Cyber Security Risk Assessment

- Purpose
  - Identify changes in risk due to remote workforce as a result of Covid-19
  - Assess the level of risk within State systems providing critical services
  - Mitigate risk and tighten cyber security within State systems
  - Design and implement automated system to track changes and perform continuous risk management

Progress

- Align with NIST Cyber Security Framework (CSF) standard
- Scope engagement
- Multi-stage process to:
  - set requirements
  - shape assessment
  - perform initial assessment to identify areas of concern
  - hands on technical assessment of critical assets
  - provide guidance for risk remediation
  - implement a system to automate governance, risk, and compliance

Timeline

- Draft RFP ready for mid-August.
- Contract expected in place for October 1, 2020.
- Scope of the assessment – (4 weeks)
- Remediation and framework system implementation – (4 weeks)
- Engagement complete for December 30, 2020.

Cybersecurity Risk Assessment

Agency of Digital Services
Scott Carbee

Project Start: Wed, 7/1/2020

Display Week: 1

TASK	ASSIGNED TO	PROGRESS	START	END
Risk Assessment				
Research and RFP production		75%	7/1/20	8/15/20
RFP issuance and contracting		0%	8/15/20	9/29/20
Assessment		0%	9/29/20	11/13/20
Remediation and framework		0%	11/13/20	12/28/20