CHERYL C. KAGAN
Legislative District 17
Montgomery County

Vice Chair
Education, Energy, and
the Environment Committee

Joint Audit and Evaluation Committee
Joint Committee on Federal Relations

Miller Senate Office Building
11 Bladen Street, Suite 2 West
Annapolis, Maryland 21401
301-858-3134 · 410-841-3134
800-492-7122 *Ext.* 3134
Fax 301-858-3665 · 410-841-3665
Cheryl.Kagan@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

SB496: Protecting 9-1-1 Centers from Attacks
Senate Judicial Proceedings Committee
February 9, 2024: 12:00 PM

We all rely on 9-1-1 in our greatest times of need. It is imperative that a 9-1-1 Specialist answers our calls or texts for services. The failure of our emergency response system can literally be a matter of **life or death.**

SB496 will help protect our 9-1-1 Centers from cyberattacks that can render them inaccessible. The targeted acts employ hundreds of calls or thousands of website visits to disrupt operations.

These electronic strikes are now a common occurrence. Earlier this week, the Pennsylvania Courts were targeted, knocking many services offline. The scariest disruption targeting PSAPs specifically occurred in 2016, when 9-1-1 call centers in 12 States came under siege. We have seen a shocking 807% increase between 2013 and 2022, with roughly 13 million digital incidents in 2022 alone.[1] In February of 2021, the Federal Bureau of Investigation released a report, "Telephony Denial of Service (TDoS) Attacks Can Disrupt Emergency Call Center Operations,"[2] outlining the significant threat that TDoS threats pose to our 9-1-1 Centers. According to the FBI, "TDoS attacks pose a genuine threat to public safety… by preventing callers from being able to request service."

The need for action was unanimously endorsed by the Next Generation 9-1-1 Commission after four years of work to update, modernize, and improve our emergency systems. In our final, 2021 report, the Commission recommended:
"Increasing penalties for misuse of the 9-1-1 system, including:

- Telephony Denial of Service (TDoS): flooding a 9-1-1 Center's voice lines, preventing legitimate emergency calls from getting through; and
- Distributed Denial of Service (DDoS): maliciously disrupting a 9-1-1 Center by overwhelming its Internet network."

Imposing harsher penalties for disrupting our 9-1-1 Centers was also recommended by the 2023 Statewide "Swatting" Task Force's report, which stated, "It is necessary to update Maryland's

[1] https://www.stationx.net/ddos-statistics
[2] https://www.ic3.gov/Media/Y2021/PSA210217

laws and increase penalties for these cyber and telephonic attacks."[3] We followed the Task Force's recommendations and passed last session, prohibiting 'Swatting,' but we still haven't implemented this part of the report. The House unanimously passed the cross-file of this bill (HB744) last year.

Penalties under SB496 include:

- For an **attempted** 9-1-1 Center interruption, imprisonment not exceeding five years and/or a fine of up to $25,000; and
- For a **successful** 9-1-1 Center interruption, imprisonment not exceeding ten years and/or a fine of up to $50,000.

I urge a favorable report on SB496.

[3]"Report of the Task Force to Study the Practice Known as 'Swatting,'" pg. 18: https://mgaleg.maryland.gov/cmte_testimony/2023/jpr/14492_02202023_153934-232.pdf

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

February 17, 2021

Alert Number
I-021721-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

Telephony Denial of Service Attacks Can Disrupt Emergency Call Center Operations

The Federal Bureau of Investigation is issuing this announcement to provide public steps to help mitigate the impact of Telephony Denial of Service (TDoS) attacks. TDoS attacks affect the availability and readiness of call centers.

WHAT IS A TDOS ATTACK?

A TDoS attack is an attempt to make a telephone system unavailable to the intended user(s) by preventing incoming and/or outgoing calls. The objective is to keep the distraction calls active for as long as possible to overwhelm the victim's telephone system, which may delay or block legitimate calls for service. The resulting increase in time for emergency services to respond may have dire consequences, including loss of life.

TDOS ATTACKS AT CRITICAL CALL CENTERS

Public Safety Answering Points (PSAPs) are call centers responsible for connecting callers to emergency services, such as police, firefighting, or ambulance services. PSAPs represent key infrastructure that enables emergency responders to identify and respond to critical events affecting the public.

TDoS attacks pose a genuine threat to public safety, especially if used in conjunction with a physical attack, by preventing callers from being able to request service. The public can protect themselves in the event that 911 is unavailable by identifying in advance non-emergency phone numbers and alternate ways to request emergency services in their area.

TYPES OF TDOS ATTACKS

TDoS attacks have evolved from manual to automated. Manual TDoS attacks use social networks to encourage individuals to flood a particular number with a calling campaign.

An automated TDoS attack uses software applications to make tens or hundreds of calls, simultaneously or in rapid succession, to include Voice Over Internet Protocol (VOIP) and Session Initiation Protocol (SIP). Numbers and call attributes can be easily spoofed, making it difficult to differentiate legitimate calls from malicious ones.[1]

TDOS ACTORS' MOTIVES

TDoS attacks can be rooted in hacktivism, financial gain or harassment.

Hacktivists might use computer network exploitation to advance their political or social causes.

Malicious actors may initiate a TDoS attack in order to extort municipalities for financial gain.

Malicious actors may also use TDoS attacks to harass call centers and distract operators, regardless of harmful effects. These attacks may be accompanied by messaging on social media platforms in order to increase the severity.

HOW TO PREPARE FOR A 911 OUTAGE

- Before there is an emergency, contact your local emergency services authorities for information on how to request service in the event of a 911 outage. Find out if text-to-911 is available in your area.

- Have non-emergency contact numbers for fire, rescue, and law enforcement readily available in the event of a 911 outage.
- Sign up for automated notifications from your locality if available to be informed of emergency situations in your area via text, phone call, or email.
- Identify websites and follow social media for emergency responders in your area for awareness of emergency situations.

Contact your local law enforcement agency or FBI office if you have information about a TDoS attack (contact information can be found at www.fbi.gov/contact-us/field-offices). Document as many details as you can, to include numbers used.

File a complaint with the **Internet Crime Complaint Center** (www.ic3.gov). When filing a complaint, be sure to use the key words **TDOS**, **PSAP**, and **Public Safety** in the incident description.

If you believe you are the victim of an Internet scam or cyber crime, or if you want to report suspicious activity, please visit the FBI's Internet Crime Complaint Center at www.ic3.gov.

1. SIP is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications. VOIP is a technology that allows voice calls to be made using broadband Internet. ↩