U.S. Department of Health and Human Services

Agency for Healthcare Research and Quality
Information Security and Privacy Program

AHRQ Security and Privacy Language for Information and Information Technology Procurements

CONTRACTS INVOLVING CLOUD SERVICES

Version 5.5

November 7, 2023

DOCUMENT CHANGE HISTORY

Version	Date	Description
1.0	August 15, 2016	Baseline Release
2.0	March 14, 2018	Document overhauled to align with *HHS Security and Privacy Language for Information and Information Technology Procurements*, Version 2.0, June 26, 2017
3.0	December 14, 2018	Updated hyperlinks
4.0	April 3, 2019	Added verbiage mandating administrator URL white listing.
4.5	May 10, 2019	Updated external hyperlinks, removed internal hyperlinks and noted these resources will be provided after contract award.
5.0	July 7, 2020	Updated vulnerability remediation timelines in Section 6. Security Assessment and Authorization (SA&A). • POA&M • Paragraph E
5.1	March 17, 2021	Added verbiage specific to annual HVA testing requirements.
5.2	June 21, 2021	Removed Records Management section.

5.3	November 16, 2021	Added section regarding reporting on user account review activities.
5.4	October 3, 2023	Removed requirement for ATO compliance within 120 days and changed to “prior to going live or hosting AHRQ data”.
5.5	November 7, 2023	Added ZTA requirements and mandated that Tenable SecurityCenter be used for vulnerability scanning.

CONTRACTS INVOLVING CLOUD SERVICES

START COPYING LANGUAGE BELOW

1. BASELINE SECURITY REQUIREMENTS

A. **Federal Policies**. The Contractor (and/or any subcontractor) shall comply with applicable federal laws that include, but are not limited to, the *HHS Information Security and Privacy Policy* (IS2P); the *AHRQ Information Security and Privacy Policy/Management Operations Manual (MOM) Instruction*; *Federal Information Security Modernization Act (FISMA) of 2014*, (44 U.S.C. 101); National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; Office of Management and Budget (OMB) Circular A-130*, Managing Information as a Strategic Resource*; and other applicable federal laws, regulations, NIST guidance, and Agency policies. Requirements contained herein may be updated as a result in changes to policies and procedures. Such changes would be coordinated with the Contractor.

B. **Applicability.** The requirements herein apply whether the entire contract or order (hereafter "contract"), or portion thereof, includes either or both of the following:

   i. Access (Physical or Logical) to Government Information: A Contractor (and/or any subcontractor) employee will have or will be given the ability to have, routine physical (entry) or logical (electronic) access to government information hosted on systems within an AHRQ controlled facility.

   ii. Operate a Federal System Containing Information: A Contractor (and/or any subcontractor) will operate a federal system and information technology containing data that supports the AHRQ mission and is physically located within an AHRQ facility. In addition to the Federal Acquisition Regulation (FAR) Subpart 2.1 definition of "information technology" (IT), the term as used in this section includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources.

C. **Safeguarding Information and Information Systems.** All AHRQ systems must be hosted internally at an AHRQ facility or by a Federal Risk and Authorization Management Program (FedRAMP) compliant cloud service provider (CSP). If an exception to this requirement is needed, it must be presented to and approved by the AHRQ CIO in writing. Additionally, the Contractor shall:

   i. Provide security for any Contractor systems, and information contained therein, connected to an AHRQ network or operated by the Contractor on behalf of AHRQ

regardless of location. In addition, if new or unanticipated threats or hazards are discovered by either the Agency or Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately, ***within one (1) hour or less***, bring the situation to the attention of the other party.

ii. Adopt and implement the policies, procedures, controls, and standards required by the HHS Information Security Program and the AHRQ Information Security and Privacy (IS&P) Program to ensure the confidentiality, integrity, and availability of government information and government information systems for which the Contractor is responsible under this contract or to which the Contractor may otherwise have access under this contract.

iii. Comply with the Privacy Act requirements and tailor FAR clauses as needed.

D. **Information Security Categorization.** In accordance with the Federal Information Processing Standards Publication (FIPS)199, *Standards for Security Categorization of Federal Information and Information Systems*, the Contractor (and/or any subcontractor) shall:

i. Protect government information and information systems in order to ensure:
- **Confidentiality**, which means preserving authorized restrictions on access and disclosure, based on the security terms found in this contract, including means for protecting personal privacy and proprietary information;
- **Integrity**, which means guarding against improper information modification or destruction, and ensuring information non-repudiation and authenticity; and
- **Availability**, which means ensuring timely and reliable access to and use of information.

ii. In accordance with FIPS 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, *Volume II: Guide for Mapping Types of Information and Information Systems to Security Categorie*s: *Appendices*, Appendix C, and based on information provided by the AHRQ Information Security and Privacy Team, Chief Information Security Officer (CISO), or other security representative, the risk level for each Security Objective and the Overall Risk Level, which is the highest watermark of the three factors (Confidentiality, Integrity, and Availability) of the information or information system are the following:

Confidentiality:	[x] Low [ ] Moderate [ ] High
Integrity:	[x] Low [ ] Moderate [ ] High
Availability:	[x] Low [ ] Moderate [ ] High
Overall Risk Level:	[x] Low [ ] Moderate [ ] High

Based on information provided by the AHRQ Information Security and Privacy Team, Privacy Office, system/data owner, or other security or privacy representative, it has been determined that this solicitation/contract involves:

[x] No PII [ ] Yes PII

Personally Identifiable Information (PII). Per Office of Management and Budget (OMB) Circular A-130, "PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Examples of PII include, but are not limited to the following: social security number, date and place of birth, mother's maiden name, biometric records, etc.

PII Confidentiality Impact Level has been determined to be: [x] Low [ ] Moderate [ ] High

E. **Protection of Sensitive Information.** For security purposes, information is *or* may be sensitive because it requires security to protect its confidentiality, integrity, and/or availability. The Contractor (and/or any subcontractor) shall protect all government information that is or may be sensitive in accordance with OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* by securing it with a FIPS 140-2 validated solution. For purposes of this contract, information is sensitive if the FIPS 199 Confidentiality or Integrity security objective is rated Moderate or High by the AHRQ Chief Information Officer (CIO) or CISO, as appropriate.

F. The Contractor shall ensure that sensitive information is not stored, processed, or transmitted on a publicly-available system (via the Internet) without the appropriate controls in place and specific authorization from the AHRQ CIO.

G. **Confidentiality and Nondisclosure of Information.** Any information provided to the Contractor (and/or any subcontractor) by AHRQ or collected by the Contractor on behalf of AHRQ shall be used only for the purpose of carrying out the provisions of this contract and shall not be disclosed or made known in any manner to any persons except as may be necessary in the performance of the contract. The Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its employees and subcontractors shall be under the supervision of the Contractor. Each Contractor employee or any of its subcontractors to whom any AHRQ records may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such employee or subcontractor can be used only for that purpose and to the extent authorized herein.

   The confidentiality, integrity, and availability of such information shall be protected in accordance with HHS and AHRQ policies. Unauthorized disclosure of information will be subject to the HHS/AHRQ sanction policies and/or governed by the following laws and regulations:

   i. 18 U.S.C. 641 (Criminal Code: Public Money, Property or Records);

   ii. 18 U.S.C. 1905 (Criminal Code: Disclosure of Confidential Information); and

iii. 44 U.S.C. Chapter 35, Subchapter I (Paperwork Reduction Act).

H. **Internet Protocol Version 6 (IPv6).** All procurements using Internet Protocol shall comply with OMB Memorandum M-05-22, *Transition Planning for Internet Protocol Version 6 (IPv6)*.

I. **Government Websites.** All new and existing public-facing government websites must be securely configured with Hypertext Transfer Protocol Secure (HTTPS) using the most recent version of Transport Layer Security (TLS). In addition, HTTPS shall enable HTTP Strict Transport Security (HSTS) to instruct compliant browsers to assume HTTPS at all times to reduce the number of insecure redirects and protect against attacks that attempt to downgrade connections to plain HTTP. For internal-facing websites, HTTPS is not required, but it is highly recommended.

Non-Repudiation. The Contractor shall provide a system that implements FIPS 140-2 validated encryption that provides for origin authentication, data integrity, and signer non-repudiation.

J. **Contract Documentation.** The Contractor shall use AHRQ provided templates, policies, forms and other agency documents to comply with contract deliverables as appropriate.

K. **Standard for Encryption.** The Contractor (and/or any subcontractor) shall:

i. Comply with the *HHS Standard for Encryption of Computing Devices and Information* to prevent unauthorized access to government information.

ii. Encrypt all sensitive federal data and information (i.e., PII, protected health information [PHI], proprietary information, etc.) in transit (i.e., email, network connections, etc.) and at rest (i.e., servers, storage devices, mobile devices, backup media, etc.) with FIPS 140-2 validated encryption solution.

iii. Secure all devices (i.e., desktops, laptops, mobile devices, etc.) that store and process government information and ensure devices meet HHS and AHRQ encryption requirements. Maintain a complete and current inventory of all laptop computers, desktop computers, and other mobile devices and portable media that store or process sensitive government information (including PII).

iv. Verify that the encryption solutions in use have been validated under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2. The Contractor shall provide a written copy of the validation documentation to the COR.

v. Use the Key Management system on the AHRQ personal identification verification (PIV) card, or establish and use a key recovery mechanism to ensure the ability of authorized personnel to encrypt/decrypt information and recover encryption keys. Encryption keys shall be provided to the COR upon request and at the conclusion of

the contract.

L. **Contractor Non-Disclosure Agreement (NDA).** Each Contractor (and/or any subcontractor) employee having access to non-public government information under this contract shall complete the HHS/AHRQ non-disclosure agreement(s) A copy of each signed and witnessed NDA shall be submitted to the CO and/or COR prior to performing any work under this acquisition.

N. **Privacy Impact Assessment (PIA).** If it is determined that a PIA is required, the Contractor shall assist the AHRQ SOP or designee with completing a PIA for the system or information within ***30 days*** from determination, and in accordance with HHS policy and OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*.

The Contractor shall assist the AHRQ SOP or designee in reviewing the PIA at least ***annually*** throughout the system development lifecycle (SDLC)/information lifecycle, or when determined by the Agency that a review is required based on a major change to the system, or when new types of PII are collected that introduce new or increased privacy risks, whichever comes first.

2. TRAINING

A. **Mandatory Training for All Contractor Staff.** All Contractor (and/or any subcontractor) employees assigned to work on this contract shall complete training consistent with the HHS/AHRQ Contractor Information Security Awareness, Privacy, and Records Management training (provided upon contract award) before performing any work under this contract. Thereafter, the employees shall complete AHRQ-specified Information Security Awareness, Privacy, and Records Management training at least ***annually***, during the life of this contract. All provided training shall be compliant with AHRQ training policies.

B. **Role-based Training.** All Contractor (and/or any subcontractor) employees with significant security responsibilities (as determined by the Program Manager and AHRQ CISO) must complete role-based training ***annually*** commensurate with their role and responsibilities in accordance with HHS/AHRQ policy and the *HHS Role-Based Training (RBT) of Personnel with Significant Security Responsibilities Memorandum*.

C. **Training Records.** The Contractor (and/or any subcontractor) shall maintain training records for all its employees working under this contract in accordance with HHS/AHRQ policy. A copy of the training records shall be provided to the CO and/or COR within ***30 days*** after contract award and ***annually*** thereafter or upon request.

3. RULES OF BEHAVIOR

A. The Contractor (and/or any subcontractor) shall ensure that all employees performing on the contract comply with a Rules of Behavior consistent with the *HHS Information Technology General Rules of Behavior* <to be provided after contract award>.

B. All Contractor employees performing on the contract must read and agree to adhere to the Rules of Behavior before accessing HHS/AHRQ data or other information, systems, and/or networks that store/process government information, initially at the beginning of the contract and at least ***annually*** thereafter. If requested, and if the training is provided by the Contractor, the signed ROB must be provided as a separate deliverable to the CO and/or COR per defined timelines above.

4. HIGH VALUE ASSET TESTING

If the information system is denoted as a High Value Asset (HVA), it must undergo yearly adversarial testing as required by FISMA. Adversarial testing is defined as "red team, penetration testing, or application testing." This testing is in addition to traditional NIST SP 800-53 based security assessment testing. Results of the annual HVA tests must be transmitted to the AHRQ Information Security and Privacy Program.

5. AHRQ FEDRAMP PRIVACY AND SECURITY REQUIREMENTS

The Contractor (and/or any subcontractor) shall be responsible for the following privacy and security requirements:

A. **FedRAMP Compliant ATO.** Comply with FedRAMP Security Assessment and Authorization (SA&A) requirements and ensure the information system/service under this contract has a valid FedRAMP compliant (approved) authority to operate (ATO) in accordance with Federal Information Processing Standard (FIPS) Publication 199 defined security categorization. If a FedRAMP compliant ATO has not been granted, the Contractor shall submit a plan to obtain a FedRAMP compliant ATO prior to going live or hosting AHRQ data.

   i. Implement applicable FedRAMP baseline controls commensurate with the agency-defined security categorization and the applicable FedRAMP security control baseline (www.FedRAMP.gov). The *HHS Information Security and Privacy Policy (IS2P)* and *HHS Cloud Computing and Federal Risk and Authorization Management Program (FedRAMP) Guidance* further define the baseline policies as well as roles and responsibilities. The Contractor shall also implement a set of additional controls identified by the agency when applicable.

B. **Data Jurisdiction.** The Contractor shall store all information within the security authorization boundary, data at rest or data backup, within the continental United States (CONUS) if so required.

C. **Service Level Agreements.** When applicable, the Contractor shall understand the terms of the service agreements that define the legal relationships between cloud customers and cloud providers and work with AHRQ to develop and maintain an SLA.

D. **Interconnection Agreements/Memorandum of Agreements.** When applicable, the Contractor shall establish and maintain Interconnection Agreements and or Memorandum

of Agreements/Understanding in accordance with HHS/AHRQ policies.

6. PROTECTION OF INFORMATION IN A CLOUD ENVIRONMENT

A. If Contractor (and/or any subcontractor) personnel must remove any information from the primary work area, they shall protect it to the same extent they would the proprietary data and/or company trade secrets and in accordance with HHS/AHRQ policies.

B. HHS/AHRQ will retain unrestricted rights to federal data handled under this contract. Specifically, HHS/AHRQ retains ownership of any user created/loaded data and applications collected, maintained, used, or operated on behalf of HHS/AHRQ and hosted on Contractor's infrastructure, as well as maintains the right to request full copies of these at any time. If requested, data must be available to HHS within ***one (1) business day*** from request date or within the timeframe specified otherwise. In addition, the data shall be provided at no additional cost to HHS/AHRQ.

C. The Contractor (and/or any subcontractor) shall ensure that the facilities that house the network infrastructure are physically and logically secure in accordance with FedRAMP requirements and HHS policies.

D. The Contractor shall support a system of records in accordance with NARA-approved records schedule(s) and protection requirements for federal agencies to manage their electronic records in accordance with 36 CFR § 1236.20 & 1236.22 (ref. a), including but not limited to the following:

   i. Maintenance of links between records and metadata; and

   ii. Categorization of records to manage retention and disposal, either through transfer of permanent records to NARA or deletion of temporary records in accordance with NARA-approved retention schedules.

E. The disposition of all HHS/AHRQ data shall be at the written direction of HHS/AHRQ. This may include documents returned to HHS/AHRQ control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

F. If the system involves the design, development, or operation of a system of records on individuals, the Contractor shall comply with the Privacy Act requirements.

7. SECURITY ASSESSMENT AND AUTHORIZATION (SA&A)

A. The Contractor (and/or any subcontractor) shall comply with HHS/AHRQ and FedRAMP requirements as mandated by federal laws, regulations, and HHS/AHRQ policies, including making available any documentation, physical access, and logical access needed to support the SA&A requirement. The level of effort for the SA&A is based on the system's FIPS 199 security categorization and HHS/*AHRQ* security policies.

i. In addition to the FedRAMP compliant ATO, the Contractor shall complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service implementation. The agency ATO must be approved by the AHRQ authorizing official (AO) prior to implementation of system and/or service being acquired.

ii. CSP systems categorized as Federal Information Processing Standards (FIPS) 199 high must leverage a FedRAMP accredited third-party assessment organization (3PAO); moderate impact CSP systems must make a best effort to use a FedRAMP accredited 3PAO. CSP systems categorized as FIPS 199 low impact may leverage a non-accredited, independent assessor.

iii. For all acquired cloud services, the SA&A package must contain the following documentation. Following the initial ATO, the Contractor must review and maintain the ATO in accordance with HHS/AHRQ policies. Work with the AHRQ Information Security and Privacy team to determine if FedRAMP templates *(http://www.fedramp.gov/)* or AHRQ templates should be used.

B. SA&A Package Deliverables – The Contractor (and/or any subcontractor) shall provide an SA&A package prior to going live or hosting AHRQ data to the CO and/or COR. The following SA&A deliverables are required to complete the SA&A package:

- **System Security Plan (SSP)** – due prior to going live or hosting AHRQ data. The SSP shall comply with the NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, the Federal Information Processing Standard (FIPS) 200, *Recommended Security Controls for Federal Information Systems*, and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* applicable baseline requirements, other NIST guidance, and HHS/AHRQ policies as applicable. The SSP shall be consistent with and detail the approach to IT security contained in the Contractor's bid or proposal that resulted in the award of this contract. The SSP shall provide an overview of the system environment and security requirements to protect the information system as well as describe all applicable security controls in place or planned for meeting those requirements. It should provide a structured process for planning adequate, cost-effective security protection for a system. The Contractor shall update the SSP at least ***annually*** thereafter.

- **Security Assessment Plan/Report (SAP/SAR)** – due prior to going live or hosting AHRQ data. The security assessment shall be conducted by an independent assessor and be consistent with NIST SP 800-53A, NIST SP 800-30, and HHS/AHRQ policies. The assessor will document the assessment results in the required SAR template.

  Thereafter, the Contractor, in coordination with AHRQ shall conduct and/or assist in the assessment of the security controls and update the SAR at least ***annually***.

- **Independent Assessment –** due prior to going live or hosting AHRQ data. The Contractor (and/or subcontractor) shall have an independent third-party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA&A package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800-53. The Contractor shall address all "*very high"* and *"high"* deficiencies before submitting the package to the Government for acceptance. All remaining deficiencies must be documented in a system Plan of Actions and Milestones (POA&M).

- **POA&M** – due prior to going live or hosting AHRQ data. The POA&M shall comply with the *HHS Standard for Plan of Action and Milestones* and related AHRQ policies.

  All vulnerabilities and other risk findings shall be remediated by the prescribed timelines from discovery:

  - **Critical findings within 15 days**
  - **High findings within 30 days**
  - **Moderate findings within 90 days**
  - **Low findings within 365 days**

  AHRQ will determine the risk rating of vulnerabilities.

  Identified risks stemming from deficiencies related to the security control baseline implementation, assessment, continuous monitoring, vulnerability scanning, and other security reviews and sources, as documented in the SAR, shall be documented and tracked by the Contractor for mitigation in the POA&M document. Depending on the severity of the risks, AHRQ may require designated POA&M weaknesses to be remediated before an ATO is issued. Thereafter, the POA&M shall be updated at least ***quarterly***.

- **Reporting POA&M**
  All weaknesses requiring corrective action and their mitigation status must be reported to HHS/AHRQ on a periodic basis. HHS will in turn report to OMB and other federal entities as mandated.

  HHS Requirements

  The HHS Security Data Warehouse Escalation Memorandum[1] requires OpDivs to submit periodic POA&M updates to HHS Security Data Warehouse (HSDW), the Department's authoritative source for all system security-related data. All OpDivs must submit POA&M updates to HSDW at least monthly (by the 3rd business day of each month) or when requested by the Department to demonstrate

[1] HHS Security Data Warehouse Escalation Memorandum, July 2013, https://intranet.hhs.gov/policy/data-warehouse-escalation.

the status of weakness mitigation activities. OpDivs should maintain all documentation supporting findings and weaknesses and make those available in a timely manner.

Specifically, OpDivs are required to submit the following information in accordance with the Department POA&M reporting requirements:

- All weaknesses associated with a program or system.
- All weaknesses associated with a system that is authorized within a boundary. These weaknesses should be tied to the system and not the authorization boundary.
- Closed weaknesses for up to one year from the date of closure.

- **Contingency Plan and Contingency Plan Test** – due prior to going live or hosting AHRQ data. The Contingency Plan must be developed in accordance with NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, and be consistent with HHS and AHRQ policies. Upon acceptance by the System Owner and the AHRQ Information Security and Privacy Program, the Contractor, in coordination with the System Owner, shall test the Contingency Plan and prepare a Contingency Plan Test Report that includes the test results, lessons learned, and any action items for address. Thereafter, the Contractor shall update and test the Contingency Plan at least ***annually***.

- **E-Authentication Questionnaire** – due prior to going live or hosting AHRQ data. The Contractor (and/or any subcontractor) shall collaborate with government personnel to ensure that an E-Authentication Threshold Analysis (ETA) is completed to determine if a full E-Authentication Risk Assessment (ERA) is necessary. System documentation developed for a system using ETA/ERA methods shall follow OMB 04-04 and NIST SP 800-63, Rev. 2, *Electronic Authentication Guidelines*.

  Based on the level of assurance determined by the ETA/ERA, the Contractor (and/or subcontractor) must ensure appropriate authentication to the system, including remote authentication, is in-place in accordance with the assurance level determined by the ETA/ERA in accordance with HHS/AHRQ policies.

C. AHRQ reserves the right to perform penetration testing (pen testing) on all systems operated on behalf of agency. If AHRQ exercises this right, the Contractor (and/or any subcontractor) shall allow AHRQ employees (and/or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with AHRQ 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. The Contractor must identify any gaps between required FedRAMP Security Control Baseline/Continuous Monitoring controls and the Contractor's implementation status as documented in the Security Assessment Report and related Continuous Monitoring artifacts. In addition, all gaps shall be documented and tracked by the Contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, AHRQ may require remediation at the Contractor's expense, before AHRQ issues an ATO.

E. The Contractor (and/or any subcontractor) shall mitigate security risks for which they are responsible, including those identified during SA&A and continuous monitoring activities. All vulnerabilities and other risk findings shall be remediated by the prescribed timelines from discovery:

- **Critical findings within 15 days**
- **High findings within 30 days**
- **Moderate findings within 90 days**
- **Low findings within 365 days**

In the event a vulnerability or other risk finding cannot be mitigated within the prescribed timelines above, they shall be added to the designated POA&M and mitigated within the newly designated timelines determined in accordance with the AHRQ Information Security and Privacy Team and approved by the CISO. AHRQ will determine the risk rating of vulnerabilities using FedRAMP baselines.

F. **Revocation of a Cloud Service**. HHS/AHRQ have the right to take action in response to the CSP's lack of compliance and/or increased level of risk. In the event the CSP fails to meet HHS and FedRAMP security and privacy requirements and/or there is an incident involving sensitive information, HHS and/or AHRQ may suspend or revoke an existing agency ATO (either in part or in whole) and/or cease operations. If an ATO is suspended or revoked in accordance with this provision, the CO and/or COR may direct the CSP to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

7. REPORTING AND CONTINUOUS MONITORING

A. As applicable, following the initial ATOs, the Contractor (and/or any subcontractor) must perform the minimum ongoing continuous monitoring activities specified below, submit required deliverables by the specified due dates, and meet with the system/service owner and other relevant stakeholders to discuss the ongoing continuous monitoring activities, findings, and other relevant matters. The CSP will work with the agency to schedule ongoing continuous monitoring activities.

B. At a minimum, the Contractor must provide the following artifacts/deliverables on a ***monthly*** basis*:*

i. Operating system, database, Web application, and network vulnerability scan results;

ii. Updated POA&Ms;

iii. Any updated authorization package documentation as required by the annual attestation/assessment/review or as requested by the AHRQ System Owner or Authorizing Official (AO); and

iv. Any configuration changes to the system and/or system components or CSP's cloud environment that may impact HHS/AHRQ's security posture. Changes to the configuration of the system, its components, or environment that may impact the security posture of the system under this contract must be approved by the Agency.

C. User Account Reviews - Perform oversight systems to ensure that (1) periodic user access reviews are performed and that (2) privileged user account activities are logged and periodically reviewed. A user is defined as any non-public person with an account used to access or administer an AHRQ information system. **Twice a year** (in January and June), submit evidence of user and privileged user account reviews as described below:

(1) User Access Reviews must be conducted at least *twice a year* for all system users. Each user account must be examined to determine if (a) the user account is still in use and necessary, and (b) the level of access is commensurate with the user's job responsibilities.
(2) Privileged User Account Activities Reviews must be conducted *monthly*. The activities of privileged users must be logged and reviewed.

Evidence of these reviews must be submitted using a spreadsheet which is organized with one tab for each type of review:

(1) The User Access Reviews must consist of a list of all users and the result of the review.
    a. the account is still needed (Yes/No)
    b. the account has the correct level of access (Yes/No)
    c. appropriate changes/updates were made (Yes/NA)
    d. date of review
(2) The Privileged User Account Activities Reviews must consist of a list of each privileged user and the result of the review
    a. the account activities were reviewed (Yes/No)
    b. date of review

FedRAMP deliverables shall be labeled according to the Contractor selected designation per document sensitivity and in conjunction with the AHRQ CISO. External transmission/dissemination of "For Official Use Only" (FOUO) information to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*.

8. CONFIGURATION BASELINE

A. The Contractor (and/or any subcontractor) shall certify that applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB), Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), Center for Information Security (CIS) Security Benchmarks or any other HHS-identified configuration baseline. The standard installation, operation, maintenance, updates, and/or patching of software shall not alter the configuration settings from the approved HHS/AHRQ configuration baseline.

B. The Contractor (and/or any subcontractor) shall use Tenable Nessus with configuration baseline scanner capabilities to certify their products operate correctly with HHS/AHRQ and NIST defined configurations and do not alter these settings.

C. The contractor shall ensure that administrator user internet access is restricted to only a select set of whitelisted sites that have been pre-approved. This requirement is intended to minimize the risk of administrators accidently accessing malicious sites that could result in system compromise.

9. ZERO TRUST ARCHITECTURE

Where applicable, the contractor shall design and implement IT solutions and systems in accordance with the five pillars of Zero Trust Architecture as defined in OMB M-22-09. Specifically, any contractor developed, or hosted system shall implement the following the ZTA best practices. Note that these requirements apply only to the environment that stores, processes, or transmits AHRQ data:

A. **Identity:** Contractors must design and implement systems that use enterprise-managed identities to access the applications they use in their work. Phishing-resistant MFA protects those personnel from sophisticated online attacks. Specifically:

i. Contractors must integrate and enforce MFA across AHRQ applications involving authenticated access to Federal systems by agency staff, contractors, and partners.
ii. MFA shall be integrated at the application layer, such as through an enterprise identity service as described above, rather than through network authentication (e.g., a virtual private network).
iii. Contractors must require their users to use a phishing-resistant method to access AHRQ accounts and systems. For routine self-service access by agency staff, contractors, and partners, contractors must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications.
iv. Contractors are encouraged to pursue greater use of passwordless multi-factor authentication as they modernize their authentication systems. However, when passwords are in use, they are a “factor” in multi-factor authentication. If outdated password requirements lead users to reuse passwords from their personal life, store

passwords insecurely, or otherwise use weak passwords, adversaries will find it much easier to obtain unauthorized account access—even within a system that uses MFA.

v. Consistent with the practices outlined in SP 800-63B, contractor systems must remove password policies that require special characters and regular password rotation. These requirements have long been known to lead to weaker passwords in real-world use and must not be employed.

vi. Public-facing AHRQ systems that support MFA must give users the option of using phishing-resistant authentication. Meeting this requirement for the general public will mean providing support for Web Authentication-based approaches, such as security keys. Contractors may also offer support for authentication using PIV and CAC credentials for agency staff and contractors who are accessing public-facing systems in their personal capacity.

vii. Contractors shall ensure their tools can execute certain protocols for authorization. Authorization, a critical aspect of zero trust architecture, is the process of granting an authenticated entity access to resources. Authentication helps ensure that the user accessing a system is who they claim to be; authorization determines what that user has permission to do.

viii. Currently, many authorization models in the Federal Government focus on role-based access control (RBAC), which relies on static pre-defined roles that are assigned to users and determine their permissions within an organization. A zero-trust architecture must incorporate more granularly and dynamically defined permissions, as attribute-based access control (ABAC) is designed to do.

B. **Devices:** Contractors must maintain an inventory of every device it operates and authorizes for Government use, and can prevent, detect, and respond to incidents on those devices. Specifically:

i. Contractors must create reliable asset inventories.

ii. Contractors must ensure their Endpoint Detection and Response (EDR) tools meet CISA's technical requirements and are deployed widely.

C. **Networks:** Contractors must encrypt all DNS requests and HTTP traffic within their environment and execute a plan to break down their perimeters into isolated environments. Specifically:

i. Contractors must resolve DNS queries using encrypted DNS wherever it is technically supported.

ii. Contractors must enforce HTTPS for all web and application program interface (API) traffic in their environment.

iii. Contractors shall avoid relying on static cryptographic keys with an overly broad ability to decrypt enterprise-wide traffic, as even a brief compromise of such a key would defeat encryption across an enterprise. Contractors must make heavy internal use of recent versions of standard encryption protocols, such as TLS 1.3, that are designed to resist bulk decryption. More generally, contractors must plan for cryptographic agility in their network architectures, in anticipation of continuing to

adopt newer versions of TLS and other baseline encryption protocols.

iv. Contractors must adjust their DNS architecture and associated monitoring to move closer to a zero-trust architecture.

v. If contractors use custom-developed software to initiate DNS requests, they must implement support for encrypted DNS. Contractors explicitly configure endpoints to use contractor-designated encrypted DNS servers, rather than relying on automatic network discovery.

D. **Applications and Workloads:** Contractors must treat all applications as internet-connected, routinely subject their applications to rigorous empirical testing, and welcome external vulnerability reports. Specifically:

i. Contractors must operate dedicated application security testing programs.

ii. Contractors must utilize high-quality firms specializing in application security for independent third-party evaluation.

iii. Contractors must provide any non-.gov hostnames they use to AHRQ

iv. Contractors must work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure.

E. **Data:** Contractors must deploy protections that make use of thorough data categorization. As applicable, contractors may take advantage of cloud security services to monitor access to their sensitive data and have implemented enterprise-wide logging and information sharing. Specifically:

i. Contractors must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.

ii. Contractors must audit access to any data encrypted at rest in commercial cloud infrastructure.

iii. Contractors must implement comprehensive logging and information sharing capabilities, as described in OMB Memorandum M-21-31.

AHRQ cannot prescribe specific technologies, solutions, or architecture best practices to enable compliance with these requirements. Contractors must read OMB M-22-09 and implement ZTA controls and solutions that are commensurate with the risk level of the system.

10. PRIVACY ACT

Records are subject to the Privacy Act of 1974 (5 U.S.C. 552a) if they constitute a "system of records," which is defined in the Privacy Act as records about individuals maintained in a system from which they are retrieved by name or other personal identifier. If it is determined that this contract is subject to the Privacy Act of 1974 because the contract provides for the design, development, or operation of a system of records on individuals, then the Contractor must work in coordination with the AHRQ Senior Official for Privacy (SOP) to determine applicable System of Record Notice (SORN), if applicable, disposition to be made of the Privacy Act records upon completion of the contract performance, etc.

11. END OF LIFE COMPLIANCE

The Contractor (and/or any subcontractor) must use Commercial Off the Shelf (COTS) software or other software that is supported by the manufacturer. In addition, the COTS/other software need to be within one major version of the current version; deviation from this requirement will only be allowed via the AHRQ waiver/risk based decision process (approved by AHRQ CISO). The Contractor shall retire and/or upgrade all software/systems that have reached end-of-life in accordance with the *AHRQ Information Security and Privacy Policy/Management Operations Manual Instruction* and *HHS End-of-Life Operating Systems, Software, and Applications Policy*.

12. DESKTOPS, LAPTOPS, AND OTHER COMPUTING DEVICES REQUIRED FOR USE BY THE CONTRACTOR

The Contractor (and/or any subcontractor) shall ensure that all IT equipment (e.g., laptops, desktops, servers, routers, mobile devices, peripheral devices, etc.) used to process information on behalf of AHRQ are deployed and operated in accordance with approved security configurations and meet the following minimum requirements:

i. Encrypt equipment and sensitive information stored and/or processed by such equipment in accordance with HHS, AHRQ, and FIPS 140-2 encryption standards;

ii. Configure laptops and desktops in accordance with the latest applicable United States Government Configuration Baseline (USGCB) and *HHS Minimum Security Configuration Standards*;

iii. Maintain the latest operating system patch release and anti-virus software definitions at least ***monthly***;

iv. Validate the configuration settings after hardware and software installation, operation, maintenance, update, and patching, and ensure changes in hardware and software do not alter the approved configuration settings; and

v. Automate configuration settings and configuration management in accordance with HHS and AHRQ security policies, including but not limited to:

- Configuring systems to allow for periodic AHRQ vulnerability and security configuration assessment scanning; and

- Using Tenable Nessus with USGCB scanner capabilities to scan systems at least ***monthly*** and report the results of these scans to the CO and/or COR, Program Manager, and any other applicable designated POC.

12. INCIDENT REPORTING

The Agency and the Contractor shall review the applicable customer responsibility matrix for the requisite system/service and determine incident response requirements. Dependent on specific

customer responsibility matrices, the Contractor (and/or any subcontractor) shall meet the following requirements:

A. The Contractor (and/or any subcontractor) shall provide an Incident and Breach Response Plan (IRP) in accordance with HHS/AHRQ, OMB, and US-CERT requirements, and obtain approval from AHRQ. In addition, the Contractor must follow the incident response and US-CERT reporting guidance contained in the HHS cybersecurity policies intranet page <to be provided after contract award>.

B. The Contractor (and/or any subcontractor) must implement a program of inspection to safeguard against threats and hazards to the security, confidentiality, integrity, and availability of federal data, afford HHS/AHRQ access to its 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. Where applicable, conduct authenticated and unauthenticated operating system/network/database/Web application vulnerability scans. Automated scans can be performed by HHS/AHRQ personnel, or agents acting on behalf of HHS/AHRQ, using agency-operated equipment and/or specified tools. The Contractor may choose to run its own automated scans or audits, provided the scanning tool used is Tenable Nessus or a waiver for another tool has been approved by the Agency. The Agency may request the Contractor's scanning results and, at the Agency discretion, accept those in lieu of Agency performed vulnerability scans.

   ii. In the event an incident involving sensitive information occurs, the Contractor must cooperate on all required activities determined by the Agency to ensure an effective incident or breach response, and provide all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents. In addition, the Contractor must follow the Agency reporting procedures and document the steps it takes to contain and eradicate the incident, recover from the incident, and provide a post-incident report that includes, at a minimum, the following:

      - Company and point of contact name;
      - Contract information;
      - Impact classifications/threat vector;
      - Type of information compromised;
      - A summary of lessons learned; and
      - Explanation of the mitigation steps of exploited vulnerabilities to prevent similar incidents in the future.

13. MEDIA TRANSPORT

A. The Contractor (and/or any subcontractor) shall be accountable for and document all activities associated with the transport of government information, devices, and media outside controlled areas and/or facilities. This includes information stored on digital and non-digital media (e.g., CD-ROM, tapes, etc.), and mobile/portable devices (e.g., USB

flash drives, external hard drives, SD cards, etc.). In accordance with the *AHRQ Information Security and Privacy Policy/AHRQ Management Operations Manual Instruction*, the following actions are required (for FIPS 199 Moderate and High AHRQ systems only):

i. System media must be protected and controlled during transport outside of controlled areas using encryption (in the case of sensitive information), or security safeguards that are commensurate with the system's FIPS 199 security categorizations for confidentiality and integrity.
   a. FIPS 140-2 validated encryption technologies must be employed on all media that stores sensitive information.
   b. All media transported by mail or courier/messenger service must be double sealed. The second envelope must be marked appropriately and labeled to indicate the sensitivity level of the information it contains.

ii. All media used to support backup and disaster recovery operations must be stored off-site at a secured location. All media must be transported securely to an off-site location that has been established in accordance with applicable contingency planning procedures.

iii. Accountability for system media must be maintained during transport outside of controlled areas.
   a. Audit trails must be established to track all deposits and withdrawals from media storage facilities and/or libraries. Audit trails must provide an accurate record of the media chain of custody and hold users accountable for the information removed from storage.
   b. The delivery and receipt of all media must be monitored and accounted for to ensure data is not lost and/or compromised while in transit.

iv. Procedures for, and activities associated with transport, must be documented.

v. Transport must be restricted to authorized personnel.

B. All information, devices and media must be encrypted with HHS/AHRQ-approved encryption mechanisms to protect the confidentiality, integrity, and availability of all government information transported outside of controlled facilities.

15. PERSONNEL SECURITY RESPONSIBILITIES

A. The Contractor, within ***seven (7) days*** after contract award (before an employee begins working on this contract), shall provide the CO and/or COR the name, position title, e-mail address, and phone number of all staff proposed to work under the contract. This is in coordination with the information provided above regarding position sensitivity levels/background investigations.

B. The Contractor (and/or any subcontractor) shall perform and document the actions identified in the HHS/AHRQ Contractor Employee Separation Form <to be provided after

contract award> when an employee terminates work under this contract within ***seven (7) days*** of the employee's exit from the contract. All documentation shall be made available to the CO and/or COR upon request.

C. The Contractor shall ensure all access and privileges to AHRQ systems, network, and facilities are suspended/terminated when employees or contractors temporarily or permanently separate from the Contractor organization (e.g., termination, resignation, leave of absence) or are reassigned within the organization. All AHRQ-owned IT resources shall be returned to the appropriate personnel upon separation or reassignment. The Contractor shall ensure that users who resign or are terminated properly dispose of all AHRQ information in electronic and hard copy formats. The Contractor shall also ensure appropriate personnel have access to records created by the separated or reassigned employee.

16. CONTRACT INITIATION AND EXPIRATION

A. **General Security Requirements.** The Contractor (and/or any subcontractor) shall comply with information security and privacy requirements, Enterprise Performance Life Cycle (EPLC) processes, and HHS Enterprise Architecture requirements to ensure information is appropriately protected from initiation to expiration of the contract. All information system development or enhancement tasks supported by the Contractor shall follow the HHS EPLC framework and methodology, and in accordance with the HHS Contract Closeout Guide (2012) <to be provided after contract award>.

B. **System Documentation.** Contractors (and/or any subcontractors) must follow and adhere to NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, at a minimum, for system development activities and provide system documentation at designated intervals (specifically, at the expiration of the contract) within the EPLC that require artifact review and approval.

C. **Sanitization of Government Files and Information.** As part of contract closeout and at expiration of the contract, the Contractor (and/or any subcontractor) shall provide all required documentation to the CO and/or COR to certify that, at the government's direction, all electronic and paper records are appropriately disposed of and all devices and media are sanitized in accordance with NIST SP 800-88, *Guidelines for Media Sanitization*.

D. **Notification.** The Contractor (and/or any subcontractor) shall notify the CO and/or COR and AHRQ Information Security and Privacy Team within ***seven (7) days*** of when an employee stops working under this contract.

E. **Contractor Responsibilities Upon Physical Completion of the Contract.** The Contractor (and/or any subcontractors) shall return all government information and IT resources (i.e., government information in non-government-owned systems, media, and backup systems) acquired during the term of this contract to the CO and/or COR within ***14 days*** of contract end. Additionally, the Contractor shall provide a certification that all government information has been properly sanitized and purged from Contractor-owned systems,

including backup systems and media used during contract performance, in accordance with HHS and/or AHRQ policies.

17. HARDWARE PROCUREMENTS

Mobile Devices. The Contractor shall follow NIST 800-124, Rev. 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise* when using mobile devices that process or store HHS/AHRQ data.

18. NON-COMMERCIAL AND OPEN SOURCE COMPUTER SOFTWARE PROCUREMENTS

Noncommercial computer software is defined as software that does not qualify as commercial in nature (e.g., commercial items and commercial off the shelf [COTS] items as defined in FAR 2.101).

The Contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by the United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), which will limit system software vulnerability exploits.

19. INFORMATION TECHNOLOGY APPLICATION DESIGN, DEVELOPMENT, OR SUPPORT

This section refers to procurements including application design, development, or support. For the purposes of this document, "Computer software" means:

a. Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

b. Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

"Computer software" does not include computer databases or computer software documentation.

1) The Contractor (and/or any subcontractor) shall ensure IT applications designed and developed for end users (including mobile applications and software licenses) run in the standard user context without requiring elevated administrative privileges.

2) The Contractor (and/or any subcontractor) shall follow secure coding best practice requirements, as directed by United States Computer Emergency Readiness Team (US-CERT) specified standards and the Open Web Application Security Project (OWASP), which will limit system software vulnerability exploits.

3) The Contractor (and/or any subcontractor) shall ensure that computer software developed on behalf of HHS or tailored from an open-source product is fully functional

and operates correctly on systems configured in accordance with government policy and federal configuration standards. The Contractor shall test applicable products and versions with all relevant and current updates and patches updated prior to installing in the HHS/AHRQ environment. No sensitive data shall be used during software testing.

4) The Contractor (and/or any subcontractor) shall protect information that is deemed sensitive from unauthorized disclosure to persons, organizations, or subcontractors who do not have a need to know the information. Information which, either alone or when compared with other reasonably-available information, is deemed sensitive or proprietary by HHS/AHRQ shall be protected as instructed in accordance with the magnitude of the loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. This language also applies to all subcontractors that are performing under this contract.

STOP COPYING LANGUAGE HERE