HB 445 - FAV - MDEM.pdf
Uploaded by: Anna Sierra
Position: FAV

Maryland
DEPARTMENT OF EMERGENCY MANAGEMENT

mdem.maryland.gov
877-636-2872
7229 Parkway Drive, Suite 200 | Hanover, MD 21076

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

FAVORABLE - HB 445
Criminal Law - Interference with a Public Safety Answering Point - Penalties

Judicial Proceedings

Maryland Department of Emergency Management
Hearing Date: 4 FEB 2025

The Maryland Department of Emergency Management (MDEM) writes today in support of **HB 445 - Criminal Law - Interference with a Public Safety Answering Point - Penalties.**

HB 445 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 is penalized and held accountable.

In conclusion, the Maryland Department of Emergency Management respectfully requests a favorable report on **HB 445 - Criminal Law - Interference with a Public Safety Answering Point - Penalties.** If you have any questions, please contact Anna Sierra, MDEM legislative liaison: anna.sierra1@maryland.gov.

Baltimore Cyber-HB 445 Support (2).pdf
Uploaded by: Bruce Spector
Position: FAV

BCR Cyber | 3700 Koppers Street, Suite 500, Baltimore, MD 21227 | (443) 545-0702 | www.brcyber.com

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

HB445 Written Testimony.pdf
Uploaded by: Dale Bowen
Position: FAV

MARYLAND STATE FIREFIGHTERS ASSOCIATION

Representing the Volunteer Fire, Rescue and Emergency Medical Services Personnel
-a 501(c)3 Organization

Legislative Committee
17 State Circle
Annapolis MD, 21401
Chair: Robert Phillips
Email: rfcchief48@gmail.com
Cell: 443-205-5030
Office: 410-974-2222

House Bill 445: Criminal Law – Interference With A Public Safety Answering Point – Penalties

My name is Dale Bowen and I am a member of the Legislative Committee for the Maryland State Firefighter's Association (MSFA).

I wish to present favorable testimony for **House Bill 445: Criminal Law – Interference With A Public Safety Answering Point – Penalties**.

The MSFA is in full support of HB 445. Public Safety Answering Points (PSAP) are vital as the first line of defense for the public. The state's 9-1-1 system operates primarily through PSAP's. This bill adds the intent and act that interrupts or impairs the function of a PSAP as criminal act.

PSAP's are also vital to our first responders. Interruption of service of a PSAP will delay our response to serious life threatening incidents as well as prevent communication between responding units.

Our citizen's safety relies on the efficiency of Public Safety Answering Points. It is for this reason that I ask for a favorable vote on House Bill 444.

Thank you for your consideration.

Respectfully,
Dale Bowen

CA-2025-HB445-HOUSE HEARING.pdf
Uploaded by: John Fiastro
Position: FAV

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.

HB0445-JUD_MACo_SUP.pdf
Uploaded by: Sarah Sample
Position: FAV

House Bill 445

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

MACo Position: **SUPPORT**

To: Judiciary Committee

Date: February 4, 2025

From: Kevin Kinnally and Sarah Sample

The Maryland Association of Counties (MACo) **SUPPORTS** HB 445, which bolsters protections against cyberattacks targeting 9-1-1 centers, a vital component of Maryland's emergency response infrastructure. By addressing these evolving threats, the bill enhances the security and stability of the 9-1-1 system, ensuring continued public safety and reliable emergency services.

Maryland's transition to Next Generation 9-1-1 (NG911) modernizes emergency communication capabilities, enabling faster and more accurate emergency response. However, this advanced system faces significant cybersecurity threats as hackers increasingly target public safety networks. HB 445 strengthens state law by expressly prohibiting acts intended to impair or disrupt 9-1-1 center operations – deterring these malicious attacks and safeguarding Maryland's 9-1-1 system.

The bill increases penalties for individuals who intentionally disrupt 9-1-1 center operations. By elevating these offenses to felonies with penalties of up to five or ten years of imprisonment and substantial fines, the bill reflects the grave danger these actions pose to public safety.

Counties operate and fund 9-1-1 centers, which safeguard Maryland's emergency response systems. A cyberattack or disruption at a 9-1-1 center threatens lives, delays critical responses, and undermines community safety. This bill equips counties and the State with additional tools to protect residents and strengthen Maryland's 9-1-1 infrastructure.

County governments are dedicated to enhancing public safety and protecting the resources counties rely on to serve their communities. Accordingly, MACo urges the Committee to issue a **FAVORABLE** report on HB 445.

Cybersecurity Laws by State (JRL 1.15.25) (4) (1)
Uploaded by: Terri Hill
Position: FAV

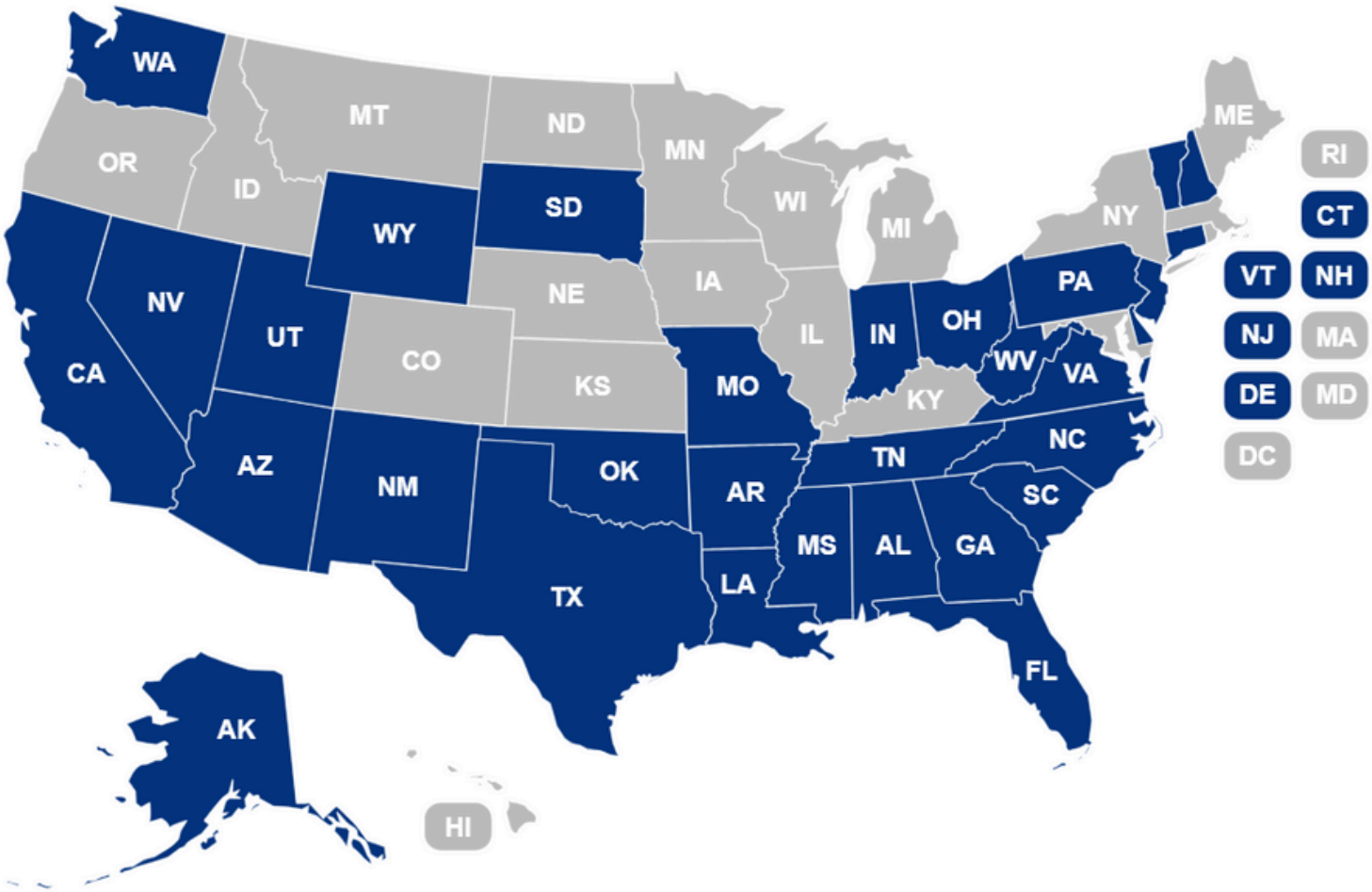
CYBERSECURITY LAWS BY STATE

State	Current Law
AL	“Disrupts or causes the disruption of a computer... or causing the denial of computer or network services to any authorized user”
AK	“Disrupts, disables, or destroys a computer, computer system, computer program, computer network, or any part of a computer system or network”
AZ	“Denying or causing the denial of computer or network services to any authorized user”
AR	“Denies, or causes the denial of access to or use of a computer, system, or network to a person who has the duty and right to use the computer, system, or network”
CA	“Denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network
CT	“Denies or causes the denial of computer services to an authorized user of a computer system
DE	“Denies or causes the denial of computer services to an authorized user”
FL	“Denies or causes the denial of the ability to transmit data to or from an authorized user”
GA	“Authorized computer user was denied service”
IN	"Denies, or causes the disruption or denial of computer system services to an authorized user”
LA	“Denial to an authorized user, without consent, of the full and effective use of or access to a computer”
MS	“Denial to an authorized user, without consent, of the full and effective use of or access to a computer”
MO	“Denies or causes the denial of computer system services to an authorized user”
NV	“Denies or causes the denial of access”
NH	“Denies or causes the denial of computer services to an authorized user of a computer or computer network”

State	Current Law
NJ	“Denies, disrupts or impairs computer service”
NM	“Disrupts or destroys any computer, computer network, computer property, computer service or computer system”
NC	“Denies or causes the denial of computer, computer program, computer system, or computer network services to an authorized user”
OH	“Denying access through the network to the targeted computer or network, resulting in what is commonly know as ‘Denial of Service’ or ‘Distributed Denial of Service’ attacks”
OK	“Deny or cause the denial of access or other computer services to an authorized user”
PA	“Intentionally or knowingly engages in a scheme or artifice, including, but not limited to, a denial of service attack upon any computer”
SC	“Denying access through the network to the targeted computer or network, resulting in what is commonly know as ‘Denial of Service’ or ‘Distributed Denial of Service’ attacks”
SD	“Knowingly disrupts, denies, or inhibits access to a computer system, without consent of the owner”
TN	“Cause the disruption to the proper operation of any computer, or perform an act which is responsible for the disruption of any computer”
TX	"Knowingly accesses… a computer, computer network, or computer system without the effective consent of the owner”
UT	“Knowingly engages in a denial of service attack”
VT	“In connection with any scheme or artifice to defraud, damaging, destroying, altering, deleting, copying, retrieving, interfering with or denial of access to, or removing any program or data contained therein”
VA	“Disabling or disrupting the ability of the computer to share or transmit instructions or data to other computers”
WA	“Intentionally interrupts or suspends access to or use of a data network or data service”
WV	“Any person who knowingly, willfully, and without authorization, directly or indirectly… denies or causes the denial of computer services to an authorized recipient”
WY	“Denies computer system services to an authorized user of the computer system services”

As of January 2025

CYBERSECURITY LAWS BY STATE



As of January 2025

HB 445 (PSAP) Delegate Testimony (final).pdf
Uploaded by: Terri Hill
Position: FAV

Terri L. Hill, M.D.
Legislative District 12A
Howard County

Health and Government Operations Committee

Subcommittees

Government Operations and Health Facilities

Public Health and Minority Health Disparities

THE MARYLAND HOUSE OF DELEGATES
ANNAPOLIS, MARYLAND 21401

Annapolis Office
The Maryland House of Delegates
6 Bladen Street, Room 404
Annapolis, Maryland 21401
410-841-3378 · 301-858-3378
800-492-7122 *Ext.* 3378
Fax 410-841-3197 · 301-858-3197
Terri.Hill@house.state.md.us

District Office
410-884-4380
Fax 410-884-5481

SUPPORT - HB445
CRIMINAL LAW – PUBLIC SAFETY – INTERFERENCE WITH A PUBLIC SAFETY ANSWERING POINT – PENALTIES

February 4, 2025

Chair Clippinger, Vice Chair Bartlett, and Members of the Judiciary Committee,

HB445 addresses the targeted, deliberate disruption and dismantling of 9-1-1 Call Centers, also known as Public Safety Answering Points (PSAPs). This bill builds on recommendations from the Next Generation 9-1-1 Commission, which emphasized the urgent need to strengthen protections for critical emergency response infrastructures.

Similar legislation was introduced in 2020, 2021, and 2022. It was modified on recommendation of the 2022 Judiciary and Judicial Proceedings summer workgroup which focused on best defining of attacks, deterrence, and penalties and reintroduced, passing the House 135-0 in 2023 and 141-0 in 2024. The bill has made it to the JPR vote list but not had a vote. **HB445** is the reintroduction of that bill and is in the same posture as last year's bill.

Cyberattacks, defined by IBM as "any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device" [1]. PSAP cyber-attacks are particularly egregious because they jeopardize Marylanders' ability to access and receive life-saving services, put the overall safety of communities at risk. In the third quarter of 2021, there was an average of over 1,000 cyber-attacks per day.

The most common methods of attacks are:

- **Telephone Denial of Service (TDoS)** involves a large volume of malicious calls made to public service response systems with the aim of overwhelming the system.
- **Distributed Denial of Service (DDoS)** involves a large volume of malicious electronic traffic generated and directed to overwhelm a site and disrupt its service.

HB445 creates penalties for actions:

- directed with the intent of disrupting the functioning of a PSAP of a felony, punishable by up to 5 years imprisonment and/or maximal fine of $25,000.
- resulting in the disruption or impairment of a PSAP of a felony, punishable by imprisonment for up to 10 years and/or a maximum fine of $50,000.

To protect Maryland from cyber-attacks on critical government and emergency response infrastructures, and ensure the proper, round-the-clock operating of our emergency reporting and response systems, I ask for a favorable report on **HB445**.

[1]https://www.ibm.com/think/topics/cyber-attack#:~:text=A%20cyberattack%20is%20any%20intentional,theft%20to%20acts%20of%20war

Sen.McKay Testimony-PSAP.pdf
Uploaded by: Terri Hill
Position: FAV

MIKE MCKAY
Legislative District 1
Garrett, Allegany, and Washington Counties

Judicial Proceedings Committee

Executive Nominations Committee

James Senate Office Building
11 Bladen Street, Room 416
Annapolis, Maryland 21401
410-841-3565 · 301-858-3565
800-492-7122 *Ext.* 3565
Mike.McKay@senate.state.md.us

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

February 04, 2025

RE: Fire/EMS Coalition Support for House Bill 445

Dear Chairman Korman, Vice Chairman Boyce, and Members of the Committee,

The Fire/EMS Coalition would like to express their support for House Bill 445: Criminal Law – Interference With a Public Safety Answering Point – Penalties. The bill will prohibit a person from taking certain actions with the intent to interfere the function of a public safety answering point. It will also prohibit a person from taking certain actions that interferes with the functioning off a public safety answering point. The authorized penalties for certain violations will be imprisonment of up to 5 years or a fine not exceeding $25,000 or both.

The Fire/EMS Coalition supports House Bill 445 as it will be beneficial to all Fire/EMS workers when responding to medical or fire calls. There are many interference issues that Maryland first responders face when responding to calls. The interferences can be life altering and life threatening when individuals prevent our first responders from doing their job. The Coalition supports this bill as it will provide a deterrent and punishment for those who intentionally get in the way of our firefighters and EMS workers.

Sincerely,

Senator Mike McKay
Representing the Appalachia Region of Maryland
Serving Garrett, Allegany, and Washington Counties

<u>Voting Organizations</u>:
Maryland Fire Chief's Association (MFCA)
Maryland State Firemen's Association (MSFA)
State Fire Marshal (OSFM)
Maryland Fire Rescue Institute (MFRI)
Maryland Institute for Emergency Medical Services System (MIEMMS)

Metro Fire Chief's Association
Professional Firefighters of Maryland

Our Mission Statement

The Maryland Fire/EMS Coalition unites Republicans and Democrats in support of fire/emergency services legislation that benefit all first responders. Becoming a member does not require taking positions on legislation; rather Coalition members are asked to offer support in a way that best benefits fire/emergency services in their respective Legislative Districts.

Summary HB445 and HB444 PSAP TDos_DDos.pdf

Uploaded by: Terri Hill

Position: FAV

SUMMARY OF AND DISTINCTIONS BETWEEN 2025HB445 AND HB444

Under § 7-302 of the Criminal Law Article, a person may not intentionally, willfully, and without authorization, access or attempt to access, cause to be accessed, or exceed the person's authorized access to all or part of a computer, computer network, computer control language, computer software, computer system, computer service, or computer database. A person may not intentionally, willfully, and without authorization, copy, attempt to copy, possess, or attempt to possess the contents of all or part of a computer database that was unlawfully accessed.

➔ Misdemeanor: up to three / $1,000

- above with the intent to
    - (1) cause the malfunction or interruption of all or any part of a computer network/ control language/ software/ computer system/ computer service/ or computer data or
    - (2) alter, damage, or destroy all or any part of data or a computer program
- intentionally, willfully, and without authorization
    - (1) possessing, identifying, or attempting to identify a valid access code or
    - (2) publicizing or distributing a valid access code to an unauthorized person.

➔ Misdemeanor: 5 years/$5,00 if aggregate loss <$10,000
Felony: 10 years/$10,000

- if intent to interrupt or impair the functioning of (1) the State government; (2) a public utility (3) a service provided in the State by a public service company; (4) a health care facility; or (5) a public school.
- If the aggregate amount of the associated loss > $10,000

➔ Felony: 10 years / $100,000.
If the aggregate amount of the loss is < $10,000

➔ Misdemeanor: 5 years / $25,000

Possession, distributing, or deploying ransom ware

➔ Misdemeanor: 2 years/ $5,000

With HB445 *(the narrower bill)*
A person who commits prohibited act with ***the*** **intent to interrupt or impair the functioning of a PSAP**
Felony: 5 years/ $25,000 *regardless of the dollar amount of aggregate loss.*
A person who commits an act ***that interrupts or impairs the functioning of a PSAP***
Felon: to 10 years /$50,000 *regardless of the dollar amount of aggregate loss.*

WITH HB444 *(the broader bill)*
Above listed penalties apply to ***PSAP and all other CRITICAL (cyber) INFRASTRUCTURE*** *as the bill defines.*