



**SB101: Criminal Law - Public Safety - Interference With Agencies and Services - Prohibitions
Judicial Proceedings Committee**

Wednesday, January 20, 2021, 11:00 AM

Mission Critical Partners in support of SB101

I represent Mission Critical Partners, a professional services firm that assists clients enhance and evolve their public safety and emergency communications systems and operations as the President of our Consulting Services Division. We provide consulting services to clients with public and life safety missions nationwide, consisting of public safety answering points (PSAPs) and emergency communications centers (ECCs) in nearly all 50 states and the District of Columbia. My career began as a 911 telecommunicator and first responder. I am a certified Emergency Number Professional (ENP) who has served numerous state and local governments, and Federal agencies including the U.S. Department of Transportation (DOT) and the Department of Homeland Security (DHS). With a team of nearly 150 public safety and emergency communications subject matter experts nationwide, these comments draw on our company's breadth of experience as 911 and telecommunications professionals prior to becoming consultants, as well as our service to local, regional, and state 911 systems.

We strongly support this legislation as it would strengthen penalties for many misuses of the 911 system through Swatting—deceptively sending public safety responders to the address of an oblivious person; Telephone Denial of Service (TDoS)—inundating a 911 Center's voice lines, preventing legitimate emergency calls from getting through; Distributed Denial of Service (DDoS)—malevolently disrupting a 911 Center by interfering with its network connectivity; and Caller ID manipulation or “spoofing”—using a false identity when making a phone call or sending a text.

The days of kids' innocent pranks conducted by immature adolescents have been replaced with a new, much more serious twist on this old crime. Disgracefully named “swatting,” which involves calling 911 and faking an emergency that draws a tactical response from law enforcement responders—usually a SWAT team—is dangerous to first responders and victims. The community is placed in danger as responders rush to the scene, taking them away from real emergencies while law enforcement is placed in danger as unsuspecting residents may try to defend themselves.

The schemes are becoming more and more sophisticated and more and more common.

- In 2007, a 19-year-old Washington state man was charged by California authorities after pretending to be calling from the home of a married California couple, saying he had just shot and murdered someone. A local SWAT team arrived on the scene, and the husband, who had been asleep in his home with his wife and two young children, heard something and went outside to investigate—after first stopping in the kitchen to pick up a knife. What he found was a group of SWAT assault rifles aimed directly at him. Fortunately, the situation didn't escalate, and no one was injured.
- In 2016, a Texas attacker sent out provocative tweet asking recipient to “click here.” Those that did were directed to attacker's webpage which launched malware attack on the user's phone. The malware caused the phone to call 911 repeatedly even though the caller did not dial it. Tens of thousands of false calls were made to 911, affecting PSAPs from coast-to-coast.

- In December 2017, law enforcement in Wichita received a call that a man had killed several family members and was going to shoot more. They arrived at the address provided in the phone call, shooting the resident when they mistook a gesture as the man reaching for a gun.

These are just a few examples of the seriousness of the problem affecting our nation's PSAPs, including those here in Maryland and the problems are becoming increasingly more complex. Just three weeks ago, the Federal Bureau of Investigation (FBI) released¹ a public service announcement warning of offenders misusing smart home devices and cameras to carry out swatting attacks.

Penalty under current Maryland law for making anonymous phone calls or sending data that is meant to torment others is a maximum imprisonment of up to three years and/or a fine of up to \$500. As a representative with thirty years of dedication to the 911 community, I support the recommendation of adding the following penalties for TDoS or DDoS:

- Someone attempting to interrupt or impair a PSAP (911 Center) would be subject to imprisonment up to 5 years and/or a fine up to \$25,000; and
- An individual who successfully interrupts a PSAP could be imprisoned for up to 10 years and/or a fine up to \$50,000.

Penalty under current Maryland law for making a false report is subject to imprisonment up to 6 months and/or a fine up to \$500. As a representative with thirty years of dedication to the 911 community, I support the recommendation of adding the following subsequent penalties for swatting, including:

- If law enforcement is dispatched to a scene based on a false report, imprisonment for up to 3 years and/or a fine up to \$5,000; and
- If serious bodily injury occurs, imprisonment for up to 5 years and/or a fine up to \$25,000.

Based on our research of other states legislation regarding Swatting, this legislation would better align Maryland with laws already in effect in California, Connecticut, Indiana, and Wisconsin that have enhanced penalties for persons convicted under their statutes. As a deterrent and illustration, stricter penalties for these events must be implemented with consequences to reflect the crime. I thank you for hearing these concerns, applaud you for taking action on this issue, and urge you to support SB101.

Respectfully submitted,

MISSION CRITICAL PARTNERS, LLC

By: */s/ John Chiaramonte*
John Chiaramonte, ENP, PMP
President of Consulting Services
Mission Critical Partners, LLC
690 Gray's Woods Blvd
Port Matilda, PA 16870

¹ <https://www.ic3.gov/Media/Y2020/PSA201229>