Legislative Information Technology -Cybersecurity Posture Overview

House Committee on Energy & Digital Infrastructure

May 8, 2025

Vermont General Assembly
Office of Legislative Information Technology

Table of Contents

Introductions

Kevin G. Moore Jr. – Director of Information Technology
Rain Torres – Network Security Administrator

Today's presentation provides a high-level overview of our cybersecurity posture – how we are protecting critical systems, managing risk, and ensuring continuity.

We'll avoid operational specifics, consistent with our practices and procedures not to disclose potentially sensitive information in public settings. However, we're happy to address these questions in an appropriate setting.

What We Mean by ‘Cybersecurity Posture’

Cybersecurity posture refers to our overall readiness. Such as how well we prevent, detect, and respond to threats.

Legislative IT focuses on building resilience, not just to stop threats, but to adapt and recover quickly if something happens. Prioritizing continuous improvement and adaptability, leveraging multiple technologies as force multipliers for our small team.

Core Elements of Our Security Posture

- Governance & Oversight
- Technical Safeguards
- Leveraging External Resources
- Monitoring & Detection
- Preparedness & Response
- Workforce Awareness & Security-First Mindset

Core Elements of Our Security Posture

Governance & Oversight

Legislative IT operates under well-established cybersecurity practices and procedures that are aligned with industry standards. These standards are often informed by leading organizations such as the National Institute of Standards and Technology (NIST), the Cybersecurity Infrastructure Security Agency (CISA). The Defense Information Systems Agency (DISA) and the Center for Internet Security (CIS). Our adherence to these protocols ensures we maintain a high level of security and resilience, effectively safeguarding our critical systems and data.

Core Elements of Our Security Posture

Technical Safeguards

Legislative IT leverages technologies and practices such as:

- Multi-Factor Authentication (MFA)
- Encryption
- Next Generation Firewalls & Network Segmentation
- Automated Threat Intelligence Feeds
- Endpoint Protection
- Extended Detection and Response (XDR)
- Microsoft 365 Advanced Threat Protection (ATP)

Core Elements of Our Security Posture

External Resources & Partnerships

Legislative IT leverages technologies and practices such as:

- MS-ISAC Cyber Hygiene Reporting
- CIS STIGs
- CISA
- DISA
- NCSL & NALIT

Core Elements of Our Security Posture

Monitoring & Detection

- IT staff proactively monitor for suspicious activity using multiple automated tools, responding quickly to any anomalies, non-compliant endpoints, and other potential concerns.
- Real-time alerting ensures a rapid response to potential threats

Core Elements of Our Security Posture

Preparedness & Response

- Incident response procedures are in place and reviewed routinely. As deficiencies are identified, IT staff incorporate updates to these procedures, ensuring we're as prepared as possible should any concerns arise. Backups, recovery procedures, and business continuity protocols are well-established, ensuring minimal disruption in case of an incident.
- Leg IT maintains a cybersecurity insurance policy, via the Office of Risk Management.

Core Elements of Our Security Posture

Workforce Awareness & Security-First Mindset

- **Cybersecurity is Everyone's Responsibility**
- Security-First Mindset
- Proactive Phishing Simulations
- Quarterly Cybersecurity Awareness Training

Security Posture Reviews (SPRs) & Architectural Maturity

- We conduct periodic, consultant led, Security Posture Reviews (SPRs) to assess the maturity of our security architecture.
- SPRs provide us with a detailed evaluation of our systems, policies, and processes to ensure they align with industry standards and best practices. Findings inform continuous improvements – this is a living program.
- Security architectural maturity is continually assessed, and improvements are made as needed to address evolving threats and new technologies. These periodic reviews are vital in ensuring that our defenses remain resilient in the face of emerging threats.

A Few Metrics

- 100% of our workstation and server assets are covered by advanced endpoint protection, ensuring that all endpoints are secure against malware and other threats
- 100% MFA adoption among staff; 43% MFA adoption among Legislators
- Average of 95% success rate across phishing simulations over the past 3 years.
- Over 9,000 malicious IP addresses blocked by external threat providers. List updated hourly. Over 195,000 blocks in ~70 days
- Approx. 191 phishing messages detected and handled daily.

Thank you for your time!

Questions?

Vermont General Assembly
Office of Legislative Information Technology