Cybersecurity Risk Assessment and Mitigation

CARES Act Funding for Covid-19 Impacts

Prepared by:

Scott Carbee

Chief Information Security Officer

Cyber Security Risk Assessment and Mitigation

- 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 systems to allow maintenance of improved security
- Consists of the following broad categories
  - IT asset inventory (deeper level than number of devices)
  - Network and security architecture (assess current structure, design for remote use)
  - Host/Server security (focus on supporting workers regardless of location)
  - Endpoint security (laptops/desktops/peripherals in the office and at home)
  - Application security (how has usage changed, how do we evaluate and secure)
  - Data security (transmission, storage, structure)
  - Cybersecurity risk management (rebuild the program for an unstructured workplace)

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
- Drafting RFP for mid-August
- Contract expected for October 15th
- Engagement complete for December 30th

Initiative Timeline and Milestones