10440 Little Patuxent Pkwy
Floor 12
Columbia, MD 21044
+443-853-1970
info@cyber-association.com
www.cyber-association.com

House Judiciary Committee
February 4, 2025
Favorable

Chair Clippinger and Members of the Committee

Good afternoon, Chair Clippinger and members of the House Judiciary Committee. My name is Tasha Cornish, and I am the Executive Director of the Cybersecurity Association, Inc. (CA), a statewide, nonprofit 501(c)(6) organization dedicated to the growth and success of Maryland's cybersecurity industry. Established in 2015, CA represents over 600 businesses ranging from Fortune 500 companies to independent operators, collectively employing nearly 100,000 Marylanders.

Thank you for the opportunity to provide testimony on **House Bill 445 – Interference With a Public Safety Answering Point – Penalties**, which seeks to enhance criminal penalties for individuals who intentionally target Maryland's 911 centers. As cybercriminals increasingly exploit vulnerabilities in critical public safety systems, it is imperative that Maryland take proactive measures to protect these essential services from disruption.

The Urgent Need for Action

According to the Cybersecurity and Infrastructure Security Agency (CISA), 911 centers across the nation face a growing array of cyber threats, including ransomware, telephony denial of service (TDoS), spear-phishing, swatting, and unauthorized network intrusions. These attacks can cripple emergency response systems, delaying life-saving assistance to Maryland residents when they need it most.

The **fiscal and policy note for SB 81 (HB 445's cross-file)** highlights that Maryland's **Next Generation 911 (NG911) systems introduce increased cybersecurity risks** due to their reliance on digital infrastructure. NG911 enables enhanced location tracking and multimedia messaging, but it also **expands the attack surface for cybercriminals**, making emergency communications vulnerable to distributed denial of service (DDoS) attacks, domain name system (DNS) hijacking, and other cyber threats. This underscores the need for stronger legal deterrents against those who attempt to disrupt emergency services.

Additionally, while existing Maryland law criminalizes computer-related offenses, **HB 445 strengthens penalties specifically for interference with Public Safety Answering Points (PSAPs)**—commonly known as 911 centers. Given that PSAPs are critical to emergency response, ensuring severe consequences for those who engage in malicious cyber activities is essential. Importantly, the **fiscal note indicates that this bill is not expected to have a material fiscal impact on State or local finances**, demonstrating that Maryland can enhance its cybersecurity protections without imposing undue financial burdens on public agencies.

Sending a Strong Message to Cybercriminals

Beyond strengthening our defenses, Maryland must send an unequivocal message to cybercriminals: **targeting critical infrastructure like 911 centers will not be tolerated.** Attacks on public safety systems are not just crimes of opportunity; they are deliberate, malicious acts that put lives in danger. Those who engage in such attacks must face severe consequences.

By passing HB 445, Maryland will demonstrate its commitment to protecting its residents and holding cybercriminals accountable. This bill will help safeguard **911 operations from cyber threats** and ensure that emergency services remain **reliable and secure for all Marylanders**.

Thank you for your time and consideration. I urge a **favorable report on HB 445**.

Sincerely,
Tasha Cornish
Executive Director
Cybersecurity Association, Inc.