# Legislative Cybersecurity

**Bob Murphy**

**Information Technology Security Engineer**

**Kansas Legislative Office of Information Services**

**January 10th, 2024**

# Agenda

1. Agencies and Standards
   - National Institute of Standards and Technology (NIST)
   - Center for Internet Security (CIS)
   - Cybersecurity and Infrastructure Security Agency (CISA)
   - Kansas Information Technology Executive Council (ITEC)
2. What's happening now…
   - Infrastructure
   - Security
   - Policy

# Agencies & Standards

# NIST

- National Institute of Standards and Technology
  - Established 1901
  - Creates cybersecurity frameworks for critical infrastructure owners in accordance with the Cybersecurity Enhancement Act of 2014
  - Frameworks are prioritized, flexible, repeatable, performance based, and cost-effective
  - Focus on utilizing business drivers to guide cybersecurity activities

# NIST Framework Core Functions

| Function | Description |
| --- | --- |
| **Identify** | Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. |
| **Protect** | Supports the ability to limit or contain the impact of potential cybersecurity events. |
| **Detect** | Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. |
| **Respond** | Develop and implement appropriate activities to act regarding a detected cybersecurity incident. |
| **Recover** | Develop and implement appropriate activities to maintain plans for resilience and to restore my capabilities or services that were impaired due to a cybersecurity incident. |

# Legislative NIST Cyber Security Framework Maturity Levels

- Policy maturity
  - How well do our policies, procedures, standards, and guidelines satisfy NIST CSF requirements?
- Practice maturity
  - How well do our operational practices satisfy NIST CSF requirements regardless of policies and standards?
- Maturity Levels
  - 1-5
  - 1 is least mature
  - 5 is most mature
- Legislative maturity level based on self-assessment conducted July 2023 was:
  - Policy – 1.41 (average)
  - Practice – 1.81 (average)

# CIS

- Center for Internet Security
  - US 501 nonprofit organization formed in October 2000
  - Helps people, business, and governments to protect themselves against pervasive cyber threats
  - Home to the Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - Offers free services to State, Local, Tribal, and Territorial (SLTT) governments
  - CIS Controls ®, CIS Benchmarks ™ , and CIS Hardened Images ® are globally recognized, community-driven, best practices for securing IT systems and data

# CISA

- Cybersecurity and Infrastructure Security Agency
  - Established 2018 under the Department of Homeland Security (DHS)
  - Leads the national effort to understand, manage, and reduce risk to U.S. cyber and physical infrastructure
  - Focused on collaboration and partnership
  - Offers free services to SLTT governments
    - .gov top-level domain
      - kslegislature.gov obtained and parked
    - Vulnerability scanning (weekly or as-needed)
    - Cybersecurity Performance Goals (CPG) assessment
    - Ransomware risk assessment
    - Custom tabletop exercises

# January 7th, 2024, CISA Scan Results

- KLOIS utilizes free cyber hygiene scanning services offered by CISA
- For the reporting period ending January 7th, 2024, CISA cyber hygiene vulnerability scans identified 15 vulnerabilities on 6 vulnerable hosts out of the 259 addresses provided to CISA
- Vulnerabilities are reviewed and remediated, wherever possible, on a weekly basis by KLOIS staff

# Cybersecurity Performance Goals (CPGs)

- CPGs are a subset of cybersecurity practices aimed at meaningfully reducing risks to critical infrastructure operations
  - CPGs provide a baseline set of cybersecurity practices with known risk reduction value
  - CPGs act as a roadmap for critical infrastructure operators to measure and improve cybersecurity maturity
  - Legislative CPG assessment conducted in conjunction with CISA on December 14th, 2023

# Ransomware Risk Assessment (RRA)

- RRA is designed to assist in understanding the current state of readiness to address ransomware threats and implement a focused path for improvement
    - A Legislative RRA was conducted in conjunction with CISA on December 14th, 2023

# Kansas ITEC

- Kansas Information Technology Executive Council
  - Established 1998 by K.S.A. 75-7202
  - Seventeen (17)-member council
    - Chaired by the three branch Chief Information Technology Officers (CITOs)
      - Alan Weis, Legislative CITO, Current chair
    - Membership includes four Legislators
      - Senator J.R. Claeys
      - Senator Jeff Pittman
      - Representative Emil Bergquist
      - Representative Pam Curtis

# Kansas ITEC Cont.

- Provides direction and coordination for the application of Kansas' IT resources
- Responsible for:
  - Adopting IT resource policies, procedures, and project management methodologies
  - Information technology architecture including telecommunications systems, networks, and equipment
  - Data management standards
  - Strategic IT planning for the State of Kansas
- ITEC cybersecurity specific policies:
  - ITEC 7230 – Enterprise Security Policy
  - ITEC 7300 – Security Council Charter
  - ITEC 7230a – IT Security Standards

# What’s happening now…

# Infrastructure

- KLISS modernization
- Upgrade to Microsoft 365 (M365, government licensing)
  - Migration to EntraID (testing)
  - Migration to Exchange Online (testing)
  - Microsoft Teams rollout and adoption (testing)
    - Teams will be utilized as the collaboration/messaging platform for the Legislature, eventually replacing Spark
- 1 Gigabits/second to 10 Gigabits/second fiber upgrades in the State House Secure Data Center
- Upgrading DNS services
  - Taking over domain management
  - Enhancing certificate management
  - Enhancing telemetry
  - www.kslegislature.gov website address change (testing)

# Security

- Managed Detection and Response (MDR) service
  - 24/7 security incident monitoring
  - 24/7 security incident response assistance (available)
  - Proactive threat hunting
  - Managed security awareness and training (bi-weekly)
  - Phishing campaign training
- Security Operations Center (SOC) utilization
- Multi-factor Authentication (MFA) (rollout in process)
- Email security enhancements (in place)
- Testing to compare endpoint detection and response (EDR) services
- In discussions to develop custom tabletop exercises w/CISA
- Annual security and awareness training
- Development of CIS Hardened Images ® in collaboration with Legislative divisions
- Analyzing possible utilization of additional email security services

# Policy

**Currently updating ALL Legislative Cybersecurity policies**

- Approved policies:
  - Data center access control
  - Acceptable use
  - Change management
- Policies currently under review and revision:
  - Patch management
  - ID & authentication
  - Access control
  - General security
  - Incident response
- Pending updates:
  - Secure configuration
  - Mobile device security
  - Security awareness and training
  - Information classification
  - Risk assessment
  - Backup and disaster recovery

# Questions