CMS Information Security

1 INFORMATION SECURITY

The *Federal Information Security Management Act of 2002 (Public Law 107-347) (FISMA)* requires each agency to develop, document, and implement an agency-wide Information Security program to safeguard information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, (including Subcontractors) or other source on behalf of an agency. That is, agency information security programs apply to all organizations (sources) which have physical or electronic access to a Federal agency's computer systems, networks, or IT infrastructure; or use information systems to generate, store, process, or exchange data with a Federal agency, or on behalf of a Federal agency, regardless of whether the data resides on a Federal Agency or a Contractor's information system. This includes services that are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions.

The Contractor and all of its respective Subcontractors shall follow and remain compliant at all times with all CMS and Federal Information Technology (IT) Security standards, policies, and reporting requirements, as well as all National Institute of Standards and Technology (NIST) standards and guidelines, other Government-wide laws and regulations for the protection and security of Government Information.

All CMS Contractors shall comply with CMS policies and other requirements below, as well as documents referenced within those policies:

- ***CMS Policy for Information Security (PIS)*** (as amended) – The high level CMS policy for the CMS Information Security Program, and is available athttp://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity.

- ***CMS Policy for the Information Security Program (PISP)*** (as amended) - Sets the ground rules under which CMS shall operate and safeguard its information and information systems to reduce the risk and minimize the effect of security incidents. This document will subsequently reference the Contractor-applicable *Acceptable Risk Safeguards (ARS)* manual and the *Risk Management Handbook (RMH)*, Volumes I, II, and/or III) Security Standards and Procedures, and is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity.

- ***CMS Policy for Investment Management and Governance*** (as amended) - Establishes the policy for systematic review, selection/reselection, implementation/control, and

continual evaluation of IT investments at CMS, and is available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/ITInvestman/index.html.

- ***Cloud Services*** - For "Cloud services[1]," all cloud-specific requirements will be as defined in Section 1.3, *Cloud-based Services*. However, for information identified as *Personally Identifiable Information (PII), Protected Health Information (PHI)*, and/or *Federal Tax Information (FTI)*, the additional security and privacy requirements listed in the ARS manual *Implementation Standards* (as amended), as applicable to PII, PHI, and/or FTI, shall be applied within cloud-based services.

- ***The CMS Information Security website at*** http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity provides a list of applicable security policies and procedures across the program.

A summary of these requirements are listed in the *Applicable Laws and Regulations* sections of the above listed CMS policies, as well as in the *Applicable Laws and Regulations* section of the *Health and Human Services (HHS) Office of the Chief Information Officer (OCIO) Policy for Information Systems Security and Privacy*, available at http://www.hhs.gov/ocio/policy/index.html.

1.1 GENERAL INFORMATION SECURITY RESPONSIBILITIES

The Contractor and all of its respective Subcontractors shall:

A. Establish senior management level responsibility for information security;

B. Define key information security roles and responsibilities within their organization;

C. Comply with a minimum set of controls established for protecting all Federal information;

D. Comply with CMS policies and procedures for information security, as well as reporting requirements.

1.1.1 SYSTEM SECURITY OFFICER

The Contractor shall appoint a Systems Security Officer (SSO) to oversee its compliance with the CMS information security requirements. The SSO responsibilities shall include implementation and oversight of all information security requirements and implementations.

[1] As defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145, *NIST Definition of Cloud Computing*, as amended.

1.1.2 SYSTEM SECURITY LEVEL

The Contractor shall develop and apply appropriate security controls to meet CMS information security requirements, as defined in the applicable appendix of the ***ARS*** manual (as amended), located on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity and in accordance with the below-listed parameters, for any/all tasks requiring the Contractor to (1) process, (2) store, (3) facilitate transport of, or (4) host/maintain Federal information (including software and/or infrastructure developer/maintainers), either at the Contractor site, or at a Federally-controlled facility (as defined in FAR Subpart 2.1):

A. **Systems Security Level:** *Low*, *Moderate*, or *High* as defined in the applicable appendix of the ***ARS*** manual, available on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity.

B. **Information Type** (as defined on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity) is used to determine the information system security level. However, additional security control requirements may be required based on the specific type of data available within the system. For information identified as *PII, PHI, and/or FTI*, the additional security and privacy requirements listed in the ARS manual *Implementation Standards*, as applicable to PII, PHI, and/or FTI, shall be applied.

C. **E-Authentication Level** 1, 2, 3, 4, or N/A, as defined in the CMS *RMH*, Volume III, Standard 3.1, *Authentication*, (available on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity) shall be applied to proof, identify and authenticate authorized users.

The contractor shall coordinate with the CMS Chief Information Security Officer (CISO) to assess and establish/update each of the above listed criteria within 30 days of contract award or when a *Significant Change*[2] has been made to its system, as defined by the CMS CISO.

1.1.3 STANDARD FOR ENCRYPTION

The Government has determined that CMS information under this contract is considered "sensitive'' in accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004.

[2] *Significant Change* means a change that is likely to affect the security state of an information system. — NIST SP 800-37 R1 p. F-7.

The following encryption requirements apply to laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive CMS information (at rest and/or in transit.) Device encryption shall occur before any sensitive data is stored on the laptop computer/mobile device, or within 45 days of the start of the contract, whichever occurs first.

The Contractor shall:

A. Use encryption that complies with FIPS 140-2, *Security Requirements for Cryptographic Module*, (as amended) to protect all instances of CMS sensitive information during storage and transmission.

B. Verify that the selected encryption product has been validated under the *Cryptographic Module Validation Program* (see http://csrc.nist.gov/cryptval/) to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the CMS CISO.

C. Use the *Key Management Key* (see Chapter 4 of FIPS 201) on the CMS Personal Identity Verification (PIV) card; or alternatively, the Contractor shall establish and use a key recovery mechanism to ensure the ability for authorized personnel to decrypt and recover all encrypted information (see http://csrc.nist.gov/drivers/documents/ombencryption-guidance.pdf). The Contractor shall notify the *Contracting Officer's Representative (COR)* of personnel authorized to decrypt and recover all encrypted information.

D. Securely generate and manage encryption keys to prevent unauthorized decryption of information in accordance with FIPS 140-2.

E. Ensure this encryption standard (all of section 1.1.3) is incorporated into the Contractor's property management/control system in order to account for all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive CMS information.

1.2 NON-CLOUD-BASED SERVICES

1.2.1 Information Security and Privacy

1.2.1.1 POSITION SENSITIVITY DESIGNATIONS

Contractor personnel shall be required to undergo a background investigation commensurate with the *Homeland Security Presidential Directive (HSPD) 12* position-sensitivity levels for the Personal Identity Verification card required to access, develop, or host and/or maintain a Federal information system(s).

The Contractor shall submit a roster that includes the name, position, email address, phone number, and area of responsibility/job functions of all staff (including Subcontractor staff)

working on the contract where the Contractor shall access, develop, or host and/or maintain a Federal information system(s). The roster shall be submitted to the COR within 14 calendar days of the effective date of any contract. Any revisions to the roster (for any reason) shall be submitted within 15 calendar days of the change.

The Contractor shall be notified by the government of the appropriate level of investigation required for each staff member. Suitability investigations are required for contractors who will need access to CMS information systems and/or CMS physical space. All Contractor employees shall comply with the conditions established for their designated position sensitivity level prior to performing any work under this contract. Upon beginning work, contractors must be issued a temporary badge and submit to fingerprinting.

1.2.1.2 INFORMATION SECURITY AWARENESS TRAINING

All Contractor employees having access to (1) Federal information or a Federal information system, (2) PII or, (3) physical or logical access to CMS IT resources, shall complete *Information Security and Privacy Awareness* training courses prior to performing any work under this contract. Thereafter, Contractor employees having the above access shall complete an annual CMS-specified refresher course during the period of performance of a contract.

CMS requires role-based training when responsibilities associated with a given role or position could, upon execution, have the potential to adversely impact the security posture of one or more CMS systems. CMS *Annual Role-Based Information Security Training Requirements* (as amended) are available at https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/CIO-Directives-and-Policies/CIO-Directives-List.html.

The Contractor shall record completion of *Information Security and Privacy Awareness* training and *Role-Based Security Training* and retain the results in accordance with CMS procedures available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity. Training shall be consistent with the requirements contained in the *Code of Federal Regulations* (C.F.R.) Part 5 Subpart C (5 C.F.R. 930.301) and conducted at least annually. The Contractor shall maintain a listing by name and title of each contractor employee working under contract with CMS that has completed the CMS mandatory training. The list shall be provided to the contract specific COR upon request to satisfy *Federal Information Security Management Act (FISMA)* requirements.

1.2.1.3 RULES OF BEHAVIOR

The Contractor shall ensure that all employees, including Subcontractor employees, comply with the *HHS Rules of Behavior (RoB) (For Use of Technology Resources and Information)*, which is available at http://www.hhs.gov/ocio/policy/. All users of HHS IT resources must read these rules and sign the accompanying acknowledgement form (within the above document) before accessing Department data/information, systems and/or networks. This acknowledgement must

be signed annually to reaffirm knowledge of, and agreement to adhere to the HHS RoB. The HHS RoB may be presented to the user in writing or electronically, and the user's acknowledgement may be obtained by written or electronic signature. These affirmations shall be provided to a contract specific COR upon request.

Contractor personnel with access to specific CMS systems may be required to sign additional *Rules of Behaviors* specific to those systems.

1.2.1.4 PRIVACY DOCUMENTATION

Contractors shall be responsible for coordinating with the CMS Privacy Officer to ensure all applicable Federal privacy requirements are being met to include, but not limited to, Privacy Act *System of Records Notification (SORN), Privacy Impact Assessments (PIAs), Data Use Agreements (DUAs),* and *Computer Matching Agreements (CMAs)* in accordance with CMS procedures available at http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy.

1.2.1.5 COMMITMENT TO PROTECT NON-PUBLIC INFORMATION CONTRACTOR AGREEMENT

The Contractor shall guarantee strict confidentiality of the information/data that is provided by the Government during the performance of a CMS contract.

1.2.2 SYSTEMS SECURITY REQUIREMENTS

1.2.2.1 COMMON SECURITY CONFIGURATIONS

The Contractor shall apply approved security configurations to IT that are used to process information on behalf of CMS.

1. The Contractor shall configure its computing systems that contain CMS data, and using "Windows"-related operating systems, including desktops and laptops—regardless of function—but not including servers, using the applicable *United States Government Configuration Baseline (USGCB)* baselines (see http://usgcb.nist.gov/index.html) and ensure that its computers have and maintain the latest operating system patch level and anti-virus software level.

2. Remaining security baseline requirements are specified in the ARS manual, security control requirement CM-6 – *Configuration Settings,* and its applicable *Enhancements* (located on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity).

3. Deviations must be approved by the CMS CISO.

The Contractor shall ensure IT applications operated on behalf of CMS are fully functional and operate correctly on systems configured in accordance with the above configuration requirements. The Contractor shall use *Security Content Automation Protocol (SCAP)*-validated tools to ensure its products operate correctly with baseline configurations and do not alter applied settings. (See http://nvd.nist.gov/validation.cfm.) The Contractor shall test applicable product versions with all relevant and current updates and patches installed. The Contractor shall ensure currently-supported versions of IT products meet the latest baseline major version, and subsequent major versions.

The Contractor shall ensure:

A. IT applications designed for end users run in the standard user context without requiring elevated administrative privileges.

B. Hardware and software installation, operation, maintenance, update, and patching will not alter the configuration settings or requirements specified above.

C. Servers, desktops, and laptops operated on behalf of CMS (1) include *Federal Information Processing Standard (FIPS) 201*-compliant (see http://csrc.nist.gov/publications/PubsFIPS.html), *Homeland Security Presidential Directive 12 (HSPD-12)* card readers with the purchase of servers, desktops, and laptops; and (2) comply with FAR Subpart 4.13, *Personal Identity Verification (PIV)*.

D. Microsoft "Windows"-based software should use the *Windows Installer Service* for installation to the default appropriate OS "Program Files" directory, and should be able to silently install and uninstall, under central administrator control.

E. All subcontractors (at all tiers) performing work under this contract shall comply with the requirements contained in this clause.

1.2.2.2 TRACKING AND CORRECTING SECURITY DEFICIENCIES

The Contractor shall track and correct any applicable information security deficiencies, conditions, weaknesses, findings, and gaps identified by audits, reviews, security control assessments, and tests, including those identified in *Chief Financial Officer (CFO)* audits, *FISMA* audits, *Statement on Standards for Attestation Engagements (SSAE) No. 16* (or *Statement on Auditing Standards [SAS] 70)* reviews, *Medicare Modernization Act (MMA) Section 912* evaluations and tests, *Inspector General (IG)* audits and reviews, *OMB Circular A-123 Management's Responsibility for Internal Controls* audits, other applicable reviews and audits, and CMS *Security Operations Center (SOC)* continuous monitoring activities such as, but not limited to, vulnerability and compliance scanning of all the CMS information systems. All *high-risk* deficiencies shall be mitigated within 30 days and all *moderate-risk* deficiencies shall be

mitigated within 90 days from the date deficiencies are formally identified. The Government will determine the risk rating of identified deficiencies.

1.2.2.3 INCIDENT RESPONSE

An information security incident is a violation, or an imminent threat of a violation, of an explicit or implied information security policy, acceptable use policies, or standard information security practices. While certain adverse events, (e.g. floods, fires, electrical outages, and excessive heat) can cause system crashes, they are not considered information security incidents. CMS information and information system security related incidents shall be reported using the *Risk Management Handbook*, Volume II, Procedure 7.2, *Incident Handling Procedure* available at the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity. An information security incident becomes a privacy incident when the incident involves the suspected or actual loss of PII. Incidents that may possibly concern PII shall be reported within one (1) hour of discovery.

1.2.2.4 SYSTEM AUTHORIZATION AND ASSESSMENT

The implementation of a Federal Government information system requires a formal Government Authorization to Operate (ATO) for infrastructure systems and/or all application systems developed, hosted and/or maintained on behalf of CMS. NIST Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, and CMS procedures (located on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity) give guidelines for performing the system ATO process. The system/application shall have a valid ATO (conveyed through the CMS Chief Information Officer (CIO) authorization decision process) before going into operation and processing CMS information. The failure to obtain and maintain a valid ATO may be grounds for termination of a contract.

A. The Contractor shall comply with ATO requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the ATO is based on the System's NIST FIPS 199 categorization and CMS procedures (located on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity). The Contractor shall coordinate with the CMS business owner to create, maintain, and update all applicable ATO documentation as defined by CMS Information Security procedures.

B. At the *Moderate* and *High* impact levels, all CMS systems and infrastructures must obtain an **independent** Security Assessment in accordance with CMS procedures (located on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity). The

Contractor shall allow CMS employees (or CMS CISO-designated third-party Contractors) to conduct Security Assessment activities to include control reviews in accordance with NIST SP 800-53/NIST SP 800-53A and CMS procedures and standards (located on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity). This includes the system supporting-infrastructure.

C. Identified gaps between required controls and the Contractor's implementation as documented in the applicable *Security Assessment Report (SAR)* shall be tracked for mitigation in a *Plan of Action and Milestones (POA&M)* completed in accordance with CMS procedures (located on the CMS Information Security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity). Depending on the severity of the gaps, the Government may require them to be remediated ***before*** an ATO is issued.

D. The Contractor shall be responsible for mitigating all applicable security risks found during the ATO process and continuous monitoring activities. All *high-risk* vulnerabilities must be mitigated within 30 days and all *moderate-risk* vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of identified vulnerabilities.

1.2.2.5 SECURITY CONTROLS COMPLIANCE ASSESSMENTS

On a periodic basis, the Government, including but not limited to, the *Office of Inspector General*, reserves the right to evaluate any/all of the security controls implemented by the Contractor.

The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the Contractor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisition Regulation (FAR) 52.239-1, Privacy or Security Safeguards, the Contractor shall be responsible for the following privacy and security safeguards:

A. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

B. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection shall include, but is not limited to:

a. Authenticated and unauthenticated operating system/network vulnerability scans,

b. Authenticated and unauthenticated web application vulnerability scans,

c. Authenticated and unauthenticated database application vulnerability scans,

d. Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

C. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

1.2.2.6 CONTINUOUS MONITORING

The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the Contractor's IT environment being used to provide or facilitate services for CMS in support of the Federal requirements to perform continuous monitoring. Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

In addition to the requirements to meet all of the CMS Information Security requirements documented at the http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity website, the Contractor shall work closely with the CMS *Security Operations Center (SOC)* to undertake security related activities including, but not limited to, the following:

A. **Continuous Monitoring Program**: As part of the CMS Continuous Monitoring Program, the Contractor's SSO shall be the official point of contact for CMS security data calls. The Contractor SSO shall provide timely responses (within no less than 48 hours) to informational requests for Contractor security status and posture. These requests may include, but are not limited to hardware/software patch implementation levels, status for specific IT security updates, system/infrastructure inventories; component or technology inventories, specific software inventories, specific network traffic levels, or other security-specific metrics.

The Contractor shall be responsible for supporting the CMS continuous monitoring program by providing automated data feeds to the CMS *Security Operations Center (SOC)* as required by the CMS CISO. The CMS SOC will supplement this by conducting independent oversight continuous monitoring activities such as, but not limited to, vulnerability and compliance scanning as well as other network monitoring related activities of all the CMS information systems. The CMS SOC provides information

security oversight and monitoring of security events across all monitored information systems that support the operations and assets of CMS. The CMS SOC will notify the appropriate security operations staff (Contractor and/or Government) of potentially malicious traffic.

Contractor shall provide updated network architecture, IP address ranges, and security points of contact information for the systems they operate on behalf of CMS to the CMS SOC on a monthly basis.

B. **SOC Credential Scanning**: Contractor shall maintain and provide changes to the system accounts needed for the CMS SOC credentialed scanning two weeks before the passwords expire or when other changes to the accounts are needed.

C. **Environmental Support**: Contractor shall provide rack space, cabling, connectivity, and appropriate environmental support for SOC-managed systems/appliances as required by the CMS CISO.

D. **Asset Management**: Upon request by the COR, the Contractor shall use any available *SCAP*-compliant automated tools to provide an inventory of all IT assets for both hardware and software, (computers, servers, routers, databases, operating systems, etc...) that are processing Government-owned information/data. It is anticipated that this inventory information will be produced at least monthly. The Contractor shall be capable of providing detailed IT asset inventory information, to include IP address, machine name, operating system level, and security patch level, and SCAP-compliant format information. When requested by the Government, the Contractor shall provide the results of the IT inventory accountability using automated tools to the Government within 48 hours.

E. **Configuration Management**: Upon request by the Government, the Contractor shall use available SCAP-compliant automated tools to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, applications, etc...) that are processing Government-owned information/data. Compliance will be measured using IT asset and system security configuration guidance provided by the Government, for a number of specific IT assets. The SCAP-compliant automated tools will compare the installed configuration to the Government specific security configuration guidance. It is anticipated that this IT asset security configuration information will be produced at least monthly. When requested by the Government, the Contractor shall provide the results of the IT asset security configuration compliance status using automated tools to the Government within 48 hours.

F. **Vulnerability Management**: Upon request by the Government, the Contractor shall use SCAP-compliant automated tools to detect any security vulnerabilities in all IT assets, (computers, servers, routers, Web applications, databases, operating systems, etc...) that are processing Government-owned information/data. It is anticipated that this IT asset security vulnerability information will be produced at least monthly. When requested by the Government, the Contractor shall provide the results of the IT asset security vulnerability scans using automated tools to the Government within 48 hours.

G. **Data Protection**: Current Federal Government security guidance requires that sensitive Government information that is stored on laptops and other portable computing devices shall be encrypted using *FIPS* 140-2 validated encryption. Upon request by the Government, the Contractor shall provide the percentage of portable IT assets that are equipped with FIPS 140-2 validated encryption, to encrypt all sensitive Government information. The IT asset security vulnerability information shall be submitted quarterly.

H. **Remote Access**: Current Federal Government security guidance requires that two factor authentication be utilized when remotely accessing sensitive Government-owned information/data on IT systems (both Government-owned, and Contractor-owned systems). Additional Federal Government security guidance when remotely accessing Government-owned information/data include the following:

- Connections shall utilize FIPS 140-2 validated encryption;
- Connections shall be capable of assessing and correcting system configurations upon connection;
- Connections shall be capable of scanning for viruses and malware upon connection;
- Connections shall prohibit split tunneling; and,
- Connections shall require timeout after 15 minutes of inactivity.

Upon request by the Government, the Contractor shall provide the following information about the Contractor's remote access solutions to Government-owned sensitive information/data:

- Percentage of current connections that allow connection using only a password;
- Percentage of connections that require the use of a Government provided personal identity verification (PIV) card as part of a two-factor solution;
- Percentage of connections that require the use of other two-factor authentication solutions;
- Percentage of connections that utilize FIPS 140-2 encryption;
- Percentage of connections that assess and correct system configurations upon connection;
- Percentage of connections that scan for viruses and malware upon connection;
- Percentage of connections that prohibit split tunneling; and,

- Percentage of connections that require timeout after 15 minutes of inactivity.

The remote access information shall be submitted quarterly.

I. **Incident Management**: Upon direction from the Government, the Contractor shall install critical security patches or take other security remediation action as directed to Federal agencies by the Department of Homeland Security (DHS) to resolve evolving weaknesses in systems processing Government-owned information/data (including reported incidents with CMS, or within *other* non-CMS Government systems). When directed, the Contractor shall report system(s) status, and provide notification when directed action has been completed. The urgent security remediation action shall be submitted two (2) times per month.

1.3 CLOUD-BASED SERVICES

1.3.1 Systems Security Requirements

In his December 8, 2011 memo titled *Security Authorization of Information Systems in Cloud Computing Environments* (available at https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf), the Federal CIO established policy for the protection of Federal information in cloud services under the *Federal Risk and Authorization Management Program (FedRAMP)*. Under the FedRAMP policy, agencies with existing cloud-based services, or that are acquiring new cloud-based services, ***shall*** use the FedRAMP information security and privacy requirements for *cloud-based services* (as defined in the *CMS RMH*, Volume III, Standard 3.2, *CMS Cloud Computing Standard*, available at the CMS information security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity) to support ATO decisions. CMS will leverage cloud services assessed-and-granted *Provisional Authorization* (as defined and granted by the FedRAMP *Joint Authorization Board [JAB]*) through the FedRAMP process to increase efficiency and ensuring security compliance.

High impact (security level) systems are ***not permitted*** in non-government-hosted cloud environments—and are not supported by the FedRAMP program. The minimum requirements for *Low* and *Moderate* impact cloud systems are contained within the *FedRAMP Cloud Computing Security Requirements Baseline* (available at http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip.) The Contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

CMS will determine the necessary security category for the cloud-based systems in accordance with *FIPS 199* (available at http://csrc.nist.gov/publications/PubsFIPS.html) and applicable CMS security policy and procedures (available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/). The Contractor shall apply the

appropriate set of security controls as required in the *FedRAMP Cloud Computing Security Requirements Baseline* document[3] (available at http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip) to ensure compliance to security standards.

1.3.2 FedRAMP Repository Requirements

The Contractor shall perform the necessary steps to ensure their cloud services are entered into the FedRAMP *Secure Repository*, in accordance with the FedRAMP *Concept of Operations (CONOPS)* available at http://www.fedramp.gov/, **with the following stipulations**:

1.3.2.1 INFRASTRUCTURE AS A SERVICE (IAAS) AND PLATFORM AS A SERVICE (PAAS)

For *Infrastructure as a Service (IaaS)* and *Platform as a Service (PaaS)* service providers (as defined in the *CMS RMH*, Volume III, Standard 3.2, *CMS Cloud Computing Standard*, available at the CMS information security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity), the following FedRAMP requirements shall be met:

- The Contractor shall create, maintain, and update *Assessment and Authorization* documentation **using FedRAMP templates and processes**, which are available at http://www.fedramp.gov/.

- For cloud-based services that may host *PII*[4] or *PHI*[5] or *Electronic PHI (ePHI)*, additional and mandatory security and privacy controls are defined in the *ARS* manual, as amended, in Appendix B, *CMS Minimum Security Requirements (CMSRs) for Moderate Impact Level Data* (available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity), and shall be applied.

- The Contractor shall be assessed utilizing a FedRAMP Accredited *Third-Party Assessment Organization (3PAO)* to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements. A listing of accredited 3PAOs is available at http://www.fedramp.gov/.

---

[3] The FedRAMP baseline controls are based on NIST Special Publication 800-53 (as amended), *Security and Privacy Controls for Federal Information Systems and Organizations* (available at http://csrc.nist.gov/publications/PubsSPs.html), and also includes a set of additional controls for use within systems providing cloud-based services to the federal government.

[4] PII is defined by OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

[5] PHI is defined in 45 C.F.R. §160.103, available at http://edocket.access.gpo.gov/cfr_2004/octqtr/pdf/45cfr160.103.pdf.

- The Contractor must have the applicable cloud service accepted by the FedRAMP *Program Management Office (PMO)* and available in the FedRAMP *Secure Repository* by June 5, 2014, or within 90 days of award; whichever is *later*.

- The Contractor *shall* receive a *JAB*–issued *Provisional Authorization* by June 5, 2014, or within 90 days of award; whichever is *later*.

- The Government may terminate a contract if the Contractor has 1) failed to achieve a FedRAMP provisional authorization by June 5, 2014 (or within 90 days of award; whichever is *later*) or, 2) for any reason, has its JAB-issued *Provisional Authorization* denied or revoked, and the deficiencies are greater than CMS risk tolerance thresholds—as determined solely by CMS.

1.3.2.2 SOFTWARE AS A SERVICE (SAAS)

For *Software as a Service (SaaS)* service providers (as defined in the *CMS RMH*, Volume III, Standard 3.2, *CMS Cloud Computing Standard*, available at the CMS information security website at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity), the following FedRAMP requirements shall be met:

- The Contractor shall create, maintain, and update *Assessment and Authorization* documentation **using FedRAMP templates**, which are available at http://www.fedramp.gov/.

- For cloud-based services that may host *PII*[6] or *PHI*[7] or *ePHI*, additional and mandatory security and privacy controls are defined in the *ARS* manual, as amended, in Appendix B, *CMS Minimum Security Requirements (CMSRs) for Moderate Impact Level Data* (available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity), and shall be applied.

- The Contractor shall be assessed utilizing a FedRAMP accredited 3PAO to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements. A listing of accredited 3PAOs is available at http://www.fedramp.gov/.

- The Contractor shall have the applicable cloud service accepted by the FedRAMP PMO and available in the FedRAMP *Secure Repository* by June 5, 2014, or within 90 days of award; whichever is *later*.

[6] PII is defined by OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.
[7] PHI is defined in 45 C.F.R. §160.103, available at http://edocket.access.gpo.gov/cfr_2004/octqtr/pdf/45cfr160.103.pdf.

- Contractors that receive a JAB-issued *Provisional Authorization* will be given preference.

- The Government may terminate for default this Contract/Award and any outstanding orders, if the Contractor has 1) failed to have the applicable cloud service available (listed and maintained) in the FedRAMP repository by June 5, 2014 (or within 90 days of award; whichever is ***later***) or, 2) for any reason, is removed or revoked from the FedRAMP repository, and the deficiencies are greater than CMS risk tolerance thresholds—as determined solely by CMS.

1.3.3 FedRAMP Privacy Requirements

Contractor shall be responsible for the following privacy and security safeguards:

A. To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

B. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, then the discoverer shall immediately bring the situation to the attention of the other party.

C. The Contractor shall comply with any *additional*, current or future, FedRAMP privacy requirements. The Contractor shall also comply with any *additional*, current or future, *Health Insurance Portability and Accountability Act (HIPAA), Privacy Act of 1974*, or *Health Information Technology for Economic and Clinical Health (HITECH) Act* privacy, security, and breach notification requirements as appropriate for the data being handled (as specified by CMS).

D. The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the Contractor's IT environment being used to provide or facilitate services for the Government. In accordance with the FAR clause 52.239-1, Contractor shall be responsible for the following privacy and security safeguards:

   a. The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

   b. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of Government data, the Contractor shall afford the Government access to the

Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of notification. The program of inspection shall include, but is not limited to:

i. Authenticated and unauthenticated operating system/network vulnerability scans,

ii. Authenticated and unauthenticated web application vulnerability scans,

iii. Authenticated and unauthenticated database application vulnerability scans,

iv. Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.

If the Contractor chooses to run its own automated scans or audits, then the results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of contractor-conducted scans shall be provided, in full, using NIST SCAP standards, to the Government, upon request, but no less than every 30 days.

Sensitive Information Storage

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a *Need-To-Know* basis. The Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, *Guidelines for Media Sanitization*, available at http://csrc.nist.gov/publications/PubsSPs.html.

The disposition of all data shall be at the written direction of the Government. This may include documents returned to Government control; destroyed; or held as specified until otherwise directed.

Protection of Information

The Contractor shall be responsible for properly protecting and safeguarding all information used, gathered, or developed as a result of work under this contract. The Contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract shall be considered as SBU information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If Contractor must remove any information from the primary work

area, then they shall protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any information that is subject to the *Privacy Act of 1974*, *HIPAA*, and/or *HITECH* will be utilized in full accordance with all rules of conduct as applicable to *Privacy Act of 1974*, *HIPAA*, and/or *HITECH* information, respectfully.

The data shall be available to the Government upon request within one (1) business day.

Security Classification

The preparation of the deliverables in this contract will be completed at a *Sensitive but Unclassified (SBU)* level.

1.3.4 Security Requirements Section

High impact (security level) systems are *not permitted* in non-government hosted cloud environments—and are not supported by the FedRAMP program. The minimum requirements for *Low* and *Moderate* impact cloud systems are contained within the *FedRAMP Cloud Computing Security Requirements Baseline* (available at http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip). The Contractor and CMS share responsibility to ensure compliance with security requirements.

1.3.4.1 ASSESSMENT & AUTHORIZATION

The implementation of a new Federal Government cloud system requires a formal process, known as *Assessment and Authorization*, which provides guidelines for performing the assessment.

FedRAMP requires cloud service providers to utilize a FedRAMP accredited 3PAO to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements. A listing of accredited 3PAOs is available at http://www.fedramp.gov/.

The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a *Provisional Authorization* decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

CMS will be able to *leverage* the *Provisional Authorization* granted by FedRAMP and any documentation prepared by the Contractor to issue a CMS ATO. A CMS-issued ATO **is required** before any *Production* (vice *Development* or *Testing*) operations may commence, or CMS sensitive information may be place in a cloud-based environment.

The Contractor is advised to review the FedRAMP guidance documents to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://www.fedramp.gov/.

1.3.4.2 FEDRAMP SECURITY COMPLIANCE REQUIREMENTS

The Contractor shall implement the controls contained within the *FedRAMP Cloud Computing Security Requirements Baseline* (available at http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip) and *FedRAMP Continuous Monitoring Requirements* (available at http://www.fedramp.gov/) for *Low* and *Moderate* impact systems (as defined in *FIPS* 199 and CMS processes). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both *Low* and *Moderate* impact systems. For information identified as *PII, PHI,* and/or *FTI,* the additional security and privacy requirements listed in the ARS manual *Implementation Standards*, as applicable to *PII*, *PHI*, and/or *FTI*, shall be applied within cloud-based services.

1.3.4.3 REQUIRED FEDRAMP POLICIES AND REGULATIONS

- The Office of Management and Budget (OMB) Memo entitled *Security Authorization of Information Systems in Cloud Computing Environments*, dated December 8, 2011, available at https://cio.gov/wp-content/uploads/2012/09/fedrampmemo.pdf.

1.3.4.4 ASSESSMENT OF THE SYSTEM

A. The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Contractor shall create, maintain and update the following documentation **using FedRAMP templates**, which are available at http://www.fedramp.gov/:

   - Privacy Impact Assessment (PIA)
   - FedRAMP Test Procedures and Results
   - Security Assessment Report (SAR)
   - System Security Plan (SSP)
   - IT System Contingency Plan (CP)
   - IT System Contingency Plan (CP) Test Results
   - Plan of Action and Milestones (POA&M)
   - Continuous Monitoring Plan (CMP)
   - FedRAMP Control Tailoring Workbook
   - Control Implementation Summary Table
   - Results of Penetration Testing

- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements

B. Information systems must be assessed by a FedRAMP Accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan. A listing of FedRAMP accredited 3PAOs is available at http://www.fedramp.gov/.

C. The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the Contractor shall allow Government employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements. Review activities include, but are not limited to, scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

D. Identified gaps between required *FedRAMP Security Control Baselines and Continuous Monitoring* controls and the Contractor's implementation as documented in the FedRAMP *Security Assessment Report (SAR)* shall be tracked by the Contractor for mitigation in a *Plan of Action and Milestones (POA&M)* document. Depending on the severity of the gaps, the Government may require them to be remediated before a *Provisional Authorization* is issued.

E. The Contractor is responsible for mitigating all security risks found during Assessment and Authorization and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

1.3.4.5 AUTHORIZATION OF SYSTEM

The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an IT security program. The Government reserves the right to conduct on-site inspections. The Contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

1.3.4.6 REPORTING AND CONTINUOUS MONITORING

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a Contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective

over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors shall provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

Additional Stipulations

A. The FedRAMP deliverables shall be labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or Contractor selected designation per document sensitivity. External transmission/dissemination of For Official Use Only (FOUO) and CUI to-or-from a Government computer shall be encrypted. Certified encryption modules shall be used in accordance with FIPS 140-2, "*Security requirements for Cryptographic Modules."*

B. Federal Desktop Core Configuration & US Government Configuration Baseline: The Contractor shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC) and US Government Configuration Baseline (USGCB). The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved FDCC/USGCB configuration. Offerings that require installation shall follow OMB memorandum 07-18 entitled *Ensuring New Acquisitions Include Common Security Configurations*. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The Contractor shall use SCAP-validated tools with FDCC/USGCB Scanner capability to certify their products operate correctly with FDCC/USGCB configurations and do not alter FDCC/USGCB settings.

C. As prescribed in the FAR Part 24.104, if the system involves the design, development, or operation of a system of records on individuals, the Contractor shall implement requirements in FAR clause 52.224-1, "Privacy Act Notification" and FAR clause 52.224-2, "Privacy Act."

D. The Contractor shall cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal government's agent.

1.3.4.7 FEDRAMP REFERENCES

- FedRAMP Cloud Computing Security Requirements Baseline http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip.

- FedRAMP Concept of Operations
  http://www.gsa.gov/graphics/staffoffices/FedRAMP_CONOPS.pdf.

- FedRAMP Templates
  http://www.gsa.gov/graphics/staffoffices/Updated_Templates_Final.zip.

ITEMS TO BE FURNISHED AND DELIVERABLES LIST: The Contractor shall submit all required reports and deliverables in accordance with the following schedule. Reports and/or deliverables submitted shall be in accordance with the information security requirements and information provided by the applicable link (i.e. additional information column) and are submitted on a comprehensive basis covering all CMS contracts, e.g., **multiple submissions for each contract are not required unless otherwise stated herein.**

External transmission/dissemination of For Official Use Only (FOUO) and CUI to-or-from a Government computer shall be encrypted. Certified encryption modules shall be used in accordance with FIPS PUB 140-2, *Security requirements for Cryptographic Modules*, available at http://csrc.nist.gov/publications/PubsFIPS.html.

Table 1 — Deliverables

Area	Applicable Section	Deliverable Name	Deliverable Description	Additional Information	Deliver to	Deliverable Due Date
				All items available in the Information Security library (denoted with an ISL) can be found at the link below. For brevity, only the title of the document as it appears on the website is listed below. All of these documents are available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html**.**		
Security	Section(s) 1.2.2.4/ 1.3.4.4	IT Systems Contingency Plan Reports	Information Technology (IT) Systems Contingency Plan, Contingency Plan Test Plan, Contingency Plan Test After Action Report	- CP Procedure (ISL), CP Template (ISL) - CP Test Template for Tabletop Tests (ISL)	CMS CISO – Mailbox: CISO@cms.hhs.gov	Initial within 90 days of award of a contract and updated annually thereafter
Security	Section(s) 1.2.2.1/ 1.2.2.4/ 1.3.4.1/ 1.3.4.4	IT Security Tests And Reports	Contractor conducted or any other independent IT evaluation	- Assessment Plan Template (ISL) - Assessment Procedure (ISL) - Assessments - Application Finding Report Template (ISL) - Assessments - Infrastructure Finding Report Template (ISL)	CMS CISO – Mailbox: CISO@cms.hhs.gov	10 business days after conducted and as required
Security	Section(s) 1.2.2.4	Risk Assessment Report	Risk Assessment Performed	- Risk Assessment Procedure (ISL) - Risk Assessment Template (ISL)	CMS CISO – Mailbox: CISO@cms.hhs.gov	Initial within 90 days of award of a contract and updated annually thereafter
Security	Section(s) 1.2.2.4	Systems Security Plan	Systems Security Plan (SSP) and SSP Workbook	- SSP Procedure (ISL) - SSP Template (ISL) - SSP Workbook App A High Impact Level Data (ISL) - SSP Workbook App B Moderate Impact Level Data (ISL) - SSP Workbook App C Low Impact Level Data (ISL) - SSP Workbook App D-G Level 1-4 e-Authentication (ISL) - SSP Workbook Main (ISL)	CMS CISO – Mailbox: CISO@cms.hhs.gov	Initial within 90 days of award of a contract and updated annually thereafter

Area	Applicable Section	Deliverable Name	Deliverable Description	Additional Information	Deliver to	Deliverable Due Date
Security	Section(s) 1.2.2.4	Statement of Security Compliance	Attestation of annual FISMA assessment	- Authorization To Operate Package Guide (ISL)- Security Certification Form Template (ISL)- ARS (ISL)- ARS Appendix A CMSR High Impact Level Data (ISL)- ARS Appendix B CMSR Moderate Impact Level Data (ISL)- ARS Appendix C CMSR Low Impact Level Data (ISL)- ARS Appendix D CMSR e-Authentication Standard (ISL)	CMS CISO – Mailbox: CISO@cms.hhs.gov	Annually and in accordance with ARS
Security	Section(s) 1.2.2.4	FISMA Assessment	Contactor shall examine and analyze implemented security safeguards to provide evidence of compliance with applicable laws, regulations, and requirements	- ARS (ISL) - ARS Appendix A CMSR High Impact Level Data (ISL) - ARS Appendix B CMSR Moderate Impact Level Data (ISL) - ARS Appendix C CMSR Low Impact Level Data (ISL) - ARS Appendix D CMSR e-Authentication Standard (ISL)	CMS CISO – Mailbox: CISO@cms.hhs.gov	Annually in accordance with ARS
Security	Section(s) 1.2.1.2/ 1.2.2.4	Security Awareness Training Report	Contactor shall submit a report of all personnel who have received annual information security awareness and role-based training as required by FISMA	- Self developed format. - FISMA - http://csrc.nist.gov/groups/SMA/fisma/index.html	CMS CISO – Mailbox: CISO@cms.hhs.gov and Contracting Officer's Representative and/or Designee	Semi-annually (1st business day in November and 1st business day in May)
Security	Section(s) 1.2.2.4/ 1.3.4.4	Interconnection Security Agreement (ISAs) and/or Memorandum of Agreements/ Understanding (MOA/MOU) (if applicable)	Contactor shall submit any Information Technology Systems Interconnection Security Agreements (ISAs) or Memorandum of Agreements (MOUs) if applicable.	- Interconnection Security Agreement (ISA) Template (ISL) - Memorandum of Understanding (MOU) Template (ISL)	CMS CISO – Mailbox: CISO@cms.hhs.gov	Initial within 90 days of award of a contract and updated in accordance with ARS thereafter
Privacy	Section(s) 1.2.1.4/ 1.2.2.4/ 1.3.4.4	Privacy Impact Assessment	Contactor shall submit a privacy impact assessment report	- http://www.hhs.gov/pia/ - http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/Privacy-Impact-Assessment.html	CMS CISO – Mailbox: CISO@cms.hhs.gov	Initial within 90 days of award of a contract and updated annually thereafter

Area	Applicable Section	Deliverable Name	Deliverable Description	Additional Information	Deliver to	Deliverable Due Date
Security	Section(s) 1.1.3	Encryption Module Validation List	Contactor shall submit a list of validated encryption modules in use	*Cryptographic Module Validation Program* (see http://csrc.nist.gov/cryptval/)	CMS CISO – Mailbox: CISO@cms.hhs.gov	Within 45 days of award of a contract and within 30 days of when changes are made.
Security	Section(s) 1.1.3	Master Key Management List	The Contractor shall provide a Master Key Management list	Chapter 4 of FIPS 201	Contracting Officer's Representative and/or Designees	Within 45 days of award of a contract and within 30 days of changes being made
Privacy	1.2.1.1	Master Roster	The Contractor shall submit a roster	Includes the name, position, email address, phone number, and area of responsibility/job functions of all staff (including Subcontractor staff) working on the contract where the Contractor shall access, develop, or host and/or maintain a Federal information system(s).	Contracting Officer's Representative and/or Designees	Within 14 days of award of a contract, and within 15 days of changes being made
Security	1.2.2.6	IP Ranges, Points of Contact (POCs), and Architecture	The Contractor shall submit an inventory of the IP Address Range, and Security POCs	Contractor shall submit and inventory of all updated network architecture, IP address ranges, and security points of contact information for the systems they operate on behalf of CMS to the CMS SOC.	CMS CISO – Mailbox: CISO@cms.hhs.gov	Within 90 days of award of a contract and on a monthly basis thereafter
Security	1.2.2.6	IT Inventory	The contractor shall submit an inventory of all IT assets for Hardware and Software that are processing information/data that are processed and government owned.	The Contractor shall use any available SCAP-compliant automated tools to provide an inventory of all IT assets for hardware and software, (computers, servers, routers, databases, operating systems, etc...) to provide a detailed IT asset inventory.	CMS CISO – Mailbox: CISO@cms.hhs.gov	Within 90 days of award of a contract and within 48 hrs., upon COR Request

Area	Applicable Section	Deliverable Name	Deliverable Description	Additional Information	Deliver to	Deliverable Due Date
Security	1.2.2.6	Configuration Scans	The contractor shall provide IT asset security configuration compliant status using and SCAP compliant automated tool.	Upon request by the COR, the Contractor shall use available SCAP-compliant automated tools to provide visibility into the security configuration compliance status of all IT assets, (computers, servers, routers, databases, operating systems, applications, etc...) that are processing Government-owned information/data. Compliance will be measured using IT asset and system security configuration guidance provided by the Government, for a number of specific IT assets.	CMS CISO – Mailbox: CISO@cms.hhs.gov	Within 90 days of award of a contract, and monthly thereafter
Security	1.2.2.6	Vulnerability Scans	The contractor shall provide vulnerability scans using an SCAP Compliant automated tool	Upon request by the COR, the Contractor shall use SCAP-compliant automated tools to detect any security vulnerabilities in all IT assets, (computers, servers, routers, Web applications, databases, operating systems, etc...) that are processing Government-owned information/data.	CMS CISO – Mailbox: CISO@cms.hhs.gov	Within 90 days of award of a contract, within 48 hrs., or upon COR Request thereafter
Security	1.2.2.6	Portable Device Encryption	The Contractor shall provide the percentage of encrypted portable IT assets	Contractor shall provide the percentage of portable IT assets that are equipped with FIPS 140-2 validated encryption, to encrypt all sensitive Government information.	CMS CISO – Mailbox: CISO@cms.hhs.gov	Within 90 days of award of a contract and quarterly thereafter.
Security	1.2.2.6	Remote Access Compliance	The contractor shall provide information related to remote access methods	The Contractor must account for the following percentages: • Percentage of current connections that allow connection using only a password; • Percentage of connections that require the use of a Government provided personal identity verification (PIV) card as part of a two-factor solution; • Percentage of connections that require the use of other two-factor authentication solutions; • Percentage of connections that utilize FIPS 140-2 encryption; • Percentage of connections that assess and correct system configurations upon connection; • Percentage of connections that scan for viruses and malware upon connection; • Percentage of connections that prohibit split tunneling; and, • Percentage of connections that require timeout after 15 minutes of inactivity.	CMS CISO – Mailbox: CISO@cms.hhs.gov	Within 90 days of award of a contract and quarterly thereafter.

Area	Applicable Section	Deliverable Name	Deliverable Description	Additional Information	Deliver to	Deliverable Due Date
Cloud	1.3.2.1	FedRAMP	The Contractor must be an approved FedRAMP Cloud Service Provider	The Contractor must have the applicable cloud service accepted by the FedRAMP Program Management Office (PMO) and available in the FedRAMP Secure Repository by June 5, 2014, or within 90 days of award; whichever is later.	CMS CISO – Mailbox: CISO@cms.hhs.gov	By June 5, 2014, or within 90 days of award of a contract; whichever is later
Cloud	1.3.3	SCAP Scans	The Cloud Service Provider/Contractor shall submit its scanning results from a government approved SCAP scanning tool.	If the contractor chooses to run its own automated scans or audits, then the results from these scans may be accepted, at the Government's discretion, in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of contractor-conducted scans shall be provided, in full, using NIST SCAP standards, to the Government, upon request, but no less than every 30 days.	CMS CISO – Mailbox: CISO@cms.hhs.gov	By June 5, 2014, within 90 days of award of a contract; whichever is later and monthly therein and after