Addendum B

INFORMATION SECURITY REQUIREMENTS

1. Contractor must have a mature Information Security ("**IS**") program that is consistent with an industry recognized framework, such as ISO 27001, COBIT, NIST, etc. When applicable, Contractor will comply with the PCI DSS standards. Confidential Information should be handled and processed by Contractor in accordance with the applicable information security framework(s), in addition to any other requirements specifically set forth in the Agreement. Key security controls that the State expects to exist as part of a mature IS program include, but are not limited to the following:

    a. Contractor shall maintain an IS office or function, with staff designated to maintain Contractor's IS program and to perform IS risk management.
    b. Contractor's IS policies and standards must be reviewed and assessed for relevance on a periodic but regular basis and updated as appropriate.
    c. All Contractor personnel or contract resources with access to sensitive data supplied by or in support of the State are expected to have removable media controls in place to guard against lost or stolen devices. Types of removable media include but are not limited to: CD/DVD, USB flash drives, smart phones, portable hard drives, and solid-state drives (i.e., electronic media with no mechanic parts).
    d. Contractor will follow industry standards, including those pertaining to encryption, when transmitting or transporting *the Confidential Information.*
    e. *Contractor* will use hard drive encryption on all laptops on which the Confidential Information is stored and/or accessed by Contractor personnel. Contractor shall utilize commercially reasonable encryption methods in accordance with industry best practices.
    f. For applications hosted on behalf of the State, Contractor is expected to implement either "two factor authentication" or have the capability to configure the password complexity and configuration of authentication to meet the State' policy requirements.
    g. Contractor is expected to perform periodic (at least annually) user access and entitlement reviews of all application and privileged accounts on systems and infrastructure that support the State organization.

2. Contractor shall complete and return to the State within thirty (30) calendar days of receipt, a Third-Party Assurance (TPA) Questionnaire. The TPA Questionnaire will be furnished by the State and/or a State representative during the term of this Agreement. Control deficiencies identified as a result of this effort will be corrected or otherwise mitigated. Contractor and the State

representatives will collaborate in good faith to address identified control deficiencies within a reasonable schedule.

3. Contractor shall maintain access and usage logs consistent with industry standards, which shall be made available for inspection if required for regulatory purposes or as a result of a security Incident that impacts the State.

4. Contractor is expected to have a third-party assurance program to validate the IS control environment of its third-party vendors/service providers) and ensure they have a comparable IS program to protect the Confidential Information in accordance with the expectations outlined in this Agreement.

5. The State must agree in writing via a Change Control Document or similar instrument to any change of country location from where Services are being provided in order to validate that the State's IS control expectations are being met. Contractor must allow the State a one hundred eighty (180) day timeframe to assess the risk and perform an on-site visit (if necessary) to validate the maturity of the control environment of the new location as well as any country specific risks introduced by the location change, provided the State will not have physical access to Cloud Services hardware.

6. All internet-facing systems servicing the State or its customers or employees (or their respective customers or employees) must be protected in a layered (defense in depth) network security architecture, including but not limited to the use of current virus definitions, firewalls, DMZs, IDS/IPS sensors, and malware detection and follow a repeatable patching process. Network diagrams of internet-facing systems or high-level diagrams supporting the State are expected to be made available upon request.

7. Contractor must ensure that all the Confidential Information which is no longer required by Contractor to perform its obligations or exercise its rights under this Agreement is securely erased or destroyed in such a manner that such Confidential Information is rendered unrecoverable. As part of such requirement, any data processing equipment which is surplus to Contractor's

requirements and which has held the Confidential Information (e.g. USB flash drives, external hard drives, computer and laptop hard drives, photocopy machines, or solid-state drives (i.e., electronic media with no mechanic parts)) must only be re-used or disposed of following the secure erasure or destruction of all such Confidential Information, and where this occurs, it must be evidenced in writing.

8. On a monthly basis, Contractor or its authorized representatives must perform vulnerability scans of any externally facing system (application and/or infrastructure) that supports the State, its Affiliates, customers or employees (a "**System**"). Alternatively, if the Contractor is unable to perform the required monthly vulnerability scans it must permit the State and/or its authorized representatives to perform such scans. If the scans are performed by Contractor or its authorized representatives, the State will, upon request, be provided with an executive summary of all findings. In either scenario, both parties will collaborate and mutually agree on the remediation schedule to address vulnerabilities in a reasonable period of time.

On an annual basis, and immediately following any major System changes, Contractor must perform an application penetration test on all affected Systems in accordance with industry best practices. Contractor is expected to provide the State with executive summary reports for each affected System upon request. These should be the most recent reports available and include details regarding scope, methodology, and confirmation that the Systems were included in the testing. Vulnerabilities identified as part of a penetration test, must be remediated per the Contractor's policy.

Note: In extenuating circumstances, when the remediation schedule cannot be accommodated, Contractor and the State representatives will collaborate in good faith to address identified control deficiencies within a reasonable schedule.

4820-2333-0405, v. 2