MDEM - SB0496 - FAV.pdf
Uploaded by: Christy Collins
Position: FAV

Maryland
DEPARTMENT OF EMERGENCY MANAGEMENT

Wes Moore | Governor
Aruna Miller | Lt. Governor
Russell J. Strickland | Secretary

SUPPORT – SB0496
Criminal Law - Public Safety - Interference with a Public Safety Answering Point

Maryland Department of Emergency Management
Judiciary Committee
Hearing Date: 9 FEB 2024

Senator William C. Smith, Jr.
Judiciary Proceedings Committee
2 East
Miller Senate Office Building
Annapolis, Maryland 21401

Senator Smith,

The Maryland Department of Emergency Management (MDEM) writes today in support of SB0496 - Interference with a Public Safety Answering Point.

SB0496 is a crucial step toward protecting access to critical emergency services for Maryland residents. This bill will criminalize actions taken intentionally to disrupt the operations of Maryland's Public Safety Answering Points (also known as 9-1-1 Centers), the universal access point to emergency services. The Maryland Department of Emergency Management, home to the Maryland 9-1-1 Board, recognizes the importance of this bill and we respectfully request a favorable report.

Public Safety Answering Points are critical in the chain of public safety response in Maryland. The current statute specifies penalties for interference with other critical services including State government, public utilities, healthcare facilities and public schools. Public Safety Answering Points should be added to this statute to ensure any individual seeking to disrupt

the first node in our life-saving emergency services system are penalized and held accountable.

In summary, the Maryland Department of Emergency Management respectfully requests a favorable report on Senate Bill 0496.

Christy Collins

Christy Collins, Ed.D.
9-1-1 Board Executive Director
Maryland Department of Emergency Management

SB496 Chiaramonte - Written Testimony - PSAP Inter
Uploaded by: John Chiaramonte
Position: FAV

MissionCriticalPartners

SB496: Criminal Law – Interference With a Public Safety Answering Point – Penalties

Judicial Proceedings Committee

Friday, February 9, 12:00 PM

Mission Critical Partners in support of SB496

I represent Mission Critical Partners, a professional services firm assisting public safety agencies nationwide to enhance their 911 systems and operations. With over 30 years of experience in 911, I urge you to support SB496 to strengthen penalties for disrupting 911 services.

Recent years have seen an alarming rise in cyberattacks on public safety answering points (PSAPs) and emergency communications centers (ECCs). These include distributed denial of service (DDoS) attacks that flood networks and block access, telephone denial of service (TDoS) attacks that inundate 911 lines, and caller ID spoofing. The harm caused can be severe—potentially blocking 911 access during a terrorist attack or natural disaster and putting lives at risk.

Our nation's critical infrastructure is under constant attack and "bad actors" are increasingly targeting local governments, including PSAPs. While some communities, including those across the State of Maryland, are taking proactive steps to reduce cyberattacks, more must be done to protect mission critical 911 operations, including strengthening penalties for those convicted of interrupting or impairing PSAP operations.

Generally, DDoS attacks are intended to block public access to an online service by flooding it with junk data or repeated requests from multiple, and often compromising sources, thereby rendering legitimate access impossible. DDoS attacks are increasing in quantity, breadth, and sophistication. Some attacks have gone as far as demanding a ransom to terminate the attack.

Government agencies are also experiencing "reciprocal effects" from non-government targeted DDoS attacks. In late 2014, upset with the creation of homeless ordinances by the city of Fort Lauderdale, the hacker collectively known as "Anonymous" carried out its threats to implement a DDoS attack for the city's online presences. By doing so, three of the 18 PSAPs in Palm Beach County, FL were overwhelmed with DDoS traffic because the county's 911 networking systems were housed in the same facility as the city's public website servers.

Similarly, a TDoS attack is a deluge of malicious inbound calls that target PSAPs, typically on non-emergency (10-digit) lines, which are also answered by 911 specialists (who are not already answering 911 calls). There is significant concern within the 911 and first responder community that a TDoS, coupled or coordinated with a physical terrorist attack or a DDoS attack, would amplify the disruption and place lives at risk. True emergency calls from citizens would not be able to be answered as 911 personnel deal with a flood of automated false calls.

Due to advances in telecommunications services, TDoS attackers have nearly unlimited access to voice over internet protocol (VoIP) services that can easily generate hundreds and thousands of simultaneous

MissionCriticalPartners

false calls into 911 centers, quickly overwhelming 911 personnel. These VoIP services can also spoof caller identification information and use computer-generated voice that makes it difficult and time consuming to differentiate false call from legitimate (and human) callers.

Penalties under current Maryland law for crimes involving telecommunications and electronics (§ 7-302) are insufficient deterrence when compared with the gravity of impairing our 911 systems. As a result, I support the recommendation of adding the following penalties:

- Someone attempting to interrupt or impair the function of a PSAP would be subject to imprisonment up to 5 years and/or a fine up to $25,000; and
- An individual who successfully interrupts or impairs PSAP operations could be imprisoned for up to 10 years and/or a fine up to $50,000.

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 support of SB496.

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

Senate Bill 496 - DoIT Written Testimony.docx.pdf
Uploaded by: Katie Savage
Position: FAV

Maryland
DEPARTMENT OF INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

TO: Senate Judicial Proceedings Committee
FROM: Department of Information Technology
RE: Senate Bill 496 - Criminal Law - Interference With a Public Safety Answering Point - Penalties
DATE: February 9, 2024
POSITION: Support

The Honorable William C. Smith, Jr., Chair
Senate Judicial Proceedings Committee
2 East, Miller Senate Office Building
Annapolis, Maryland 21401

Dear Chairman Smith,

The Department of Information Technology (DoIT) supports Senate Bill 496 - Criminal Law - Interference With a Public Safety Answering Point - Penalties. This bill aims to address and deter interference with public safety answering points. Public safety answering points play a critical role in ensuring the safety and well-being of our communities by handling emergency calls and dispatching appropriate response teams.

The proposed amendments to Article 7-302 of the Criminal Law are essential in addressing intentional and unauthorized actions that may interrupt or impair the functioning of a public safety answering point. By explicitly prohibiting such activities and imposing significant penalties, the bill seeks to safeguard the integrity and effectiveness of these crucial communication hubs.

The inclusion of specific provisions related to the possession of ransomware with malicious intent is particularly commendable. This demonstrates a forward-thinking approach to addressing evolving threats in the digital landscape and reinforces the importance of protecting our public infrastructure.

Furthermore, the bill establishes appropriate penalties for violations, distinguishing between misdemeanors and felonies based on the severity of the offense. These penalties send a clear message that interference with public safety answering points is a serious offense that will be met with significant consequences.

Maryland
DEPARTMENT OF
INFORMATION TECHNOLOGY

Wes Moore | Governor
Aruna Miller | Lt. Governor
Katie Savage | Secretary

For these reasons, the Maryland Department of Information Technology respectfully requests a favorable report on Senate Bill 496.

Best,

Katie Olson Savage
Secretary
Department of Information Technology

SWATTING ADL testimonies in senate - SB496.pdf
Uploaded by: Meredith Weisel
Position: FAV

Maryland General Assembly
Senate Judicial Proceedings Committee
February 9, 2024
Testimony of Meredith R. Weisel
ADL Washington D.C. Regional Director

ADL (the Anti-Defamation League) is pleased to submit this testimony in support of ***Senate Bill 496 – Criminal Law – Interference With a Public Safety Answering Point – Penalties.***

ADL (the Anti-Defamation League)

Since 1913, the mission of ADL (the Anti-Defamation League) has been to "stop the defamation of the Jewish people and to secure justice and fair treatment to all." Dedicated to combating antisemitism, prejudice, and bigotry of all kinds, as well as defending democratic ideals and promoting civil rights, ADL has long been recognized as a leading resource on effective responses to violent bigotry, conducting an annual Audit of Antisemitic Incidents and drafting model hate crime statutes for state legislatures.

Since its inception over a century ago, ADL has been the leading organization fighting hate. As we have said time and time again, where people go, hate follows—including online. That is why, in the early days of dial-up, ADL anticipated the ways in which hate speech could poison the internet and made certain we were investing our time and resources to communicate to the key players in the industry the need for clear and understandable terms of service on hate speech and encouraged them to enforce these policies aggressively. In 2017, we doubled down on our efforts and launched the Center for Technology and Society (CTS). CTS is a leader in the global fight against online hate and harassment.

In a world riddled with antisemitism, bigotry, and extremism, ADL has worked with the tech industry and elected leaders to promote best practices that can effectively address and counter these threats. Our combination of technical and policy expertise–and decades of lived experience embedded in a community that has been targeted, often lethally, by bigots and extremists–informs our approach to fighting online hate, protecting targets of online harassment, and holding platforms accountable. Strengthening our laws to ensure we are protecting vulnerable groups against actions of online hate and harassment as well as its consequences on the ground should be a major priority for Maryland.

Impact of Hate Online

In addition to the surge of hate crimes in our communities, the growth of online hate and harassment targeting marginalized groups is a trend that deserves action by policymakers. According to a recent national ADL study called ***"Online Hate and harassment: The American Experience 2023,"*** among adults 52% reported being harassed online in their lifetime. The 2023

study also showed that both adults and teens are facing severe acts of harassment online and overall reports of hate and harassment have increased in nearly every measure and within almost every demographic group. Defined as physical threats, sustained harassment, stalking, sexual harassment, doxing, and/or swatting, severe harassment of some kind was reported by a majority of respondents. All Maryland residents have a stake in effective responses to hate online.

Swatting

We must do more to ensure we are protecting vulnerable groups against actions of online hate and harassment as well as its consequences on the ground. Such actions include the emerging threat of swatting. Initiating a false alarm is also known as "swatting" when it involves the malicious act of creating a 911 hoax with the goal of sending emergency responders to another's dwelling. The objective of swatting is none other than to weaponize emergency response systems to harass and intimidate others. It is costly, hazardous, and causes trauma and serious harm to individuals and to communities. This dangerous conduct has resulted in physical and psychological injuries—including at least one death—to direct targets as well as unintended victims.

Swatting has happened across Maryland, resulting in a grave misuse of government emergency response resources, serious bodily harm to targets, and severe emotional distress to victims. **Last year the Maryland General Assembly passed important legislation to help counter the act of swatting and address this problem by holding swatting perpetrators responsible, empowering victims, and establishing sentencing guidelines that reflect the severity of these incidents and can deter future incidents.**

SB496 would help to specifically address the significant issue of disruption and impairment of our public safety answering points. Swatting not only causes harm to individuals being targeted or witnesses nearby, but it has a ripple effect on our emergency services that are needed elsewhere at the same time. Emergency responders may not be able to get to someone who is suffering a medical emergency, or car accident, or some other actual emergency when the 911 system is disrupted.

Recommendation

For these reasons, ADL recommends **SB496** be enacted to address the impact of swatting in Maryland. If passed, this law would help enhance the work started last year to prohibit a person from making emergency reports with reckless disregard of causing bodily harm to an individual as a direct result of a hoax swatting call.

We urge the Senate Judicial Proceedings Committee to give SB496 a favorable report.

2024 Skyline Testimony for SB496.pdf
Uploaded by: Mia Millette
Position: FAV

February 9, 2024

Chair William C. Smith, Jr.
Judicial Proceedings Committee
Maryland State Senate
2 West Miller Senate Office Bldg.
11 Bladen Street
Annapolis, MD 21401

SUBJECT: Senate Bill 496 – Favorable

Dear Chair Smith, Vice Chair Waldstreicher, and members of Judicial Proceedings Committee,

My name is Matthew Smith, and I am the Chief Network Architect at Skyline Technology Solutions LLC. The pursuit of our mission, "to build a more resilient and connected society", drives our passion to support Governmental inter-communication through infrastructure and application development that facilitates increased levels of data sharing and collaboration within and between the partners we serve. Increases in connectedness between organizations often also results in an increased threat landscape against the critical communications infrastructures used both for internal as well as citizen service delivery. As experts in Information Technology communications infrastructure, we have seen firsthand how technology can also be used as a weapon intended to disrupt critical communication services. We have supported the Maryland State Department of Information Technology's networkMaryland™ program and in partnership with DoIT have supported mitigation of many distributed denial of service attacks launched against its subscriber community. While DoIT's investment in mitigation technologies and services have limited the impacts of these large-scale DDoS events some level of disruption of services is unavoidable. The costs of mitigating these attacks, overall loss of productivity, as well as subsequent investigations and counter measures result in a high burden. As a Maryland company we support the legislation under SB496 that prohibits and penalizes perpetrators that intentionally interrupt or impairs public safety answering points.

Technology is being increasingly leveraged by emergency response organizations to better serve our communities. Next Generation 9-1-1 (NG911) is a nationwide, standards-based system that will transition our 9-1-1 system from analog to IP based systems. The NG systems will allow the public to send digital data like photos, videos, and texts to PSAPs/ECCs. It will also allow telecommunicators to share data with field responders, other PSAPs/ECCs, and other agencies and organizations. As Maryland transitions to NG9-1-1 it Is critical that our laws also evolve to ensure the infrastructure

supporting our communities. While any Intentional impairment or attempt to impair a computer system should not be permitted, such attacks against NG9-1-1 and/or critical supporting systems are particularly abhorrent as disruptions and/or impairments of these services directly impact life safety services. Our NG9-1-1 systems need to be protected both technically and lawfully and we fully support SB496.

Sincerely,

Matthew Smith
Chief Network Architect

Skyline Technology Solutions

SB0496-JPR_MACo_SUP.pdf
Uploaded by: Sarah Sample
Position: FAV

MARYLAND Association of COUNTIES

Senate Bill 496

Criminal Law - Interference With a Public Safety Answering Point - Penalties

MACo Position: **SUPPORT**

To: Judicial Proceedings Committee

Date: February 9, 2024

From: Kevin Kinnally and Sarah Sample

The Maryland Association of Counties (MACo) **SUPPORTS** SB 496. This bill would bolster state laws to protect against sophisticated cyber-attacks that pose a significant threat to the security and stability of Maryland's 9-1-1 system.

In 2019, the General Assembly passed Carl Henn's Law, landmark legislation to update state laws and the 9-1-1 financing system to provide the flexibility and resources needed for the deployment of a statewide Next Generation 9-1-1 (NG911) system that Maryland residents expect and deserve. As Maryland continues the move toward NG911, proper safeguards are necessary to protect against new and evolving cyber threats, including denial-of-service attacks and intrusions by malicious hackers.

SB 496 generally prohibits any actions that intend to interrupt or impair the functioning of a 9-1-1 center. Under the bill, if an individual commits a prohibited act that intends to interrupt the operations of a 9-1-1 center, the person is guilty of a felony and subject to imprisonment for up to five years and/or a fine up to $25,000. In addition, if an individual perpetrates an illegal act that disrupts the operations of a 9-1-1 center, the violator is guilty of a felony, punishable by imprisonment for up to ten years and/or a $50,000 maximum fine.

Hackers are increasingly targeting state and local governments – including public safety agencies – with sophisticated cyberattacks that can jeopardize sensitive information and disrupt emergency services. By strengthening state laws to protect against growing and evolving cyber threats, SB 496 would enhance public safety communications in Maryland and in our local communities.

For these reasons, MACo urges a **FAVORABLE** report for SB 496.

SB496_SenKagan.pdf
Uploaded by: Sen. Cheryl Kagan
Position: FAV

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. ↩

SB0496_Senator Kagan_Interference With a Public Sa
Uploaded by: Susan Greentree
Position: FAV

SB0496 – Interference With a Public Safety Answering Point – Penalties

Susan Greentree – Retired 9-1-1 Specialist (Anne Arundel County) / Appointee to the Maryland 9-1-1 Board

Sue.Greentree@yahoo.com ------- sgreentree@verizon.net

Cell: 410-852-3362

257 Overleaf Drive, Arnold MD 21012-1947

I respectfully request SB0496, Interference With a Public Safety Answering Point – Penalties be passed into law.

I worked in the Anne Arundel County 9-1-1 center for 35+ years (1984-2020). In the past several years there have been numerous instances of cyber-attacks on 9-1-1 centers across the country. It is unfathomable to me that anyone would want to take down a 9-1-1 center, but sadly they do. SB0496 moves to make those who seek to disrupt 9-1-1 operations in Maryland, therefore the health and safety of the public, to be found guilty of a felony.

MD, Baltimore City 9-1-1 was attacked March 25th 2018, bringing down 9-1-1 operations.

MD, Baltimore City Gov't was attached in 2019.

MD, St Mary's County public safety systems were attacked going into the Thanksgiving weekend of 2016. Fortunately, their IT person on duty picked up on the activity in time to secure their system and recover.

CA, Hayward declares an emergency after cyber-attack impedes 9-1-1 dispatching in 2023.

NY, Suffolk County 9-1-1 operations resulting in the 9-1-1 dispatch center implementing manual operations, pen and paper to process calls for service.

Maryland has been a leader in advancing public safety and 9-1-1. Legislation requiring PSAP's (Public Safety Answering Point) to implement cybersecurity monitoring, enhanced training requirements for 9-1-1 Specialist and upgrading the public safety systems to NG9-1-1. All of that is great, but NOW is the time to implement laws that hold those who would work to attack our 9-1-1 centers operations accountable. I urge you to vote YES for SB0496

Thank you.

UNF SB0496 (JPR) vmcavoy.pdf
Uploaded by: vince mcavoy
Position: UNF

UNFAVORABLE on SB0496
Criminal Law - Interference With a Public Safety Answering Point – Penalties
vince mcavoy baltimore maryland

Dear Senators of JPR,
Senator Kagan, whose work with the 9-1-1 system is admirable, has written a bill that extends to any number of scenarios outside of the example given.

The penalties involved and the ambiguity of such words as “interrupt” or “impair” are not reasonable. If I didn’t like what Governor Hogan was saying during press conferences as he blathered on about the scamdemic, then went up near the podium and made hand gestures next to his several hearing-impaired sign languagers, would that be an “impairment”?

Further, this bill opens an ability for any tyrannical state official to say being yelled at from the audience, accidentally kicking a power cable or just blocking an aisle for a few extra seconds to be caught up in dictatorial powers.

When we have 9-1-1 hacking and other serious issues, we can use state and/or federal regulations. Those are rightfully set as felonies.
We do not need bills potentially curtailing freedom of speech at what are often politically-inspired rallies. This is America, not China.

I urge an UNFavorable for this inhuman approach of SB0496.
humbly offered
~vince