|  |
| --- |
| **Business Impact Analysis**  **for**    **{System Name}**  **{IC}**    Security Categorization: {High, Moderate, Low}        **Version {Revision}**      **March 15, 2017**          **Prepared by**  Click or tap here to enter text.  **FOR OFFICIAL USE ONLY** |

**Document Revision History**

This {System Name} Business Impact Assessment (BIA) is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to this document are recorded in the version history matrix below.

At a minimum, this document will be reviewed and assessed annually. Reviews made as part of the assessment process shall also be recorded below.

This document history shall be maintained throughout the life of the document and the associated system.

| **Date** | **Description** | **Version** | **Author** |
| --- | --- | --- | --- |
| mm/dd/yyyy | Document Publication | 1.0 | Program Office |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Business Impact Assessment Approval Signatures**

I have reviewed the {System Name} Business Impact Assessment and accept the analysis and findings within.

|  |  |
| --- | --- |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| {System Owner Full Name} | Date |
| System Owner |  |
|  |  |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_ |
| {Information System Security Officer Full Name} | Date |
| Information System Security Officer |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Table of Contents**

[1 Overview 5](#_Toc531509728)

[1.1 Purpose 5](#_Toc531509729)

[1.2 NIH Mission and Goals 5](#_Toc531509730)

[1.3 BIA Steps 6](#_Toc531509731)

[2 System Identification 7](#_Toc531509732)

[2.1 System Name/Title 7](#_Toc531509733)

[2.2 System Type and Purpose 7](#_Toc531509734)

[2.3 System Operational Status 7](#_Toc531509735)

[2.4 Security Categorization 7](#_Toc531509736)

[2.5 System Owner 7](#_Toc531509737)

[2.6 Information System Security Office (ISSO) 8](#_Toc531509738)

[2.7 IC Chief Information Officer 8](#_Toc531509739)

[3 BIA Data Collection 9](#_Toc531509740)

[3.1 Step 1: Determine {System Name} Components and Recovery Criticality 9](#_Toc531509741)

[3.2 Step 2: Identify Resource Requirements 12](#_Toc531509742)

[3.3 Step 3: Identify Recovery Priorities for System Resources 13](#_Toc531509743)

# 1 Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for {System Name}.

## 1.1 Purpose

The purpose of this BIA is to identify and prioritize {System Name} components as each relates to NIH’s missions and goals. Using this information, the BIA categorizes and shows the overall business impact to NIH when components or the entire {System Name} is lost due to outage or a major contingency event.

## 1.2 NIH Mission and Goals[[1]](#footnote-1)

NIH’s mission is to seek fundamental knowledge about the nature and behavior of living systems and the application of that knowledge to enhance health, lengthen life, and reduce illness and disability.

The goals of the agency are:

* to foster fundamental creative discoveries, innovative research strategies, and their applications as a basis for ultimately protecting and improving health;
* to develop, maintain, and renew scientific human and physical resources that will ensure the Nation's capability to prevent disease;
* to expand the knowledge base in medical and associated sciences in order to enhance the Nation's economic well-being and ensure a continued high return on the public investment in research; and
* to exemplify and promote the highest level of scientific integrity, public accountability, and social responsibility in the conduct of science.

In realizing these goals, the NIH provides leadership and direction to programs designed to improve the health of the Nation by conducting and supporting research:

* in the causes, diagnosis, prevention, and cure of human diseases;
* in the processes of human growth and development;
* in the biological effects of environmental contaminants;
* in the understanding of mental, addictive and physical disorders; and
* in directing programs for the collection, dissemination, and exchange of information in medicine and health, including the development and support of medical libraries and the training of medical librarians and other health information specialists.

## 1.3 BIA Steps

The three steps used to conduct this BIA are as follows:

* Determine {System Name} component and recovery criticality:
  + Determine the {System Name} functions supported by the system
  + Identify outage impacts & estimate the maximum downtime NIH can tolerate and still maintain its mission and goals
* Identify resource requirements
  + Identify and evaluate resources required (facilities, personnel, equipment, software, data files, and system components) to resume {System Name} operations as quickly as possible
* Identify recovery priorities for system resources
  + Based upon the results from the previous activities, identify the system resources that are linked to critical NIH missions and goals
  + Establish priority levels for sequencing recovery activities and resources

# 2 System Identification

## 2.1 System Name/Title

| **Unique Identifier (UUID)** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| {UUID} | {System Name} | {System Abbreviation} |

**2.1.1 Responsible NIH Organization**

| **IC Name** | **Shared Accountability Partner(s)** |
| --- | --- |
| {IC Name} | {IC Name} |

## 2.2 System Type and Purpose

{System Name} is a {Entity Type}. {System Description}

## 2.3 System Operational Status

The system is currently in the {SDLC Phase} phase of the system development life cycle.

## 2.4 Security Categorization

{System Name} was evaluated against FIPS 199 and NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*.  The following FIPS 199 security impact ratings are outlined in the *{System Name} Security Categorization* (see Appendix C).

| **Security Objective** | **Low, Moderate or High** |
| --- | --- |
| Confidentiality | {High, Moderate, Low} |
| Integrity | {High, Moderate, Low} |
| Availability | {High, Moderate, Low} |
| **Overall** | **{High, Moderate, Low}** |

## 2.5 System Owner

|  |  |
| --- | --- |
| **Name** |  |
| **Title** |  |
| **IC Name** |  |
| **Address** |  |
| **Telephone** |  |
| **Email** |  |
| **Responsibility** |  |

## 2.6 Information System Security Office (ISSO)

|  |  |
| --- | --- |
| **Name** |  |
| **Title** |  |
| **IC Name** |  |
| **Address** |  |
| **Telephone** |  |
| **Email** |  |
| **Responsibility** |  |

## 2.7 IC Chief Information Officer

|  |  |
| --- | --- |
| **Name** |  |
| **Title** |  |
| **IC Name** |  |
| **Address** |  |
| **Telephone** |  |
| **Email** |  |
| **Responsibility** |  |

# 3 BIA Data Collection

## 3.1 Step 1: Determine {System Name} Components and Recovery Criticality

**3.1.1 {System Name} Components and Descriptions**

| **Component** | **Description** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**3.1.2 Outage Impacts and Estimated Downtime**

**Outage Impacts**

The following impact categories represent important areas for consideration in the event of an outage:

| **Impact Category** | **Impact Values** | | |
| --- | --- | --- | --- |
| **Severe**  *(Systems in this category should consider fault-tolerant architecture and design)* | **Moderate**  *(Systems in this category should consider alternate site processing options, or have tested rapid recovery processes)* | **Minimal**  *(Systems in this category can tolerate prolonged disruptions, and do not require fault-tolerant or rapid recovery solutions)* |
| **Cost** | $1M+ | $250K-$1M | <$250K |
| **Service Delivery** | Disruption has a severe to catastrophic negative effect on the ability for NCI to perform its mission. | Disruption has a limited to severe negative effect on the ability for NCI to perform its mission. | Disruption has no, or only limited impact on NCI’s ability to perform its mission. |
| **Image/Credibility** | Disruption has a severe to catastrophic negative effect on NCI’s reputation or credibility. | Disruption has a noticeable to severe negative effect on NCI’s reputation or credibility. | Disruption has no negative impact NCI’s reputation or credibility. |
| **Health & Safety** | Disruption has a severe to catastrophic (unacceptable) negative effect on the health and safety of patients, staff, animals, or other NCI stakeholders. | Disruption has minimal to severe negative effect on the health and safety of patients, staff, animals, or other NCI stakeholders. | Disruption has no health or safety impacts. |
| **Regulatory** | Disruption has an unacceptable negative effect on NCI’s regulatory mission. | Disruption has a limited negative effect on NCI’s regulatory mission. | Disruption has no negative impact on NCI’s regulatory mission. |

The table below summarizes the impact for each {System Name} component on NIH’s missions and goals if the component were unavailable:

| **Component**  **[Components are listed in table 3.1.1]** | **Impact Category** |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Cost** | **Service Delivery** | **Image/**  **Credibility** | **Health & Safety** | **Regulatory** | **Overall Impact** |
| <Insert Component> | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
| <Insert Component> | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
|  | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
|  | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
|  | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
|  | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
|  | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. | Choose an item. |

**Estimated Downtime**

The estimated downtime factors are as follows:

* **Maximum Tolerable Downtime (MTD):** The MTD represents the total amount of time leaders/managers are willing to accept for a {System Name} component outage or disruption and includes all impact considerations.
* **Recovery Time Objective (RTO):** RTO defines the maximum amount of time that a {System Name} component can remain unavailable before there is an unacceptable impact on other NIH resources and the MTD.[[2]](#footnote-2)
* **Recovery Point Objective (RPO):** The RPO represents the point in time, prior to a disruption or system outage, to which {System Name} component data must be recovered (given the most recent backup copy of the data) after an outage.

The drivers for the MTD, RTO, and RPOs are as follows:

* <Insert Drivers>

The table below identifies the MTD, RTO, and RPO (as applicable) for the {System Name} components:

| **Component** | **MTD** | **RTO** | **RPO** |
| --- | --- | --- | --- |
| Insert Component and MTD/RTO/RPO | (Example: 1 Week) | (Example: 1 Week) | (Example: 24 hours (last backup) |
| Insert Component and MTD/RTO/RPO | [Duration] | [Duration] | [Duration] |
| Insert Component and MTD/RTO/RPO | [Duration] | [Duration] | [Duration] |

**Alternative Means of Recovering {System Name} Operations**

[Describe current or planned alternative processing or continuity solutions for the system].

## 3.2 Step 2: Identify Resource Requirements

**3.2.1 Physical/Host Locations**

| **Common Name/Reference** | **Physical Address** |
| --- | --- |
|  |  |
|  |  |
|  |  |

**3.2.2 Physical Resources**

| **TYPE** | **NAME** | **DNS NAME** | **IP ADDRESS** | **GUEST OS** | **{System Name} COMPONENT** | **ASSET TAG** | **LOCATION**  **(Common Name)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Physical |  |  | 128.xxx.xxx | (Example: Ubuntu 12.04.4 LTS) |  |  |  |
| Physical |  |  | 192.xxx.xxx |  |  |  |  |

**3.2.3 Virtual Resources**

| **TYPE** | **NAME** | **DNS NAME** | **IP ADDRESS** | **GUEST OS** | **{System Name} COMPONENT** | **LOCATION**  **(Common Name)** |
| --- | --- | --- | --- | --- | --- | --- |
| Virtual |  |  |  | (Example: Microsoft Windows Server 2008 R2 (64-bit)) |  |  |
| Virtual |  |  |  |  |  |  |

## 3.3 Step 3: Identify Recovery Priorities for System Resources

The table below lists the order of recovery for the {System Name} resources. The table also identifies the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption.

| **Priority** | **{System Name} Component** | **Worst Case Recovery** |
| --- | --- | --- |
| 1 |  | (Example: 4 weeks to rebuild or replace) |
| 2 |  |  |
| 3 |  |  |

<Insert any details to support above Priorities>

**END OF DOCUMENT**

1. National Institutes of Health. (2015, April 9). About NIH. Retrieved from What We Do: Mission and Goals: https://www.nih.gov/about-nih/what-we-do/mission-goals. [↑](#footnote-ref-1)
2. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD. [↑](#footnote-ref-2)