Project Report

1. Behavior-based Anti-virus

- **Objective**: Install behavior-based anti-virus on employee workstations to protect against ransomware and other advanced malware attacks.
  - Phase 1: Install 12,000 licenses.
  - Phase 2: Install up to additional 3,000 licenses if needed.
- **Status**:
  - Phase 1: Closed (100%), initiated in July 2019, completed in December 2019.
  - Phase 2: Not started (0%), may not be required.
- **Expenditure**: Spent $575k for 12,000 licenses for FY20 and FY21, may spend up to an additional $144k for 3,000 more licenses if needed.
- **Notes**: Currently installed 13,745 licenses on employee workstations, utilized some existing licenses, may not need to purchase additional licenses this biennium.

2. Cybersecurity Staff

- **Objective**: Retain current cybersecurity staff and recruit additional cybersecurity staff to protect citizen's data and the State's information assets.
  - Phase 1: Retain current staff by raising salaries and increasing training budgets.
  - Phase 2: Recruit new staff - hired three, interviewing one, and re-drafting one position:
- **Status**:
  - Phase 1: Executing (50%), initiated in July 2019, on schedule to complete in June 2021.
  - Phase 2: Executing (75%), initiated in July 2019, on schedule to complete in December 2019.

Position Code	Status	Title
61106990	Planning	Apprentice
61106991	Hired	SIEM Optimization and Monitoring Specialist
61106992	Interviewing	Firewall Security Expert
61106993	Hired	ISSO / Vulnerability Management
61106994	Hired	ISSO / Business Continuity & Disaster Recovery

- **Expenditure**: Spent $55k for FY20, upcoming FY20 expenses estimated at $250k.
- **Notes**: Repurposed non-HB2 Business Analyst position as a Business Coordinator to drive service excellence, efficiency, and effectiveness to maximize utilization of Security Services staff.

3. Cybersecurity Job Programs

- **Objective**: Develop cybersecurity job programs to provide hands-on cybersecurity skills to people with (apprenticeship) and without (intern) cybersecurity knowledge.
  - Phase 1: Hire a Cybersecurity Apprentice.
  - Phase 2: Hire a Cybersecurity Intern.
- **Status**:
  - Phase 1: Initiating (20%), initiated in July 2019, on schedule to complete in June 2020.

  - Phase 2: Not started (0%), planning to initiate in April 2020 and complete in June 2021.
- **Expenditure**: None.
- **Notes**: Developing apprenticeship program, targeting college career fairs in 2020; will develop internship program after apprenticeship program.

4. Web Application Firewall

- **Objective**: Implement web application firewalls to protect the State's web applications, sites, and data.
- **Status**: Executing (25%), initiated in August 2019, on schedule to complete in January 2020.
- **Expenditure**: Spent $491k for FY20.
- **Notes**: Appliances installed and cabled at datacenters.

5. Email Security Gateway

- **Objective**: Implement an email security gateway to protect the State's email systems.
- **Status**: Executing (90%), initiated in July 2019, on schedule to complete in December 2019.
- **Expenditure**: Spent $192k for FY20.
- **Notes**: Two enhancements pending.

6. Security Information and Event Management

- **Objective**: Upgrade licensing to 1TB per day to detect and respond to cybersecurity events.
- **Status**: Closed (100%), initiated in July 2019, completed in September 2019.
- **Expenditure**: Spent $341k for FY20.
- **Notes**: New licenses have been activated and allocated; old licenses have been removed.

7. Analytics-Driven Security and Continuous Monitoring for Threats

- **Objective**: Implement solutions to detect emerging threats to the State's people, processes, and technology.
  - Phase 1: Enhance external threat intelligence.
  - Phase 2: Consolidate multiple threat intelligence feeds.
- **Status**:
  - Phase 1: Closed (100%), initiated in July 2019, completed in August 2019.
  - Phase 2: Not Started (0%), planning to initiate in July 2020 and complete in December 2020.
- **Expenditure**: Spent $25k for Phase 1 for FY20.
- **Notes**: Phase 2 deferred to FY21 due to HB2 funding allocation.

8. Governance, Risk, and Compliance

- **Objective**: Implement an enterprise Governance, Risk, and Compliance (GRC) system to optimize risk and compliance management.
  - Phase 1: Implement "Assessment & Authorization" and "Plan of Action and Milestones" modules.
  - Phase 2: Implement "Continuous Monitoring" module.
- **Status**:
  - Phase 1: Initiating (5%), initiated in July 2019, on schedule to complete in March 2020 (ready for enterprise use in June 2020).

  - Phase 2: Not Started (0%), planning to initiate in July 2020 and complete in March 2021.
- **Expenditure**: Spent $230k for Phase 1 for FY20, FY21, and FY22.
- **Notes**:
  - Phase 1: Licenses are for three years; vendor minimum is three-year contract.
  - Phase 2: Deferred to FY21 due to HB2 funding allocation.

9. Enterprise Risk Assessment

- **Objective**: Hire a third party to perform an independent risk assessment to identify and prioritize key risks to the State.
- **Status**: Not Started (0%), planning to initiate in July 2020 and complete in June 2021.
- **Expenditure**: None.
- **Notes**: Deferred to FY21 due to HB2 funding allocation.

10. Digital Forensics Lab

- **Objective**: Upgrade the digital forensics lab hardware and software to enhance the State's response to cybersecurity events.
  - Phase 1: Install high-speed isolated internet connection.
  - Phase 2: Update forensic hardware and software.
- **Status**:
  - Phase 1: Closed (100%), initiated in July 2019, completed in December 2019.
  - Phase 2: Not Started (0%), planning to initiate in July 2020 and complete in December 2020.
- **Expenditure**: Spent $12k for FY20 to implement Phase 1 with $60/month ongoing charges for service.
- **Notes**:
  - Phase 1: Isolated high-speed internet connection required for forensic team to safely investigate potentially malicious files off the State's network.
  - Phase 2: Deferred to FY21 due to HB2 funding allocation.

11. Source Code Repository

- **Objective**: Implement an enterprise-class source code repository to protect the State's source code.
- **Status**: Executing (75%), initiated in July 2019, on schedule to complete in March 2020.
- **Expenditure**: Spent $23k for FY20.
- **Notes**: Exploring enterprise offering options.

12. Security Orchestration, Automation and Response (SOAR), and outsourced Professional Services

- **Objective**: Augment the State's cybersecurity people, processes, and technology to enhance and expedite security functions.
  - Phase 1: Utilize professional services to configure and integrate software that requires specialized expertise to implement.
  - Phase 2: Implement and integrate software to augment existing enterprise tools to help security and IT teams respond faster to threats.

  - Phase 3: Implement and integrate software to augment existing enterprise tools to enhance visibility, improve service, and increase agility.
- **Status**:
  - Phase 1: Initiating (5%), initiated in September 2019, on schedule to complete in March 2020.
  - Phase 2: Not Started (0%), planning to initiate in March 2020 and complete in December 2020.
  - Phase 3: Not Started (0%), planning to initiate in July 2020 and complete in June 2021.
- **Expenditure**: Spent $57k for Phase 1 for FY20.
- **Notes**:
  - Phase 2: Dependent on completion of Phase 1.
  - Phase 3: Deferred to FY21 due to HB2 funding allocation.

Expense Report

1. Personnel Expenses

Salaries	40,796
Employee Benefits	14,649
Total	**55,445**

Spent 6% of FY20 Personnel Expenses budget of $1.0 million.

2. Operating Expenses

Other Services	-
Communications	514,285
Rent	-
Repair & Maintenance	-
Supplies & Materials	-
Travel	-
Utilities	945,371
Other Expenses	4,000
Equipment	200,979
Total	**1,664,635**

Spent 77% of FY20 Operating Expenses budget of $2.16 million.

3. Total Expenses

FY2020 Budget	Actuals to Date	Fixed	Upcoming Expenses	Project FYE Actuals	Surplus (Deficit) vs Budget
3,160,000	**1,720,080**	**1,664,635**	**659,937**	**2,380,018**	**779,983**

Spent 54% of FY20 total budget $3.16 million.