**Purpose:** The Security Self-Assessment Checklist (SSAC) is used by the NASA Headquarter Information Technology System Services (HITSS) Security Team to assess the security posture of an application/information system. The information collected in this document maps directly to NASA Procedural Requirements and NIST Special Publication 800-53 Security Controls. The information will be used to perform a risk assessment and be used to update the applicable NASA HQ System Security Plan (SSP). Below is a listing of the sections within the SSAC:

**Section 1: General Service Request Information**

**Section 2: Risk Management Information**

**Section 3: Infrastructure Information**

**Section 4: Application/Interface Information**

**Section 1: General Service Request Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **General Service Request Information** | | | |
| **Service Request #:** | 2015-0002618 | **ORR Date:** | 2015-06-05 |
| **PM Name:** | Luis Ayala | **Phone Number:** | 202 350 2103 |
| **Developer Name:** | Marithe Le | **Phone Number:** | 571 385 4030 |
| **IT Security Name:** | Karim Said | **Phone Number:** | 202 358 0985 |

**Section 2: Risk Management Information**

|  |  |
| --- | --- |
| **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)} |

**Section 3: Infrastructure Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Infrastructure Information** | | | |
| **7 System Name:** | cmts.hq.nasa.gov (App Server), rivers.hq.nasa.gov (Database Server) | | |
| **8 Management IP Address:** | cmts.hq.nasa.gov: TBD  Rivers: 131.182.5.219 | | |
| **9 Hardware Type:** | cmts.hq.nasa.gov: HQ VM  rivers: N/A | | |
| **10 Operating System:** | cmts.hq.nasa.gov: Red Hat 6.5  rivers: Sun One | | |
| **11 Ports/Protocols:** | cmts.hq.nasa.gov: 443  rivers: 1521 | | |
| **12 Encryption Type:** | SSL | | |
| **13 System Administrator(s):** | UNIX team, DBA | | |
| **14 System Account Type(s):** | Individual | | |
| **14a Do regular users have accounts on the system?** | No | | | |
| **15 Permission Type(s):** | Role-based | | |
| **16 Authentication Type(s):** | Access Launchpad username and password/ RSA Authentication | | |
| **17 Audit Log Location(s):** | Audit log is stored on the ColdFusion server | | |
| **18 System Password Policy** | | | |
| **a Length:** | N/A | **e Complexity:** | N/A |
| **b History:** | N/A | **f Nontrivial Enforced:** | N/A |
| **c Age:** | N/A | **g Password Recovery:** | N/A |
| **d Encrypted:** | N/A | **h Lockout Tolerance:** | N/A |
| **19 Local Access Restrictions:** | Authentication page | | |
| **20 Remote Access Restriction(s):** | Firewalls and VPN | | |
| **21 Baselines:** | HITSS Solaris Build, CIS Oracle baseline, ColdFusion build. | | |
| **22 SDD:** | N/A | | |
| **23 Backup Strategy:** | NASA HQ Enterprise Backup | | |

**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 | | |

**Section 5: Notes**

The CMTS servers are publically accessible systems. Admin web console access requires 2-factor RSA authentication. Network based intrusion detection systems are monitoring inbound and outbound traffic. Additionally, outbound traffic is protected by WebSense and DNS black holes. The NASA Security Operations Center (SOC) monitors the entire defense in depth infrastructure 24x7.

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).