VERMONT
JUDICIARY

To: **Joint Information Technology Oversight Committee**
From: **Marcia J. Schels, Chief Technology Innovation Officer**
Joe Paquin, Director of Cybersecurity, Infrastructure, and Technology Support Services
Re: **Overview of Judiciary IT Cybersecurity**
Date: **September 30, 2025**

Thank you for the opportunity to provide an overview of the Judiciary's IT Cybersecurity to the Joint Information Technology Oversight Committee on September 30, 2025. Cybersecurity is a critical component of the Judiciary's IT footprint, as we increasingly rely on technology for managing and facilitating all aspects of Vermont's court operations.

During our testimony, we will describe how the Judiciary has implemented Cybersecurity protections to safeguard our systems, networks, and data from unauthorized access, misuse, malicious threats and cyberattacks. Specifically, the Judiciary has in place a multi-layered Cybersecurity defense system, utilizing a variety of vendors with varying expertise, which we will describe in more detail during our testimony:

- **Prevention:** Measures to prevent cyberattacks from occurring in the first place.
  - Zero Trust Network Access (ZTNA) – Aruba ClearPass
  - End-User Cybersecurity Training Program – Huntress
  - Endpoint Protection – Cortex XDR, Microsoft Windows Defender
  - Endpoint Management – Microsoft Intune
  - Network Firewalls (Internal, External, Cloud) – Palo Alto Networks
  - Web Application Protection – Akamai
  - Cloud-Native Application Protection Platform (CNAPP) – Palo Alto Cortex Cloud
  - Security Auditing & Penetration Testing – Security Analyst now on staff
  - Identity and Access Management Auditing

- **Detection:** Tools and techniques to detect and respond to ongoing or suspected cyberattacks.
  - 24/7 Monitoring Security Operations Center as a Service – Huntress
  - Threat Detection (Malware Protection Engine) – Wildfire
  - Infrastructure Monitoring – Paessler PRTG, UpTime.com
  - status.vtcourts.gov – Online, Real-time Status Updates

- **Response:** Having a plan to respond to and recover from a successful cyberattack.
  - Response and Mitigation – Palo Alto Networks Unit 42, Xerox IT Solutions
  - Security Information and Event Management (SIEM) - Huntress
  - Air-Gap Backup Protection – Rubrik
  - Disaster Recovery Redundancy – 2 Network Edges, Primary & Secondary Data Centers, Azure Cloud Infrastructure
  - Backups Stored at Multiple Locations
  - Privacy, Security, and Technology Insurance – CyberRisk Connect (managed by the Agency of Administration's Office of Risk Management)