The NCI Central Institutional Review Board (CIRB)

NCI CIRB Manager Information System
FIPS 199 Security Categorization
Annual Report

Version 5.0
September 01, 2018

Prepared for:
The National Cancer Institute
Clinical Trials Operations & Informatics Branch
Co-Contracting Officer Representative CIRB

Contracting Number: HHSN261201400023C

SENSITIVE

Record of Changes/Version History

Version Number	Date of Change	Summary of Changes	Sections Changed	Person Entering Change
1.0	09/30/2014	Initial submission	New Submission	Jennifer Dugan / Brian Campbell
2.0	09/01/2015	Annual review	No changes	Jennifer Dugan / Brian Campbell
3.0	09/01/2016	Annual review	Section 1	Jennifer Dugan / Brian Campbell
4.0	09/01/2017	Annual review	Throughout	Jennifer Dugan/ Brian Campbell
5.0	09/01/2018	Annual review	Throughout	Brian Campbell

Table of Contents

1. INTRODUCTION

The Federal Information Processing Standard 199 (FIPS-199) Categorization (Security Categorization) report is a key document including the determination of the security impact level for the CIRB Web System. The ultimate goal of the security categorization is to be able to select and implement security controls applicable to its environment.

1.1. Purpose

The purpose of the FIPS-199 Categorization assessment is to determine categorization of environment, to provide the categorization to the NCI in helping them make a determination of the CSP's ability to host systems at that level. The completed security categorization assessment will aid the NCI in selection and implementation of security controls at the determined categorization level.

1.2. Scope

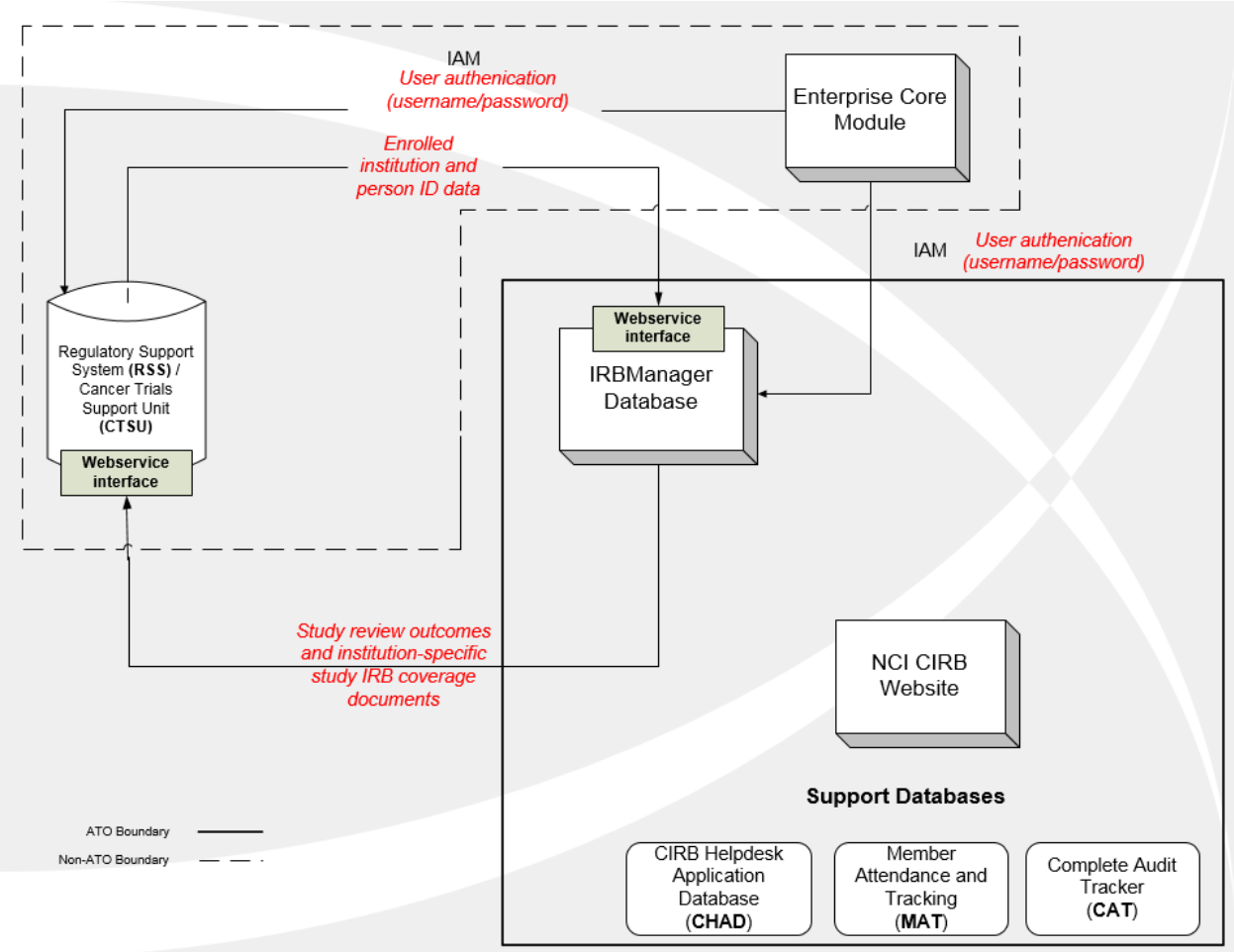
The scope of the FIPS-199 Categorization includes assessment of the information type categories as defined in the NIST Special Publication 800-60 Volume 2 Revision 1 document.

1.3. System Description

The NCI CIRB Manager system has been determined to have a security categorization of **Low**.

The Central Institutional Review Board (CIRB) provides a central resource for expediting Institutional Review Board (IRB) activities for National Cancer Institute (NCI) Network Group clinical trials. For informatics systems to support all CIRB Operations, EMMES provides a suite of informatics systems for comprehensive data collection, data management and information dissemination. These systems support CIRB study tracking and CIRB Operations support for the CIRBs; enrollment and management of Signatory Institutions and associated institution and person records; and the NCI CIRB website. The systems are fully interoperable on both the Test and Production instances, and are configured to support industry-standard best practices for Software Development Life Cycle (SDLC).

The systems and their interoperability are outlined in the figure below:



2. METHODOLOGY

Impact levels are determined for each information type based on the security objectives (confidentiality, integrity, availability). The confidentiality, integrity, and availability impact levels define the security sensitivity category of each information type. The FIPS-199 Categorization is the high watermark for the impact level of all the applicable information types.

The FIPS 199 analysis represents the information type and sensitivity levels CIRB data system offering. The analysis must be added as an appendix to the SSP and drive the results for the Categorization section.

The NCICIRB Manager system categorization is expected to resolve: Low.

Table 1, summarizes the potential impact definitions for each security objective—confidentiality, integrity, and availability.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

3. Applicable Information Types with Security Impact Levels

Table 2, provide a summary of information types based on NIST SP 800-60 Version 2, Revision 1, and FIPS 199 assessment.

Information Type	NIST SP 800-60 V2 R1 Recommended Confidentiality Impact Level	NIST SP 800-60 V2 R1 Recommended Integrity Impact Level	NIST SP 800-60 V2 R1 Recommended Availability Impact Level	CSP Selected Confidentiality Impact Level	CSP Selected Integrity Impact Level	CSP Selected Availability Impact Level	Statement for Impact Adjustment Justification
Regulatory Development - Guidance Development Information	Low	Low	Low	Low	Low	Low	Low
Public Relations - Customer Service Information	Low	Low	Low	Low	Low	Low	Low
Public Relations - Official Information Dissemination Information	Low	Low	Low	Low	Low	Low	Low
Public Relations - Outreach Information	Low	Low	Low	Low	Low	Low	Low
Public Relations Information	Low	Low	Low	Low	Low	Low	Low

4. System Security Categorization Approval

Table provides a summary of the information types that apply based on the selections identified in the FIPS 199 assessment.

Table 3: FIPS 199 Security Categorization Summary

Information Type Name	Security Objective			Rationale for Selecting or Adjusting Security Categorization Levels
	Confidentiality	Integrity	Availability	
Regulatory Development	Low	Low	Low	Due to the change in user authentication protocol and the transition of the responsibilities from the CIRB website to the CTSU website
Public Affairs	Low	Low	Low	All information provided is on the public website

Provide the overall impact rating (i.e., the high water mark) for each security objective:

Confidentially = **Low**

Integrity = **Low**

Availability = **Low**

Based on the above information, the System Impact Level for the CIRB Web System is: **Low**.

I, Mike Montello, approve the System Impact Level selected for the CIRB Web System. Changes to the data processed, stored and transmitted by the information system will require a review and update to the Security Categorization.

Mike Montello
NCI CIRB

Date

System Owner for the CIRB Web System