**National Aeronautics & Space Administration**

**Headquarters**

**SECURITY REVIEW REPORT**

**Migrate CMTS to HQ VM cluster**

Service Request #2015-0002618

Issue Date: 2015-06-10

Effective Date: 2015-06-10

Verify that this is the correct version before use.

Revision 1.0

***WARNING:*** *This document is SENSITIVE BUT UNCLASSIFIED (SBU). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with NASA policy relating to SBU information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized NASA official.*



National Aeronautics and

Space Administration

NASA Headquarters

*Washington, DC*

# Table of Contents

Table of Contents 2

Revision History 3

Introduction 3

Methodology 3

Scope 3

Application Profile 4

Risk Management 5

Risks: 6

Recommendation 6

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Rev. Number** | **Date** | **Originator/Phone** | **Description** |
| 1.0 | 2015-06-10 | Karim Said / 202 358 0985 | Initial Version |

# Introduction

This report presents the results of an Information Technology (IT) Security Review undertaken by the HITSS IT Security team for SR 2015-002618. This review addresses the impact this project may have on the confidentiality, integrity, and availability of the NASA HQ organizational operations, assets, and individuals. Additionally, it will identify vulnerabilities present in the system/application, the threats against the system/application, and the impact of those risks.

# Methodology

HITSS Security, in collaboration with the HITSS Application Development team, reviewed and tested the proposed release of the CMTS application within the NASA HQ VM Cluster environment.

# Scope

The scope of the risk assessment is limited to the risks identified in the CMTS application. The risk assessment will evaluate the existing and potential risks to the system, its supporting IT infrastructure, operational environment, as well as the customer or users.

# Application Profile

CMTS is a web application used to manage career progress information for NASA employees.

The scope of this SR is to migrate the application from WESTPrime into the HQ VM cluster. Code changes in this release are due to minor differences in the configuration of web servers and their connection to Launchpad (i.e., some static paths in the code had to be updated).

**Section 4: Application/Interface Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Application Information** | | | |
| **24 Application Name:** | Career Management Tracking System (CMTS) | | |
| **25 Application Owner:** | De Andrea Peters | | |
| **26 Application URL:** | https://cmts.hq.nasa.gov | | |
| **27 SEF Application URL:** | https://cmts.stage.hq.nasa.gov | | |
| **28 Ports/Protocols:** | TCP 443 / SSL | | |
| **29 Programming Language:** | Cold Fusion 10, JavaScript, SQL | | |
| **30 COTS/GOTS Software:** | ColdFusion 10, Oracle 11g | | |
| **31 Data Description:** | The **CMTS** stores career tracking data. | | |
| **32 Server Architecture:** | Application server is running under Redhat 6.5 and has ODBC connection with Oracle server. | | |
| **33 Application Dependency:** | Application requires the use of the Access Launchpad and the Headquarters Transition System (HQTS). | | |
| **Logical Controls** | | | |
| **34 Auditing:** | User access, data manipulation | | |
| **35 Audit Log Location(s):** | Audit log information is stored in the Oracle database | | |
| **36 Authentication Type:** | Access Launchpad authentication | | |
| **37 Access Controls:** | Restricted under NASA Firewall for NASA users only | | |
| **38 Session Timeout:** | 30 minutes | | |
| **38 Parameter Validation:** | Yes | | |
| **39 Database/Query Input Validation:** | Yes | | |
| **40 URL/Form Input Validation:** | Yes | | |
| **41 Error Handling:** | Custom error page is used | | |
| **42 Encryption Types:** | SSL for all URL access | | |
| **43 Physical Controls:** | The server is host inside firewalls and we have implemented ACLs on the server to restrict access to NASA Agency IP addresses only; application is also protected by Access Launchpad. | | |
| **44 Network:** | HQ Intranet/ cmts.hq.nasa.gov/ rivers.hq.nasa.gov | | |
| **45 Warning Banner:** | NASA standardized warning banner on Launchpad’s Login page as well as inside CMTS’s Home page. | | |
| **46 App Administrators:** | NASA HQ Server Administrators (UNIX team) | | |
| **47 App Account Type(s):** | This is a permission based application | | |
| **48 Permission Type(s):** | This is a role based application | | |
| **49 Design Documentation:** | Yes | | |
| **50 Application Password Policy (Access Launchpad)** | | | |
| **a Length:** | N/A | **e Complexity:** | N/A |
| **b History:** | N/A | **f Nontrivial:** | N/A |
| **c Age:** | N/A | **g Password Recovery:** | N/A |
| **d Encrypted:** | N/A | **h Lockout:** | N/A |
| **50 Local Access Restrictions:** | Local access to TCP 443 on CMTS.hq.nasa.gov is unrestricted | | |
| **51 Remote Access Restrictions:** | Remote access to TCP 443 on CMTS.hq.nasa.gov is restricted by the NASA HQ Perimeter firewall | | |

# Risk Management

|  |  |
| --- | --- |
| **Risk Management Information (Completed by HITSS IT Security)** | |
| **1 Security Boundary:** | OA-8401-M-NHQ-3322 |
| **2 System Owner:** | Dennis Groth |
| **3 FIPS 199** | Moderate |
| **4 IT System Type:** | General support system |
| **5 System Security Categorization:** | Moderate |
| **6 Data Types(s):** | **C.2.8.9 Personal Identity and Authentication** =  {(Confidentiality, Moderate), (Integrity, Moderate), (Availability, Moderate)}  C.2.3.6 Workforce Planning Information Type =  {(Confidentiality, Low), (Integrity, Low), (Availability, Low)} |

## Risks:

**No risks identified.**

# Recommendation

HITSS Security has determined the following security ratings: The likelihood that a potential vulnerability could be exercised by a given threat-source is Low. The adverse impact resulting from a successful threat-source exploiting vulnerability is Low. The overall risk determination for the proposed SR is Low.

HITSS Security recommends that ITCD proceed as normal.