

****

Office of Information Technology

Division of Information Security & Privacy Management

Centers for Medicare & Medicaid Services

**Security Assessment Report**

**Template**

Version 2.0

January 9, 2019

## Table of Contents

[Table of Contents ii](#_Toc10020855)

[List of Tables ii](#_Toc10020856)

[List of Figures ii](#_Toc10020857)

[1. Executive Summary 3](#_Toc10020858)

[2. Background 3](#_Toc10020859)

[3. Assessment Scope 3](#_Toc10020860)

[4. Summary of Findings 3](#_Toc10020861)

[5. Summary of Recommendations 4](#_Toc10020862)

[2. Introduction 4](#_Toc10020863)

[1. Assessment Methodology 4](#_Toc10020864)

[2. Detailed Findings 5](#_Toc10020865)

[3. Methodology for the Security Control Assessment 5](#_Toc10020866)

[4. Methodology for Security Test Reporting 5](#_Toc10020867)

[3.1 Business Risks 7](#_Toc10020868)

[3.1.1 Moderate 8](#_Toc10020869)

[Assessed-2017-SCA-IA-2-12 8](#_Toc10020870)

[4. Documentation Lists 10](#_Toc10020871)

## List of Tables

[Table 1. Risk Level Definitions 5](#_Toc10020872)

[Table 2. Ease-of-Fix Definitions 6](#_Toc10020873)

[Table 3. Estimated Work Effort Definitions 7](#_Toc10020874)

[Table 4. CFACTS System Names 7](#_Toc10020875)

[Table 5. Documentation Requested 10](#_Toc10020876)

## List of Figures

[Figure 1. Reported Findings by Risk Level 3](#_Toc10020949)

[Figure 2. Open Findings by Risk Level 4](#_Toc10020950)

## Executive Summary

## Background

## Assessment Scope

## Summary of Findings

Of the findings discovered during our assessment, 0 were considered High risks, 2 Moderate risks, 0 Low, and 0 Informational risks. The risks found during the assessment are broken down as shown on the graph in Figure 2.



Figure 1. Reported Findings by Risk Level

Two (2) Moderate risk findings remain open. The risks found during the assessment are categorized as shown on the graph in Figure 3.



Figure 2. Open Findings by Risk Level

## Summary of Recommendations

# Introduction

## Assessment Methodology

The purpose of this assessment was to do the following:

* Ensure that the system was in compliance with the CMS Information Security (IS) Acceptable Risk Safeguards (ARS), including the CMS Minimum Security Requirements (CMSR), Version 2.0, [[1]](#footnote-2) HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications, CMS Policy for Information Security Program (PISP),[[2]](#footnote-3) and CMS Business Partners Systems Security Manual Version 11.0 (BPSSM)[[3]](#footnote-4).
* Determine if the application was securely maintained.

## Detailed Findings

Section 3 provides a descriptive analysis of the vulnerabilities identified through the SCA process. Each vulnerability is thoroughly explained, specific risks to the continued operations of CMS information systems are identified, and the impact of each risk is analyzed as a business case. The Business Risks also contain suggested corrective actions for closing or reducing the impact of each vulnerability.

Preceding the detailed Business Risks, the methodologies for performing the SCA and reporting test results are presented. These sections explain the SCA process, and describe how the Business Risk Level, Ease-of-Fix, and Estimated Work Effort metrics have been assessed.

## Methodology for the Security Control Assessment

**3.1.2 Tests and Analyses**

**3.1.3 Tools**

## Methodology for Security Test Reporting

The format and content of this report has been developed in accordance with the CMS Chapter 4 Security Assessment and Authorization Risk Management Handbook. The CMS Reporting Standard requires that a Risk Level assessment value be assigned to each Business Risk, in order to provide a guideline by which to understand the procedural or technical significance of each finding. Further, an Ease-of-Fix and Estimated Work Effort value must be assigned to each Business Risk, to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close, or reduce the impact of each vulnerability.

**3.1.1 Risk Level Assessment**

Each Business Risk has been assigned a Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in Table 1 apply to risk level assessment values.

Table 1. Risk Level Definitions

| Rating | Definition of Risk Rating |
| --- | --- |
| High Risk | Exploitation of the technical or procedural vulnerability will cause substantial harm to CMS business processes. Significant political, financial and legal damage is likely to result |
| Moderate Risk | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity and/or availability of the system, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment to CMS |
| Low Risk | Exploitation of the technical or procedural vulnerability will cause minimal impact to CMS operations. The confidentiality, integrity and availability of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment |
| Informational | An “Informational” finding, is a risk that has been identified during this assessment which is reassigned to another Major Application (MA) or General Support System (GSS). The finding must already exist and be open for the reassigned MA or GSS. The informational finding will be noted in a separate section in the final SCA report, but will not be the responsibility of the assessed application to create a Corrective Action Plan, as it is reassigned to the MA or GSS |
| Observations | An observation may arise as a result of a number of situations:A security policy or document may be changing and serves to inform the system owner. This gives ample time to prepare for and make appropriate changes;A security policy or document has changed, and CMS has granted a grace period for completion. The observation provides a mechanism to the Business Owner/ISSO that the item requires attention before the end of that grace period;A possible finding that the Security Assessment Contractor may have observed and cannot verify by testing as part of the existing tasking; orIssues related to industry “best practices” and that are not identified in the CMS Acceptable Risk Safeguards (ARS) or other guidelines referenced by the ARS. These items are considered “Opportunities for Improvement” (OFI) |

**3.1.2 Ease-of-Fix Assessment**

Each Business Risk has been assigned an Ease-of-Fix value of Easy, Moderately Difficult, Very Difficult, or No Known Fix. The Ease-of-Fix value is an assessment of how difficult, or easy, it will be to complete reasonable and appropriate corrective actions required to close or reduce the impact of the vulnerability. The definitions in Table 2 apply to the Ease-of-Fix values.

Table 2. Ease-of-Fix Definitions

| Rating | Definition of Risk Rating |
| --- | --- |
| Easy | The corrective action(s) can be completed quickly with minimal resources, and without causing disruption to the system or data |
| Moderately Difficult | Remediation efforts will likely cause a noticeable service disruption* A vendor patch or major configuration change may be required to close the vulnerability
* An upgrade to a different version of the software may be required to address the impact severity
* The system may require a reconfiguration to mitigate the threat exposure
* Corrective action may require construction or significant alterations to the manner in which business is undertaken
 |
| Very Difficult | The high risk of substantial service disruption makes it impractical to complete the corrective action for mission critical systems without careful scheduling* An obscure, hard-to-find vendor patch may be required to close the vulnerability
* Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity
* Corrective action requires major construction or redesign of an entire business process
 |
| No Known Fix | No known solution to the problem currently exists. The Risk may require the Business Owner to:* Discontinue use of the software or protocol
* Isolate the information system within the enterprise, thereby eliminating reliance on the system

In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going business functions, no less than quarterly monitoring shall be conducted by the Business Owner, and reviewed by CMS IS Management, to validate that security incidents have not occurred |

**3.1.3 Estimated Work Effort Assessment**

Each Business Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial, or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. The definitions in Table 3 apply to the Estimated Work Effort values.

Table 3. Estimated Work Effort Definitions

| Rating | Definition of Estimated Work Effort Rating |
| --- | --- |
| Minimal | A limited investment of time (i.e., roughly three days or less) is required of a single individual to complete the corrective action(s) |
| Moderate | A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions |
| Substantial | A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture, and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units |
| Unknown | The time necessary to reduce or eliminate the vulnerability is currently unknown |

**3.1.4 CMS FISMA Controls Tracking System Names**

To ensure that the final security controls/findings worksheet can be properly loaded into the CMS FISMA Controls Tracking System (CFACTS), the following system name has been used to populate the System Name field in the Final Management Worksheet, delivered as an attachment to this report.

Table 4. CFACTS System Names

| CFACTS System Names |
| --- |
|  |

###  Business Risks

Business Risks within this section are technical or procedural in nature, and may result directly in unauthorized access.

The Business Risks are ordered first by Risk Level (from High Risk to Low Risk) and then by Estimated Work Effort (from Substantial to Minimal). This format will help CMS identify critical risks that must be immediately addressed with little time and effort. Each discussion section identifies the servers, and whether the production or test environment is impacted by the vulnerability. CMS should initially focus on addressing critical risks that impact the production environment.

|  |  |
| --- | --- |
| Moderate | Assessed-2017-SCA-IA-2-12 |
|  |
| **Applicable Standards:** |
| **NIST Security Control Families:** | Identification and Authentication |
| **Reference:** | IA-2(12) |
| **Risk Level: (Risk Level is High, Moderate, or Low)** |
| Moderate |
| **Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)** |
| Very Difficult |
| **Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)** |
| Substantial |
| **Description:** |
| Assessed.... |
| ***Finding*** |
| Assessed ..... |
| Impacted systems include Assessed ...... |
| ***Failed Test Description*** |
| CMS Information Security ARS Appendix B-CMSR Moderate Impact Level Data requires the information system accepts and electronically verifies Personal Identity Verification (PIV) credentials. |
| ***Actual Test Results*** |
| Assessed...... |
| **Recommended Corrective Action(s):** |
| .................. |
| **Status:** |
| Identified (Date) |

|  |
| --- |
| **Applicable Standards:** |
| **NIST Security Control Families:** | Identification and Authentication |
| **Reference:** | IA-8 |
| **Risk Level: (Risk Level is High, Moderate, or Low)** |
| Moderate |
| **Ease-of-Fix: (Ease-of-Fix is Easy, Moderately Difficult, Very Difficult, or No Known Fix)** |
| Moderately Difficult |
| **Estimated Work Effort: (Estimated Work Effort is Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)** |
| Moderate |
| **Description:** |
| Assessed... |
| ***Finding*** |
| Assessed ..... |
| Impacted systems include Assessed.... |
| ***Failed Test Description*** |
| CMS Information Security ARS Appendix B-CMSR Moderate Impact Level Data requires the information system uniquely identifies and authenticates non-organizational users. |
| ***Actual Test Results*** |
| Assessed ..... |
| **Recommended Corrective Action(s):** |
| ...... |
| **Status:** |
| Identified (Date) |

# Documentation Lists

The following table lists documentation that the Assessor requested prior to the onsite visit, as well as documentation provided to the Assessor during, and after, the visit. The tables include the document element number, document title or information requested, and comments. Comments may include the name of the individual, organization, or agency that sent or delivered the documents, and the date the Assessor received the documents.

Table 5. Documentation Requested

See Attached

1. http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ARS.pdf (July 31, 2012). [↑](#footnote-ref-2)
2. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/PISP.pdf (August 31, 2010). [↑](#footnote-ref-3)
3. http://www.cms.gov/manuals/downloads/117\_systems\_security.pdf (September 30, 2011). [↑](#footnote-ref-4)