|  |
| --- |
|  Cover Page NIH logo     **System Assessment Report** **for****[System Name] ([System Acronym])**Security Categorization: [High, Moderate, or Low]**[IC Name] ([IC Acronym])** **Version [Revision X.X]**  **[MM/DD/YYYY]**   **Prepared by**Click or tap here to enter text.**FOR OFFICIAL USE ONLY** |

**Document Revision History**

This [System Name] System Assessment Report (SAR) 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 |
| 08/06/2018 | Fix typographical errors | 1.1 | ISAO-A&A |
| 10/25/18  | Fixed typographical and grammatical errors in sections 1.3, 1.4, 2.1, 2.2, 2.3, 3.0, 3.2 & 4.0  | 1.2 | NIH Information Security Program |
| 04/01/2020  | Removed Privacy Coordinator’s Signature | 1.3 | NCI EST |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |
|   |   |   |   |

 **Security Assessment Report Approval Signatures**

I have reviewed the [System Name] Security Assessment Report and accept the analysis and findings within.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Security Control Assessor Full Name]

Security Control Assessor

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[System Owner Full Name]

System Owner

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[Information System Security Officer Full Name]

Information System Security Officer

**Table of Contents**

[1. Overview 6](#_Toc528930724)

[1.1 Applicable Laws and Regulations 6](#_Toc528930725)

[1.2 Applicable Standards and Guidance 7](#_Toc528930726)

[1.3 Purpose 8](#_Toc528930727)

[1.4 Scope 8](#_Toc528930728)

[2 System Overview 10](#_Toc528930729)

[2.1 System Name 10](#_Toc528930730)

[2.2 General System Description and Purpose 10](#_Toc528930731)

[2.3 Security Categorization 10](#_Toc528930732)

[3 Assessment Methodology 11](#_Toc528930733)

[3.1 Perform Tests 11](#_Toc528930734)

[3.2 Identification of Vulnerabilities 12](#_Toc528930735)

[3.3 Consideration of Threats 12](#_Toc528930736)

[3.4 Perform Risk Analysis 15](#_Toc528930737)

[3.5 Document Results 16](#_Toc528930738)

[4 Security Assessment Results 17](#_Toc528930739)

[5 Non-Conforming Controls 19](#_Toc528930740)

[6 Authorization Recommendation 20](#_Toc528930741)

**List of Tables**

[Table 1‑1 Physical Location 9](#_Toc533764609)

[Table 2‑1 System Identifiers 10](#_Toc533764610)

[Table 2‑2 Security Categorization 10](#_Toc533764611)

[Table 3‑1 Threat Categories and Origination 12](#_Toc533764612)

[Table 3‑2 Potential Threats 14](#_Toc533764613)

[Table 3‑3 Likelihood Definitions 15](#_Toc533764614)

[Table 3‑4 Impact Definitions 15](#_Toc533764615)

[Table 3‑5 Risk Exposure Ratings 15](#_Toc533764616)

[Table 1‑1 Security Assessment Results 18](#_Toc533764617)

# Overview

This document represents the *Security Assessment Report (SAR)* for [System Name] as required by NIH for security authorization. This SAR contains the results of the comprehensive security test and evaluation of [System Name]. This assessment report, and the results documented herein, supports program goals, efforts, and activities necessary to achieve compliance with organizational security requirements. The SAR describes the risks associated with the vulnerabilities identified during [System Name]’s security assessment and also serves as the risk summary report as referenced in *NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems*.

All assessment results have been analyzed to provide both the information system owner, IC ISSO, and the authorizing officials, with an assessment of the security controls as described in the [System Name] System Security Plan.

Title III, Section 3544, of the E-Government Act of 2002, dated December 17, 2002, requires agencies to conduct periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. Appendix III of Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, requires federal agencies to:

* *Review the security controls in each system when significant modifications are made to the system, but at least every three years.§3(a)(3)*
* *Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information. §8(a)(1)(g); §8(a)(9)(a)*
* *Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time. §8(b)(3)(b)(iv)*
* *Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.§(3)(b)(4)*

## Applicable Laws and Regulations

The following laws and regulations are applicable to NIH:

* Computer Fraud and Abuse Act (P.L. 99-474, 18 USC 1030), October 1986
* Federal Information Security Modernization Act (FISMA) (P.L. 113-283, 44 USC 35), December 2014
* Privacy Act of 1974 as amended (P.L. 93-579, 5 USC 552a), December 1974
* Freedom of Information Act as Amended (15 CFR § 270.350), January 2018
* Records Management by Federal Agencies (44 USC 31), January 2012
* Office of Management and Budget (OMB) Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act, January 2017
* Office of Management and Budget (OMB) Circular A-123, Management’s Responsibility for Enterprise Risk Management and Internal Control, July 2016
* Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, July 2016
* Office of Management and Budget (OMB) M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, December 2000
* Office of Management and Budget (OMB) M-04-04, E-Authentication Guidance, December 2003
* Office of Management and Budget (OMB) M-05-24, Implementation of HSPD-12 - Policy for a Common Identification Standard for Federal Employees and Contractors, May 2005
* Office of Management and Budget (OMB) M-06-16, Protection of Sensitive Agency Information, June 2006
* Office of Management and Budget (OMB) M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 2017
* Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection, December 2003
* Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 2005

## Applicable Standards, Guidance, and Policy

The following standards. Guidance, and policy are applicable to the organization:

* Health and Human Services (HHS) Information Systems Security and Privacy Policy (IS2P), July 2014
* National Institutes of Health (NIH) Information Security Policy Handbook 4.0, May 2018
* National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, December 2002
* National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
* National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
* National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 201-2, Personal Identity Verification (PIV) of Federal Employees and Contractors, September 2013
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Rev 1 Guide for Developing Security Plans for Federal Information Systems, February 2006
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Rev 1 Guide for Conducting Risk Assessments, September 2012
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 Rev 1 Contingency Planning Guide for Federal Information Systems, November 2010
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev 1 Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 2014
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47 Security Guide for Interconnecting Information Technology Systems, September 2002
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A Rev 4 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, December 2014
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4 Security and Privacy Controls for Federal Information Systems and Organizations, January 2015
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-59 Guideline for Identifying an Information System as a National Security System, August 2003
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 1 Rev 1 Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 2 Rev 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices, August 2008
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev 2 Computer Security Incident Handling Guide, August 2012
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-64 Rev 2 Security Considerations in the System Development Life Cycle, October 2008
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-115 Technical Guide to Information Security Testing and Assessment, September 2008
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-128 Guide for Security-Focused Configuration Management of Information Systems, August 2011
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011
* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 The NIST Definition of Cloud Computing, September 2011

## Purpose

The purpose of the Security Assessment Report is to provide the system owner, ISSO, and security authorization officials with a summary of the risks associated with the vulnerabilities identified during the security assessment for [System Name]. A security assessment has been performed on [System Name] to evaluate the system’s implementation of, and compliance with, the organization's baseline security controls. The details of the implementation of security controls are described in the System Security Plan, and required by HHS to meet *Federal Information Security Management Act (FISMA)* compliance mandates.

The organization requires information systems to use internal and third party assessment organizations to perform independent security assessment testing and documentation of the SAR. Security testing for [System Name] was performed by [fullname] in accordance with the [System Name] Security Assessment Plan.

## Scope

This SAR applies to [System Name] which has a unique identifier, name, and acronym, noted in Section 2.1.

Documentation used by the assessor to perform the assessment of [System Name] includes the following:

* [System Name] FIPS199 Categorization
* [System Name] E-Authentication
* [System Name] System Security Plan
* [System Name] Contingency Plan and Test Results
* [System Name] Business Impact Analysis
* [System Name] Configuration Management Plan
* [System Name] Incident Response Plan and Test Results
* [System Name] Privacy Threshold Analysis/Privacy Impact Assessment
* [System Name] Security Assessment Plan

[System Name] is physically located at the facilities and location noted below.

Table 1‑1 Physical Location

| **Site Name** | **Address** |
| --- | --- |
|  |  |

# System Overview

## System Name

Table 2‑1 System Identifiers

| **Unique Identifier (SBID or UUID)** | **Information System Name** | **Information System Abbreviation** |
| --- | --- | --- |
| [SBID or UUID] |  [System Name] |  [System Acronym] |

## General System Description and Purpose

|  |
| --- |
| Instruction: This should be a copy of the SSP System Description.Please delete these instructions before finalizing this document. |

[System Name] is a [System Type]. [System Description and Purpose]

##  Security Categorization

The [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 Appendix C (*Security Categorization*) of the *[System Name]* System Security Plan (SSP).

Table 2‑2 Security Categorization

| **Security Objective** | **Low, Moderate or High** |
| --- | --- |
| Confidentiality | [Rating] |
| Integrity | [Rating] |
| Availability | [Rating] |
| **Overall** | **[Rating]** |

# Assessment Methodology

The security assessment use as logical and prescriptive process for determining risk exposure for the purpose of facilitating decisions as is aligned with the Risk Management Framework (RMF) described in NIST 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The RMF describes six steps that apply to the system development life-cycle and assessing security controls constitutes Step 4 as illustrated in Figure 3-1.



Figure 3-1: Risk Management Framework

This methodology used to conduct the security assessment for [System Name] system is summarized in the following steps:

1. Perform tests from the Security Assessment Plan workbook and record the results
2. Identify vulnerabilities on the platform
3. Identify threats and determine which threats are associated with the cited vulnerabilities
4. Analyze risks based on vulnerabilities and associated threats
5. Recommend corrective actions
6. Document the results

## Perform Tests

Security tests were performed on the [System Name]and tests were concluded on [date]. The Security Assessment Plan (SAP) separately documents the schedule of testing. The results of the tests are recorded in the Security Test Procedures workbooks which are attached in the appendices. The findings of the security tests serve as inputs to this Security Assessment Report.

## Identification of Vulnerabilities

Vulnerabilities have been identified for the [System Name] through security control testing. The results of the security control testing are recorded in Security Test procedures workbooks and in NSAT (NIH Security Authorization Tool).

Vulnerability is an inherent weakness in an information system that can be exploited by a threat or threat agent, resulting in an undesirable impact in the protection of the confidentiality, integrity, or availability of the system (application and associated data).  A vulnerability may be due to a design flaw or error in configuration which makes your network, or a host on your network, susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in multiple areas of your system or facilities, such as in your firewalls, application servers, Web servers, operating systems or fire suppression systems.

Whether or not a vulnerability has the potential to be exploited by a threat depends on a number of variables including (but not limited to):

* The strength of the security controls in place
* The ease at which a human actor could purposefully launch an attack
* The probability of an environmental event or disruption in a given local area

An environmental disruption is usually unique to a geographic location. Depending on the level of the risk exposure, the successful exploitation of a vulnerability can vary from disclosure of information about the host to a complete compromise of the host. Risk exposure to organizational operations can affect the business mission, functions, or the organizational reputation.

The vulnerabilities that were identified through security control testing (including penetration testing) for the [System Name] are identified in Table 4.1: Security Assessment Results.

## Consideration of Threats

A threat is an adversarial force or phenomenon that could impact the availability, integrity, or confidentiality of an information system and its networks including the facility that houses the hardware and software. A threat agent is an element that provides the delivery mechanism for a threat. An entity that initiates the launch of a threat agent is referred to as a threat actor.

A threat actor might purposefully launch a threat agent (e.g. a terrorist igniting a bomb). However, a threat actor could be a trusted employee that acts as an agent by making an unintentional human error (e.g. a trusted staff clicks on a phishing email that downloads malware). Threat agents may also be environmental in nature with no purposeful intent (e.g. a hurricane). Threat agents working alone, or in concert, exploit vulnerabilities to create incidents. NIH categorizes threats using a threat origination taxonomy of P, U, or E type threats as described in Table 3-1.

Table 3‑1 Threat Categories and Origination

| **Threat Origination Category** | **Origination Identifier** |
| --- | --- |
| Threats launched purposefully | P |
| Threats created by unintentional human or machine errors  | U |
| Threats caused by environmental agents or disruptions | E |

Purposeful threats are launched by threat actors for a variety of reasons and the reasons may never be fully known. Threat actors could be motivated by curiosity, monetary gain, political gain, social activism, revenge or many other driving forces. It is possible that some threats could have more than one threat origination category.

Some threat types are more likely to occur than others. NIH takes threat types into consideration to help determine the likelihood that a vulnerability could be exploited. The threat table shown in Table 3-2 is designed to offer typical threats to information systems and these threats have been considered for [System Name].

Table 3‑2 Potential Threats

| **Threat Name** | **Origination Identifier** | **Description** | **Typical Impact to Data or System** | **Impact Level** | **Likelihood** | **Risk** |
| --- | --- | --- | --- | --- | --- | --- |
| **Confidentiality** | **Integrity** | **Availability** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

## Perform Risk Analysis

The goal of determining risk exposure is to facilitate decision making on how to respond to real and perceived risks. The outcome of performing a risk analysis, yields risk exposure metrics that can be used to make risk-based decisions.

The NIH risk analysis process is based on qualitative risk analysis. In qualitative risk analysis the impact of exploiting a threat is measured in relative terms. When a system is easy to exploit, it has a High likelihood that a threat could exploit the vulnerability. Likelihood definitions for the exploitation of vulnerabilities are found in Table 3-3.

Table 3‑3 Likelihood Definitions

| **Likelihood** | **Description** |
| --- | --- |
| Low | There is little to no chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| Moderate | There is a moderate chance that a threat could exploit a vulnerability and cause loss to the system or its data. |
| High | There is a high chance that a threat could exploit a vulnerability and cause loss to the system or its data. |

Impact refers to the magnitude of potential harm that could be caused to the system (or its data) by successful exploitation. Definitions for the impact resulting from the exploitation of a vulnerability are described in Table 3-4. Since exploitation has not yet occurred, these values are perceived values. If the exploitation of a vulnerability can cause significant loss to a system (or its data) then the impact of the exploit is considered to be High.

Table 3‑4 Impact Definitions

| **Impact** | **Description** |
| --- | --- |
| Low | If vulnerabilities are exploited by threats, little to no loss to the system, networks, or data would occur. |
| Moderate | If vulnerabilities are exploited by threats, moderate loss to the system, networks, and data would occur. |
| High | If vulnerabilities are exploited by threats, significant loss to the system, networks, and data would occur. |

The combination of High likelihood and High impact creates the highest risk exposure. The risk exposure matrix shown in Table 3-5 presents the same likelihood and impact severity ratings as those found in *NIST SP 800-30 Risk Management Guide for Information Technology Systems.*

Table 3‑5 Risk Exposure Ratings

| **Likelihood** | **Impact** |
| --- | --- |
| **Low** | **Moderate** | **High** |
| High | Low | Moderate | High |
| Moderate | Low | Moderate | Moderate |
| Low | Low | Low | Low |

## Document Results

Documenting the results of security testing creates a record of the security posture for the system at a given moment in time. The record can be reviewed for risk-based decision making and to create plans of action to mitigate risks.

The Federal Information Security Management Act (FISMA) requires that a Plan of Action and Milestones (POA&M) be developed and utilized as the primary mechanism for tracking all system security weaknesses and issues. Security Control Assessors will leverage the SAR to create a Plan of Action and Milestones (POA&M) for [System Name]. The POA&M is a mitigation plan designed to address specific residual security weaknesses and includes information on costing, resources, and target dates.

# Security Assessment Results

This section describes all security weaknesses found during testing. The following elements for each security weakness are reported:

* Finding Number
* Status
* Source
* Finding Description
* Business Impact Statement
* Recommended Corrective Action
* Link to Control(s)/Test Case(s)
* Likelihood
* Impact
* Risk Level

The reader of the SAR should anticipate that the security weakness elements are described as indicated below.

* **Finding Number:** The unique application-generated security finding number.
* **Status:** The computed lifecycle status associated with the finding.  If the finding is linked to a weakness for remediation management, the finding status is computed based on the completed status of the weakness.  Finding status described below:
	+ **Unlinked** - The finding is not linked to a weakness.
	+ **Active** - The finding has been linked to a weakness that has an open status.
	+ **Completed** - The finding has been linked to a weakness where remediation has been completed successfully (i.e. the weakness is in completed status).
	+ **Rejected** - The finding has been rejected either as a false positive or risk accepted (i.e. risk-based decision).  No remediation is required for the security finding.
* **Source:**The finding type such as vulnerability assessment, security audit, etc., and the failed security control in which the finding was created.
* **Finding Description:** This is the description of the finding as defined from the vulnerability assessment, security audit report, or from the results of an internal security review.
* **Business Impact Statement:** Impact of the finding to the organization if exploited.
* **Recommended Corrective Action:** The recommended control(s) needed to remediate the finding.
* **Link to Control(s)/Test Case(s):** The control and/or test case associated with the finding.
* **Likelihood:** The likelihood that the finding will be exploited (High, Moderate, or Low).
* **Impact:**The impact to the organization if the finding is exploited (High, Moderate, or Low).
* **Risk Level:** The computed risk level associated with the finding based on the selected likelihood and impact.  Please refer to Table 3-5 Risk Exposure Ratings for details.

Table 1‑1 Security Assessment Results

| **ID** | **Weaknesses** | **Remediation Actions** | **POC** | **Scheduled Completion Date** | **Status** | **Risk Level** |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Non-Conforming Controls

In certain instances, the [System Name] system may not have the technical capability to implement a security control or the system owner may have made a decision not to implement a control based on the cost or feasibility of implementing the control relative to the risk exposure. The status of such controls is designated "Not Implemented" or "Partially Implemented" or "Alternative Implementation" in the System Security Plan. A summary of theses controls are listed in Table 5-1 along with a justification statement that offers an explanation for the non-conformance with NIH requirements. Control categories are designated as either Management, Technical, or Operational as defined in NIST SP 800-53, Revision 4.

Table 5-1. Non-Conforming Controls

| **Control ID** | **Control Category** | **Description** | **Justification Statement** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|   |   |   |   |
|   |   |   |   |

# Authorization Recommendation

The assessment indicates that the identified risks are deemed either a) to be acceptable, b) higher than desired, or c) to be unacceptable. The authorizing official should consider the risks presented herein in determining the authorization decision.