

TO: The Honorable Luke Clippinger, Chair, House Judiciary Committee and Members of the Committee

FROM: Bruce Spector, Chairman of the Board, Baltimore Cyber Range

DATE: January 31, 2025

RE: HB 445 – Interference With a Public Safety Answering Point – Penalties

POSITION: **SUPPORT**

Good afternoon, Chair Clippinger and members of the House Judiciary Committee. My name is Bruce Spector, and I am the Chairman of Baltimore Cyber Range, a Maryland based company that specializes in providing state of the art cybersecurity training to Maryland's citizens and filling the over 30,000 job vacancies in cybersecurity that exist in Maryland.

I am writing to express my strong support for House Bill 445- Interference With a Public Safety Answering Point - Penalties, which seeks to enhance the criminal penalties for those who would 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 are facing 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.

Moreover, 37% of surveyed public safety entities report that cyber incidents have directly impacted their ability to communicate over the past five years (CISA). This alarming statistic underscores the need for safeguards to prevent similar disruptions in our state.

The transition to Next Generation 911 (NG911) systems, while bringing technological advancements, also expands the attack surface for cybercriminals. NG911 systems, which rely on digital infrastructure, are vulnerable to distributed denial of service (DDoS) attacks and domain name system (DNS) hijacking, posing further risks to Maryland's emergency response capabilities.

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 can demonstrate its commitment to protecting its residents and holding cybercriminals accountable.

Sincerely,

Bruce Spector, Chairman of the Board, Baltimore Cyber Range