COOP)	The COOP focuses on restoring an organization's (usually a headquarter's element) essential functions at an alternate site and performing those functions for up to 30 calendar days before returning to normal operations. Because a COOP addresses headquarter's-level issues, it is developed and executed independently from the business continuity plan. Standard elements of a COOP include Delegation of Authority statements, Orders of Succession, and Essential Records and Databases. Minor disruptions that do not require relocation to an alternate site are typically not addressed. However, the COOP may include the business continuity plan, business resumption plan, and disaster recovery plan as appendices.
Continuity Plan	Refer to Business Continuity Plan.
COOP	Continuity of Operations Plan
CP	Contingency Planning
CPE	Current Production Environment
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.
D/A	Department and Agency
DISA	Defense Information Systems Agency
Disaster Recovery	The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

Exhibit 10.8.13-1 (Cont. 2) (06-03-2024)

Terms and Acronyms

Disaster Recovery Plan (DRP)	A plan created and maintained by IT or any information technology service provider that defines the resources, roles, responsibilities, actions, tasks, and the steps required, down to a key step level, to restore an IT system to its full operational status at the current or alternate facility after a disruption. The DRP can be a part of the ISCP, a standalone document, or separate disaster recovery keystroke procedures.
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).
DRP	Disaster Recovery Plan
ELC	Enterprise Life Cycle
EOps	Enterprise Operations
EOs	Executive Orders
ESA	Essential Supporting Activity
Essential Records	Records an agency needs to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). (NARA: 36 CFR 1223)
FCD	Federal Continuity Directive
Federal Information Security Modernization Act of 2014 (FISMA)	FISMA, among other things, amends Chapter 35 of title 44, United States Code, adding a new sub chapter: "SUBCHAPTER III — INFORMATION SECURITY" which provides additional security requirements on federal agencies.
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FSIS	Filing Season Integration Services
Host Application	An application that has one or more sub-applications or components that run under the application.

Exhibit 10.8.13-1 (Cont. 3) (06-03-2024)
Terms and Acronyms

Impact	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Impact Level	High, Moderate, or Low security categories of an information system established in FIPS 199 which classify the intensity of a potential impact that may occur if the information system is jeopardized.
Incident Management Plan	The Incident Management Plan is a site's specific plan that focuses on the command and control, coordination activities, and management of a disruption at any IRS site.
Information System	A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Contingency Plan (ISCP)	Documents created and maintained by IT, Cybersecurity, and system owners that provide procedures and capabilities for recovering an information system and define the resources, roles, responsibilities, and procedures for recovering a single information system after a disruption.
ISCP	Information System Contingency Plan
IT	Information Technology
ITIL	Information Technology Infrastructure Library
Keystroke Recovery (KR)	Detailed step-by-step instructions, including keystroke-by-keystroke details, to restore an IT system to its full operational status following a disruption.
LSS	Lean Six Sigma
Maximum Tolerable Downtime (MTD)	The maximum amount of time a business can tolerate the outage of a critical business function. MTD is sometimes referred to as Maximum Tolerable Outage (MTO).
MEF	Mission Essential Functions
MTD	Maximum Tolerable Downtime
NARA	National Archives and Records Administration
NCS	National Communications System
NEF	National Essential Functions
NIST	National Institute of Standards and Technology

Exhibit 10.8.13-1 (Cont. 4) (06-03-2024)

Terms and Acronyms

OMB	Office of Management and Budget
OneSDLC	One Solution Delivery Lifecycle
PMEF	Primary Mission Essential Function
POA&M	Plan of Action & Milestones
POC	Point of Contact
PPD	Presidential Policy Directive
RBD	Risk-Based Decision
Recovery Point Objective (RPO)	The point in time, prior to a disruption or system outage (e.g., end of previous day's processing) to which data can be recovered (given the most recent backup copy of the data) after an outage. RPOs are often used as the basis for the development of backup strategies, and as a determinant of the amount of data that might need to be recreated after the systems or functions have been recovered. RPO factors how much data will be lost based on the date of the last backup.
Recovery Time Objective (RTO)	The length of time an information system component can be in the recovery phase before negatively impacting the organization's mission or mission/business functions. RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.
Risk-Based Decision	A decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessments, and processes. The type of information considered when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information considered are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive).
SA	System Administrator
SA&A	Security Assessment & Authorization
SC	Service Continuity
SCTE	Security Controls Testing & Evaluation
SDLC	System Development Life Cycle

Exhibit 10.8.13-1 (Cont. 5) (06-03-2024)
Terms and Acronyms

SECURE	Stakeholder Enterprise Cybersecurity Unified Risk Evaluation
Security Controls	The management, operational, and technical controls (e.g., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
SL	Service Level
SLA	Service Level Agreement
SLO	Service Level Objective
SLR	Service Level Requirement
SOP	Standard Operating Procedure
SRM	Security Risk Management
SRMA	Security Risk Management and Analysis
Sub-Application	An application that is dependent on a host application for processing.
System Development Life Cycle (SDLC)	The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.
TD	Treasury Directive
Test	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. For additional information about testing, refer to IRM 10.8.62.
Toolkit Suite with Command Centre (TSCC)	IRS enterprise-level repository and incident management decision support tool and plan repository for BIA documents.
TSCC	Toolkit Suite with Command Centre
TT&E	Test, Training, and Exercise
Umbrella Application	An application name that designates a program, boundary or grouping.

Exhibit 10.8.13-2 (06-03-2024)**Related Resources****IRS Publications**

- IRM 2.16.1, *Enterprise Life Cycle (ELC), ELC Guidance*
- IRM 10.6.1, *Continuity Operations Program, Overview of Continuity Planning*
- IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*
- IRM 10.9.1, *National Security Information, Classified National Security Information (CNSI)*

#**Department of the Treasury**

- TD P 85–01, Version 3.1.3, *Department of the Treasury Information Technology (IT) Security Program*, February 28, 2022

National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
- NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (Errata page - November 11, 2010)
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 20, 2018
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 20, 2020 (Updated 12/10/2020)
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, January 2022
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, October 2020 (Updated 12/10/2020)
- NIST SP 800-60, Volume 2 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 1, 2008

Other Publications

- *E-Government Act of 2002* (Public Law 107-347), Title III, Federal Information Security Management Act of 2002 (FISMA)
- Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directive 1 (FCD-1), *Federal Executive Branch National Continuity Program and Requirements*, January 17, 2017
- Department of Homeland Security, Federal Emergency Management Agency, Federal Continuity Directive 2 (FCD-2), *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*, dated June 13, 2017
- Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, July 15, 2016

