APPENDIX A – AGENCY ANNUAL ASSESSMENT AND COMPLIANCE REPORT TEMPLATE

[AGENCY LETTER HEAD]

TO: Eric Boyette

State Chief Information Officer

FROM: [AGENCY]

SUBJECT: 2018 Agency Compliance Report

Pursuant to the authorities and powers of the State Chief Information Officer enumerated in Session Law 2015-241, and as Agency head for [AGENCY];

A. I certify that [AGENCY] has implemented the appropriate processes and procedures listed below to be in compliance with the Statewide Information Security Manual and State statues:

No data of a confidential nature, as defined in the General Statutes or federal law, was entered into or processed through any information technology system or network established under this Article until safeguards for the data's security satisfactory to the State CIO have been designed and installed and are fully operational.

Agency obtained approval from the State CIO prior to contracting for the storage, maintenance, or use of State data by a private vendor.

Agency ensured all information technology security goods, software, or services purchased using

State funds, or for use by a State agency or in a State facility, was subject to approval by the State

CIO in accordance with security standards

Agency completed annual risk assessments to identify compliance, operational, and strategic risks to the enterprise network. These assessments may include methods such as penetration testing or similar assessment methodologies.

Agency ensured all contracts for third party assessment and testing, was approved by the State CIO (as applicable), and resulting sanitized assessment reports were made public.

Agency provided the full details of the State agency's information technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation

Agency designated an agency liaison in the information technology area to coordinate with the State CIO.

Agency completed an annual assessment of the agency's contracted vendors, to comply with the current security enterprise-wide set of standards. The assessment shall include, at a minimum, the rate of compliance with the enterprise-wide security standards and an assessment of security organization, security practices, security information standards, network security architecture, and current expenditures of State funds for information technology security.

Agency submitted disaster recovery plans to the State CIO on an annual basis and as otherwise requested by the State CIO

Agency achieved completion rate > 90 percent for annual Cybersecurity Awareness Training

during CY 2017

[AGENCY] has not completed all requirements but have identified a plan to be in compliance.

Attached is our assessment report to include corrective action plan indicating when the agency

will meet these requirements.

B. In accordance with § 143B-1342, below is the estimated cost to implement security measures needed for agencies to fully comply with the standards.

SECURITY / BUDGET DEFICIENCIES:

1. **Security Boundary Devices**:

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Personnel**:

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Cybersecurity/IT Training:**

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Vulnerability Management:**

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**5**. **End of Lifecycle Systems:**

[INSERT JUSTIFICATION/COMMENTS or N/A]

Cost to Remediate: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For additional information about this submission please contact: [INSERT AGENCY CONTACT]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name of Secretary/CIO or Designee [Date]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature of Secretary/CIO or Designee