EXHIBIT G – STATE AUDITOR'S OFFICE (SAO) SECURITY QUESTIONNAIRE

Please answer with as much description and detail as possible to the following questions. Questions and requests for information are in support of SAO compliance requirements derived from OCIO Standard No. 141.10. This standard can be retrieved from: https://ocio.wa.gov/policies/141-securing-information- technology-assets/14110-securing-information-technology-assets.

Physical and Environmental Protection

1. Please describe the physical attributes and controls used to protect computer hardware, documents and all related material that could or will be associated with any contracted data exchange between the State Auditor's Office and the audited entity.

[12]

2. Will your organization be storing any contract related data on other systems in addition to workstations such as servers or cloud service providers? If so, describe the physical security and controls in order to protect contract related data.

[12]

3. Will your organization's assigned agents associated with any contract with SAO be accessing and storing any contract data on mobile devices such as phones and tablets. If so, describe any controls used to protect contract related data on those devices.

[12]

Network Security *(Regarding any systems that will be storing, processing or used for transitory (email for example) functions with contract related data)*

1. If applicable, how will your organization apply and enforce network controls to protect segments and individual systems with each segment in order to prevent unauthorized access to contract related data.

[12]

2. How does your organization ensure that systems are up-to-date with latest software security patches and updates? Please explain your organization's patch management process and provide your organization's patch management policy.

[12]

3. Please provide your organization's password policy.

[12]

Operations Management

1. Describe your organizations media handling and disposal process? Please provide your associated policy if applicable.

[12]

2. Does your organization have a data backup processes in place that will capture and backup any data related to the contract? If so, please describe the backup process and procedures and any controls (e.g., encryption) used to protect contract related data in backup systems? Please provide your associated policy if applicable.

[12]

Security Monitoring and logging

1. What type of auditing capabilities, features and settings does your organization enable on systems such as security event logs? Please provide your organization's policy associated to this question.

[12]

2. How long are logs retained on any system that will be handling contract related data?

[12]

Incident Response - In the event of any confirmed compromised or breach of data related to protected contract related data, explain or provide your organization's Incident Response protocol or plan. Please provide all associated organizational policies with this question.

Data Security

1. Please describe your organization's use of multifactor authentication for onsite and remote users.

2. Please explain any controls (encryption; role-based security for example) your organization uses to protect contract related data on systems such as servers to prevent unauthorized access to data-at- rest.

3. Will your organization be using any system(s) for data transfer or transmission such as file transfer or email type systems to transmit contract related data? If so, please describe all controls that will ensure the data exchange is secure and that data cannot be deciphered during transmission.

Security Review

1. Please provide information about any certifications or external audits your organization has completed about your organization's security such as a System and Organization Controls

(SOC) audit or a Cybersecurity Maturity Model Certification (CMMC).