SERVICE PROVIDER SECURITY ASSESSMENT QUESTIONNAIRE

Instructions: (1) Attach additional pages or documents as appropriate and make sure answers cross reference to the questions below. (2) As used in this Questionnaire, the phrase "government information" shall have the meaning defined in the clause titled "Information Security." (3) This Questionnaire must be read in conjunction with both of the following two clauses (a) Service Provider Security Assessment Questionnaire – Required, and (b) Service Provider Security Representation.

1. Describe your policies and procedures that ensure access to government information is limited to only those of your employees and contractors who require access to perform your proposed services.

2. Describe your disaster recovery and business continuity plans.

3. What safeguards and practices do you have in place to vet your employees and contractors who will have access to government information?

4. Describe and explain your security policies and procedures as they relate to your use of your contractors and next-tier sub -contractors.

5. List any reports or certifications that you have from properly accredited third-parties that demonstrate that adequate security controls and assurance requirements are in place to adequately provide for the confidentiality, integrity, and availability of the information systems used to process, store, transmit, and access all government information. (For example, an ISO/IEC 27001 compliance certificate, an AICPA SOC 2 (Type 2) report, or perhaps an AICPA SOC 3 report (i.e., a SysTrust or WebTrust seal)). For each certification, describe the scope of the assessment performed. Will these reports / certifications remain in place for the duration of the contract? Will you provide the state with most recent and future versions of the applicable compliance certificate / audit report?

6. Describe the policies, procedures and practices you have in place to provide for the physical security of your data centers and other sites where government information will be hosted, accessed or maintained.

7. Will government information be encrypted at rest? Will government information be encrypted when transmitted? Will government information be encrypted during data backups, and on backup media? Please elaborate.

8. Describe safeguards that are in place to prevent unauthorized use, reuse, distribution, transmission, manipulation, copying, modification, access or disclosure of government information.

9. What controls are in place to detect security breaches? What system and network activity do you log? How long do you maintain these audit logs?

10. How will government information be managed after contract termination? Will government information provided to the Contractor be deleted or destroyed? When will this occur?

11. Describe your incident response policies and practices.

12. Identify any third party which will host or have access to government information.

Offeror's response to this questionnaire includes any other information submitted with its offer regarding information or data security.

SIGNATURE OF PERSON AUTHORIZED TO REPRESENT THE ACCURACY OF THIS INFORMATION ON BEHALF OF CONTRACTOR:

By: _____
(authorized signature)

Its: _____
(printed name of person signing above)

_____
(title of person signing above)

Date: _____

SPSAQ (JAN 2015) [09-9025-1]