ADDITIONAL INFORMATION SECURITY AND PRIVACY REQUIREMENTS FOR CLOUD-BASED SOLUTIONS

NOTE: When the Contractor's proposed solution involves or may involve the use of cloud technology, the Contractor must also comply with all of the following information security and privacy requirements.

1. **FEDRAMP Authorization Requirements**. The Contractor shall comply with FedRAMP SA&A requirements and ensure the information systems and services under this contract have a valid FedRAMP compliant (approved) Authority To Operate (ATO) in accordance with FIPS Publication 199 defined security categorization at the time of contract. If the cloud service product is not listed in the FedRAMP Marketplace (https://marketplace.fedramp.gov/#/products) with a "FedRAMP Authorized" status, the Contractor shall submit a plan to obtain a FedRAMP approved ATO (60) days prior to contract award.

2. **Compliance.** In the event the Cloud Service Provider (CSP) fails to meet both SSA and FedRAMP security and privacy requirements or there is an incident involving confidential information, SSA may suspend or revoke an existing agency ATO (either in part or in whole) and cease operations. If SSA suspends or revokes an agency ATO in accordance with this provision, the CO or COR may direct the CSP to take additional security measures to secure confidential information. These measures may include restricting access to confidential information on the Contractor information system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the confidential information from the Internet or other networks or applying additional security controls.

3. **SSA Authorization Requirements.** The Contractor shall:

    a. In addition to the FedRAMP compliant ATO, upon SSA's request, complete and maintain an agency SA&A package to obtain agency ATO prior to system deployment/service. The SSA authorizing official must approve the agency ATO prior to implementation of the system or acquisition of the service

    b. 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, the Contractor shall document and track all gaps for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the risks, SSA may require remediation at the Contractor's expense, before SSA issues an ATO.

4. **Physical Access Records.** The Contractor shall record all physical access to the cloud storage facilities and all logical access to the federal information as specified in

the contract. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the CO or designee in accordance with the contract or upon request to comply with federal authorities.

5. **Availability.** The Contractor shall inform the COR of any interruption in the availability of the cloud service as required by the service level agreement. Whenever there is an interruption in service, the Contractor shall inform the COR of the estimated time that the system or data will be unavailable. The estimated timeframe for recovery of the service must be related to the FIPS 199 system categorization for the availability of the system and if specified, agreed upon service level agreements (SLA) and system availability requirements. The Contractor must provide regular updates, at intervals specified by the COR, to the COR on the status of returning the service to an operating state according to the agreed upon SLAs and system availability requirements.

6. **Continued Compatibility.** The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with the agency's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing notification, **within 1 hour of discovery**, to the COR and shall be responsible for working with the agency to identify appropriate remedies and if applicable, work with the agency to facilitate a smooth and seamless transition to an alternative solution and/or provider.

7. **Service Level Agreement (SLA).** The Contractor shall understand any applicable terms of the service agreements that define the legal relationships between cloud customers and cloud providers and shall work with SSA to develop and maintain a Service Level Agreement.

8. **Notification Banners.** The Contractor shall display The Standard Mandatory Notice and Consent Banner at log on to all information systems. Choose either banner "a" or "b" based on the character limitations imposed by the system. The formatting of these documents, to include the exact spacing between paragraphs, must be maintained. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."

    a. Banner for desktops, laptops, and other devices accommodating banners of 1300 characters.

    You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

    By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

OK

b. For devices with severe character limitations:

I've read & consent to terms in IS user agreem't.

9. **Facility Inspections.** The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by the agency conduct a security audit based on the agency's criteria at least once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with the COR within 20 days of the Contractor's receipt of the audit results. In addition, the agency reserves the right to inspect the facility to conduct its own audit or investigation.

10. **Cloud Security Governance**. The Contractor shall:

a. Ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Modernization Act) 44 U.S.C. § 3541, et seq.), NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60. In addition, the Contractor must provide the CO with any documentation it requires for its reporting requirements within 10 days of a request.

b. Make the environment accessible for an agency security team to evaluate the environment prior to the placement of any federal information in the environment and allow for periodic security reviews of the environment

during the performance of this contract. The Contractor shall also make appropriate personnel available for interviews and provide all necessary documentation during these reviews.

11. **Maintenance.** The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement to proactively prevent the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the Contractor's PVM systems and programs apply standardized configurations with automated continuous monitoring to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained to assure all software products deployed in the Contractor's operating environment and serving the agency are compatible with existing systems and architecture of the agency.

12. **Continuous Monitoring.** The Contractor shall provide all reports required to be completed; including self- assessments required by the FedRAMP Continuous Monitoring Strategy Guide to the COR. In addition, the agency may request additional reports based on data required to be collected by FedRAMP's continuous monitoring requirements. If requested, the Contractor will provide the report to the agency within 10 business days.

13. **Penetration Testing.** The SSA reserves the right to perform penetration testing on Contractor's systems, facilities, or cloud services used by the Contractor to deliver services to the SSA. If the agency exercises this right, the Contractor shall allow agency employees (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), Intrusion Detection System/Intrusion Prevention System, databases, and other applicable systems (including general support structure that support the processing, transportation, storage, or security of SSA confidential information for vulnerabilities).

14. **Risk Remediation.** In the event the Contractor cannot mitigate a vulnerability or other risk finding within the prescribed timelines above, and upon agreement with the CO they shall be added by the Contractor to the designated POA&M and mitigated within the agreed upon timelines. SSA will determine the risk rating of vulnerabilities using FedRAMP baselines.