Information Technology

Legislative Cybersecurity Update

Presenters –
Douglas Camin – Chief Information Officer
Gary Pullis – Information Security Analyst

Highlights – Department Overview

- 30 IT Staff, 2 Full-time Contractors
- Supports 2000 internal users, 50+ outside agencies for emergency services
- Teams for Service Desk, Systems Administration, Development, and Data-Communications
- Significant internal change in process – new Assistant Director, process changes underway
- Six month anniversary (Doug) – Three Month anniversary (Gary)

Cybersecurity Program Overview

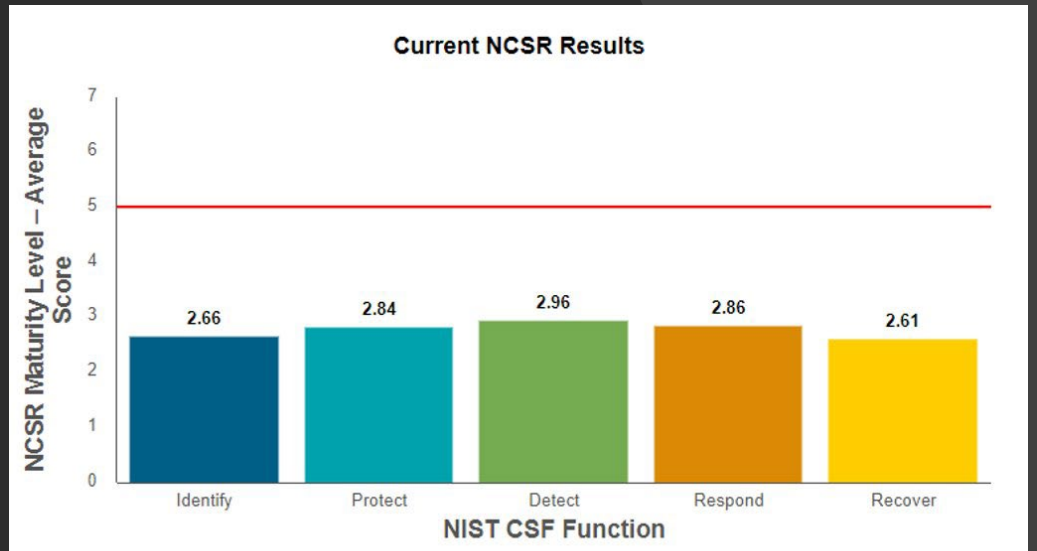
- Current program governed by existing County Security policy
- Planning in process to standardize to CIS framework
- CIS Controls – using Implementation Group 2 (of 3)
- Policies are in draft form and in review stage
- Planned to be fully adopted by mid-2022
- Leveraging external resources to accelerate process and provide breadth

Cybersecurity Program Overview 2

- Partners with numerous external agencies and resources for us to leverage

Cybersecurity Program Overview 3

- NCSR (National Cyber Security Review)
- Self-Reporting Audit
- Required to be done annually (tied to grant funding)



The red line indicates an average score of 5, which is designated as the recommended minimum maturity level

Question	Response	Numerical Score
Identify		2.66
ID.AM		2.83
D.AM-1: Physical devices and systems within the organization are inventoried.	Partially Documented Standards and/or Procedures	4.00
D.AM-2: Software platforms and applications within the organization are inventoried	Documented Policy	3.00
D.AM-3: Organizational communication and data flows are mapped	Informally Done	2.00
D.AM-4: External information systems are catalogued	Informally Done	2.00
D.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	Documented Policy	3.00
D.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	Documented Policy	3.00

Mitigation Measures Already In Place

- Multi-Factor Authentication
- Account Uniqueness
- Asset Inventory
- Ransomware Protection
- Backup Strategies

Q&A