HB444 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 444: Criminal Law – Interference With Critical Infrastructure Or 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 444: Criminal Law – Interference With Critical Infrastructure Or A Public Safety Answering Point – Penalties**.

The MSFA is in full support of HB 444. 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. Adding Critical Infrastructure will strengthen the existing law. This law also provides punishment for someone who "intends" to deny access to an authorized user or interrupt or impair the function of critical infrastructure or a PSAP.

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

Letter for HB444.pdf
Uploaded by: Mike McKay
Position: FAV

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

Judicial Proceedings Committee
Executive Nominations Committee

Joint Committees
Administrative, Executive, and Legislative Review
Children, Youth, and Families
Program Open Space and Agricultural Land Preservation

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Annapolis Office
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

Cumberland Office
100N Mechanic Street
Cumberland, Maryland 21502
240-362-7040

Williamsport Office
2N Conococheque Street
Williamsport Town Hall
Williamsport, Maryland

January 24, 2025

RE: Fire/EMS Coalition Support for HB444

Dear Chairman Clippinger, Vice Chair Bartlett, and Members of the Committee,

The Fire/EMS Coalition would like to express their support for House Bill 444:
Criminal Law – Interference with Critical Infrastructure or a Public Safety Answering Point – Penalties. This bill will prohibit an individual from taking certain actions with the intent to deny access to an authorized user or interrupt or impair the functioning of critical infrastructure or a public safety answering point. This bill will also prohibit an individual from taking certain actions to deny access to an authorized user, interrupt, or impair the functioning of critical infrastructure/public safety answering point. There will be authorizations for penalties for the aforementioned violations.

The Fire/EMS Coalition supports House Bill 444 as it will penalized those who are obstructing the carrying out of first responders' duties.

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 Firefighter'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.

HB0444-JUD_MACo_SUP.pdf
Uploaded by: Sarah Sample
Position: FAV

House Bill 444

Criminal Law – Interference With Critical Infrastructure or 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 444. This bill bolsters protections against cyberattacks targeting 9-1-1 centers and other critical infrastructure, which are vital components of Maryland's emergency response framework. By addressing these evolving threats, the bill enhances the security and stability of the 9-1-1 system and other infrastructure, ensuring continued public safety and reliable services.

Maryland's transition to Next Generation 9-1-1 (NG911) modernizes emergency communication capabilities, enabling faster and more accurate emergency response. Additionally, government infrastructure for fiscal management, public health, and public safety have migrated to digital infrastructure to enhance service delivery for residents. However, these advanced systems face significant cybersecurity threats as hackers increasingly target public infrastructure networks. HB 444 strengthens state law by expressly prohibiting acts intended to impair or disrupt the functionality of these programs − deterring these malicious attacks and safeguarding Maryland's crucial infrastructure.

The bill increases penalties for individuals who intentionally disrupt certain government infrastructure that could result in serious public harm. 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 health and safety.

Counties operate and fund digital infrastructure that enables them to provide necessary services to residents statewide. A cyberattack or disruption to these programs 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 state and local 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 444.

MD 2025 HB 444 Columbia Gas Testimony Final.pdf
Uploaded by: Scott Waitlevertch
Position: FAV

Columbia Gas of Maryland
A NiSource Company

SUPPORT – House Bill 444
Interference With Critical Infrastructure or a Public Safety Answering Point -- Penalties
House Judiciary Committee

Columbia Gas of Maryland, Inc. (Columbia) supports HB 444 as introduced. The legislation amends Maryland law to prohibit a person from denying access to or impairing the functioning of critical infrastructure, which Columbia interprets to include natural gas utility equipment, facilities and pipelines. Under the proposed legislation, a person who denies access or impairs the functioning of critical infrastructure is guilty of a felony and subject to imprisonment or a fine or both.

Columbia supports public policies protecting its equipment, facilities and pipelines from attack or interference. Ensuring we can safely and reliably provide energy to our customers is our priority. Columbia works with industry, federal and state agencies and organizations to develop standards and best practices to manage cybersecurity risks and to promote the protection of our critical infrastructure.

Unfortunately, there have been attacks on utility facilities and infrastructure. These attacks can be carried out by various actors including terrorists, extremist groups, disgruntled individuals, nation-states seeking to destabilize a region, or criminals aiming to disrupt operations for personal gain.

Recent examples include shooting incidents at power substations in the United States where individuals have targeted electrical substations with gunfire, causing power outages. There has also been vandalism of energy infrastructure where unknown actors have deliberately damaged electrical equipment or transformers. According to an April 2024 report by POLITICO's E&E News, analysis of Department of Energy data showed the nation's power providers reported 185 instances of mostly physical attacks or threats against critical grid infrastructure in 2023, beating the previous record number of reports from 2022.

In addition, in October 2024 the U.S. Department of Homeland Security (DHS) highlighted in its 2025 Homeland Threat Assessment (HTA) that domestic and foreign adversaries are almost certain to continue posing threats to the integrity of the nation's critical infrastructure over the next year. This is partly because they believe that targeting these sectors could have widespread effects on U.S. industries and the standard of living.

Mitigating attacks and interference with critical infrastructure is a joint effort between at-risk industries and federal, state and local governments. Legislation such as HB 444 can assist in the possible prevention of future attacks and interference of critical infrastructure.

Columbia believes the requirements of House Bill 444 are appropriately and reasonably crafted policies related to the protection of Maryland's critical infrastructure and supports the legislation as introduced.

.

February 4, 2025

Contact:
Carville Collins
(410) 332-8627
carville.collins@saul.com

Contact:
Scott Waitlevertch
(724) 888-9774
swaitlevertch@nisource.com

HB444_Susan Greentree Testimony_1-31-2025_Del Hill
Uploaded by: Susan Greentree
Position: FAV

HB444 Criminal Law – 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 Cell: 410-852-3362

257 Overleaf Drive, Arnold MD 21012-1947

I respectfully request HB444 - 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. HB444 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.

1) MD, Baltimore City 9-1-1 was attacked March 25th 2018, bringing down 9-1-1 operations.
2) MD, Baltimore City Gov't was attached in 2019.
3) MD, St Mary's County was 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.

The following page has data on several other Public Safety agencies that have been breached. **PLEASE** note the three 9-1-1 centers in California all hit the same day. As you can see, these criminals can shut down several 9-11 centers operations in little time. It is **CRITICAL** Maryland pass this legislation and hold those who disrupt the safety of Maryland residents accountable.

I urge you to vote YES for HB444

Thank you.

01-23-2024-PA-Bucks C...

STATUS
New

STATE
Pennsylvania

DELIVERY
Unknown

EXPLOIT
Ransomware

TARGET
Public Safety

TARGETED GROUP
Bucks County Department of Emergency Communications

COUNTY
Bucks

VENDOR/3RD PARTY?
No

IMPACTED VENDOR/3RD PARTY

ARTICLE DATE
1/23/2024

HEADLINE
Cybersecurity incident impacting Bucks County's emergency communication system

State
California

Delivery
Unknown

Exploit
Ransomware

Target
Public Safety

Targeted Group
Manhattan Beach

County
Los Angeles

Vendor/3rd party?
No

Impacted Vendor/3rd Party

Article Date
7/16/2024

Headline
911 services in parts of California come under cyber attack

Excerpt 1
California's 911 services have been disrupted by ransomware amid a spate of cyber attacks on the Golden State.

Excerpt 2

State
California

Delivery
Unknown

Exploit
Ransomware

Target
Public Safety

Targeted Group
Culver City

County
Los Angeles

Vendor/3rd party?
No

Impacted Vendor/3rd Party

Article Date
7/16/2024

Headline
911 services in parts of California come under cyber attack

Excerpt 1
California's 911 services have been disrupted by ransomware amid a spate of cyber attacks on the Golden State.

Excerpt 2

State
California

Delivery
Unknown

Exploit
Ransomware

Target
Public Safety

Targeted Group
Hermosa Beach

County
Los Angeles

Vendor/3rd party?
No

Impacted Vendor/3rd Party

Article Date
7/16/2024

Headline
911 services in parts of California come under cyber attack

Excerpt 1
California's 911 services have been disrupted by ransomware amid a spate of cyber attacks on the Golden State.

Excerpt 2

03-20-2024-MI-Branch ...

STATUS
New

STATE
Michigan

DELIVERY
Phishing

EXPLOIT
Malware

TARGET
Public Safety

TARGETED GROUP
Branch County

COUNTY
Branch

VENDOR/3RD PARTY?
No

IMPACTED VENDOR/3RD PARTY

ARTICLE DATE
3/20/2024

HEADLINE
Quincy pays county to clean malware off police computer

Crowdstrike History.pdf
Uploaded by: Terri Hill
Position: FAV

Cyberattacks on Infrastructure in the United States

Cyberattacks on critical infrastructure have increasingly become a major concern for national security. The **Colonial Pipeline ransomware attack** in May 2021, carried out by the Russian-linked group DarkSide, disrupted fuel supplies across the East Coast for **six days** and caused panic buying of gasoline. The attack cost the company **$4.4 million in ransom**, though only part of it was recovered, and it is considered one of the most destructive cyberattacks on U.S. energy infrastructure to date (Reuters, 2025a). No deaths were reported, but the economic disruption was widespread, highlighting vulnerabilities in energy systems.

Similarly, the **Stuxnet worm** of 2010, a sophisticated cyber weapon likely developed by the United States and Israel, targeted Iran's nuclear facilities and set a precedent for industrial sabotage. While not directly targeting U.S. systems, it underscored the potential for cyberattacks to disrupt critical infrastructure globally (Politico, 2024).

In the **2017 WannaCry ransomware attack**, hospitals across the globe, including some in the U.S., were paralyzed. Medical devices were rendered unusable, and surgeries were postponed, demonstrating the risk to healthcare systems. British hospitals reported **deaths from delayed care**, though the exact numbers remain uncertain (Food and Wine, 2025). In the U.S., flights were also grounded during various cyber incidents, such as a ransomware attack in 2021 that affected the IT systems of the Federal Aviation Administration (FAA) (Reuters, 2025a).

Water and wastewater systems are also at significant risk. The Environmental Protection Agency found that water systems serving **193 million people** are vulnerable to cyberattacks. Such incidents could result in the contamination or shutdown of drinking water supplies (Food and Wine, 2025).

The U.S. government has responded with initiatives such as the **Cybersecurity and Infrastructure Security Agency (CISA)** and the **National Cybersecurity Strategy**, which emphasize mandatory reporting of cyber incidents and public-private collaboration to bolster defenses (Rand Corporation, 2024).

Cyberattacks on Infrastructure in Maryland

Maryland, with its proximity to Washington, D.C., and concentration of federal agencies, remains a prominent target for cyberattacks. The **2019 Baltimore ransomware attack**, executed by a group called RobbinHood, lasted **over two weeks**, locking city systems and preventing access to email and payment portals. The city refused to pay the **$76,000 ransom** but spent **$18 million** on recovery and rebuilding IT infrastructure (Politico, 2024). No deaths occurred, but critical city services were severely disrupted. Baltimore County Public Schools suffered a ransomware attack in 2020 during the COVID-19 pandemic, which disrupted online learning for **115,000 students** for nearly a week. The attack highlighted the vulnerabilities of educational systems during a critical time for remote learning (ODNI, 2024).

Healthcare systems in Maryland are also frequent targets. Hospitals within the University of Maryland Medical System have faced ransomware attacks that **temporarily shut down critical IT systems**,

delaying care and increasing risks to patients during high-demand periods (Maryland Attorney General, 2024).

Maryland's **Maryland Cybersecurity Council** has spearheaded efforts to strengthen the state's defenses, including mandating stronger cybersecurity practices for state agencies. Additionally, the Maryland Air National Guard's **Cyber Fortress 3.0** training exercise tested responses to potential attacks on power grids and water systems (National Guard, 2024).

The University of Maryland's START program has been instrumental in developing a dataset on cyberattacks targeting critical infrastructure, offering insights into regional and national trends. These efforts are supported by **$6.5 million in state and federal funding** aimed at bolstering local cybersecurity capabilities (Raskin House, 2024).

CrowdStrike's Role in Cybersecurity and Addressing Cyberattacks

CrowdStrike, a leading cybersecurity company founded in 2011, has played a pivotal role in identifying and mitigating cyber threats against critical infrastructure in the United States and globally. CrowdStrike is best known for its **Falcon platform**, which provides AI-driven, cloud-native endpoint protection and advanced threat intelligence.

Key Incidents and CrowdStrike's Role

1. Democratic National Committee (DNC) Hack (2016):
    - CrowdStrike was instrumental in attributing this hack to two Russian state-backed groups, Cozy Bear and Fancy Bear, linked to the Russian intelligence agencies (Reuters, 2025a).
    - The hack persisted over several months before detection.
    - The attack exposed sensitive emails and influenced political narratives during the U.S. presidential election.
    - The fallout included reputational damage and financial costs associated with improved cybersecurity measures.
    - No deaths occurred, but the incident emphasized the potential for cyberattacks to disrupt democratic processes.
2. Healthcare and Hospital Attacks:
    - CrowdStrike has been involved in addressing ransomware attacks on healthcare systems, including the WannaCry attack in 2017, which disrupted hospital operations globally.
    - Medical devices were rendered inoperable, critical surgeries were delayed, and some treatment interruptions were linked to patient deaths (Food and Wine, 2025).
    - The global cost of WannaCry exceeded $4 billion.
3. Colonial Pipeline Attack (2021):
    - CrowdStrike contributed to understanding the tactics of the DarkSide group, a ransomware collective responsible for the attack.
    - The attack lasted six days, causing fuel shortages across the East Coast.
    - Colonial Pipeline paid $4.4 million in ransom, although some of it was recovered later (Reuters, 2025a).

    - No direct fatalities were reported, but the incident highlighted the risks of delayed emergency responses due to fuel shortages.
4. Microsoft Outage and Air Travel Delays (2023):
    - While CrowdStrike did not directly attribute the cause of the outage, it investigated disruptions stemming from vulnerabilities in cloud-based systems.
    - The outage disrupted critical systems for several hours globally.
    - More than 3,500 flights were delayed, and airline communication systems were temporarily disabled (NBC Washington, 2023).
    - Banks, airlines, and global companies faced service disruptions, highlighting the cascading effects of cloud-based system vulnerabilities.
5. Aviation and Transportation Attacks:
    - CrowdStrike has monitored and mitigated cyber threats against aviation systems, such as ransomware attacks on the FAA in 2021 that grounded dozens of flights.
    - These incidents caused economic losses and logistical challenges for airlines and passengers (Reuters, 2025a).

Broader Impact of CrowdStrike on Cybersecurity

- Detection and Response:
    - CrowdStrike's Falcon OverWatch continuously monitors and detects threats in real time, providing rapid response to mitigate damages.
    - The platform uses behavioral analytics and AI to identify potential attacks before they escalate.
- Cost Savings and Prevention:
    - Organizations leveraging CrowdStrike's services often avoid the multimillion-dollar costs associated with ransomware payments and operational downtime.
    - CrowdStrike assists companies in avoiding indirect costs such as legal fees, reputational damage, and customer attrition.
- Public-Private Collaboration:
    - CrowdStrike collaborates with government agencies, including the FBI and Department of Homeland Security (DHS), to share intelligence on cyber threats.
    - The company has participated in national efforts to safeguard elections, critical infrastructure, and corporate assets.
- Impact on Maryland:
    - Given Maryland's role as a cybersecurity hub, CrowdStrike engages with institutions like the NSA, Cyber Command, and regional entities to bolster local cyber defenses.
    - The company contributes to cybersecurity workforce development through partnerships with academic institutions such as the University of Maryland.

References

1. NBC Washington. (2023). Microsoft Outage Disrupts Flights, Banks, Companies Globally. Retrieved from https://www.nbcwashington.com
2. Food and Wine. (2025). EPA Finds the Drinking Water for 193 Million People in the U.S. Is Vulnerable to Cyberattacks. Retrieved from https://www.foodandwine.com
3. Maryland Attorney General. (2024). Maryland Cybersecurity Council Interim Report. Retrieved from https://www.marylandattorneygeneral.gov
4. National Guard. (2024). Maryland Airmen Test Cyber Skills in Virginia Exercise. Retrieved from https://www.nationalguard.mil
5. ODNI. (2024). Recent Cyber Attacks on U.S. Infrastructure. Retrieved from https://www.dni.gov
6. Politico. (2024). U.S. Allies Accuse Russia of Cyberattacks. Retrieved from https://www.politico.com
7. Rand Corporation. (2024). Threats to America's Critical Infrastructure. Retrieved from https://www.rand.org
8. Raskin House. (2024). Maryland Delegation Announces Funding to Enhance Cybersecurity. Retrieved from https://raskin.house.gov
9. Reuters. (2025a). As China Hacking Threat Builds, Biden to Order Tougher Cybersecurity Standards. Retrieved from https://www.reuters.com
10. Reuters. (2025b). U.S. Has Responded to Chinese-Linked Cyberattacks. Retrieved from https://www.reuters.com
11. START. (2024). Dataset on Cyberattacks Against Critical Infrastructure. Retrieved from https://www.start.umd.edu

Cybersecurity Laws by State (JRL 1.15.25).pdf
Uploaded by: Terri Hill
Position: FAV

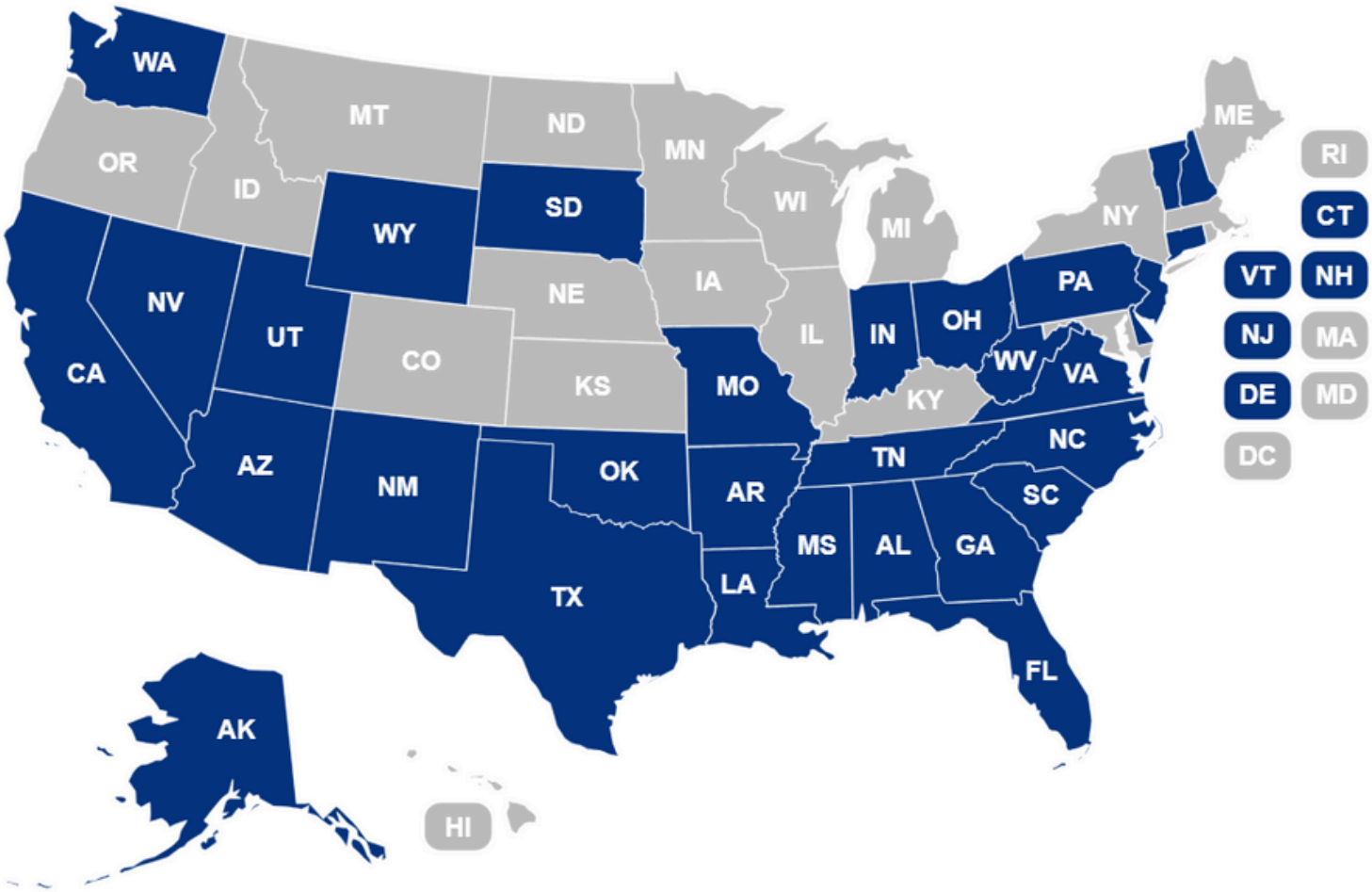
CYBERSECURITY LAWS BY STATE

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

Cybersecurity Laws by State (JRL 1.15.25).pdf
Uploaded by: Terri Hill
Position: FAV

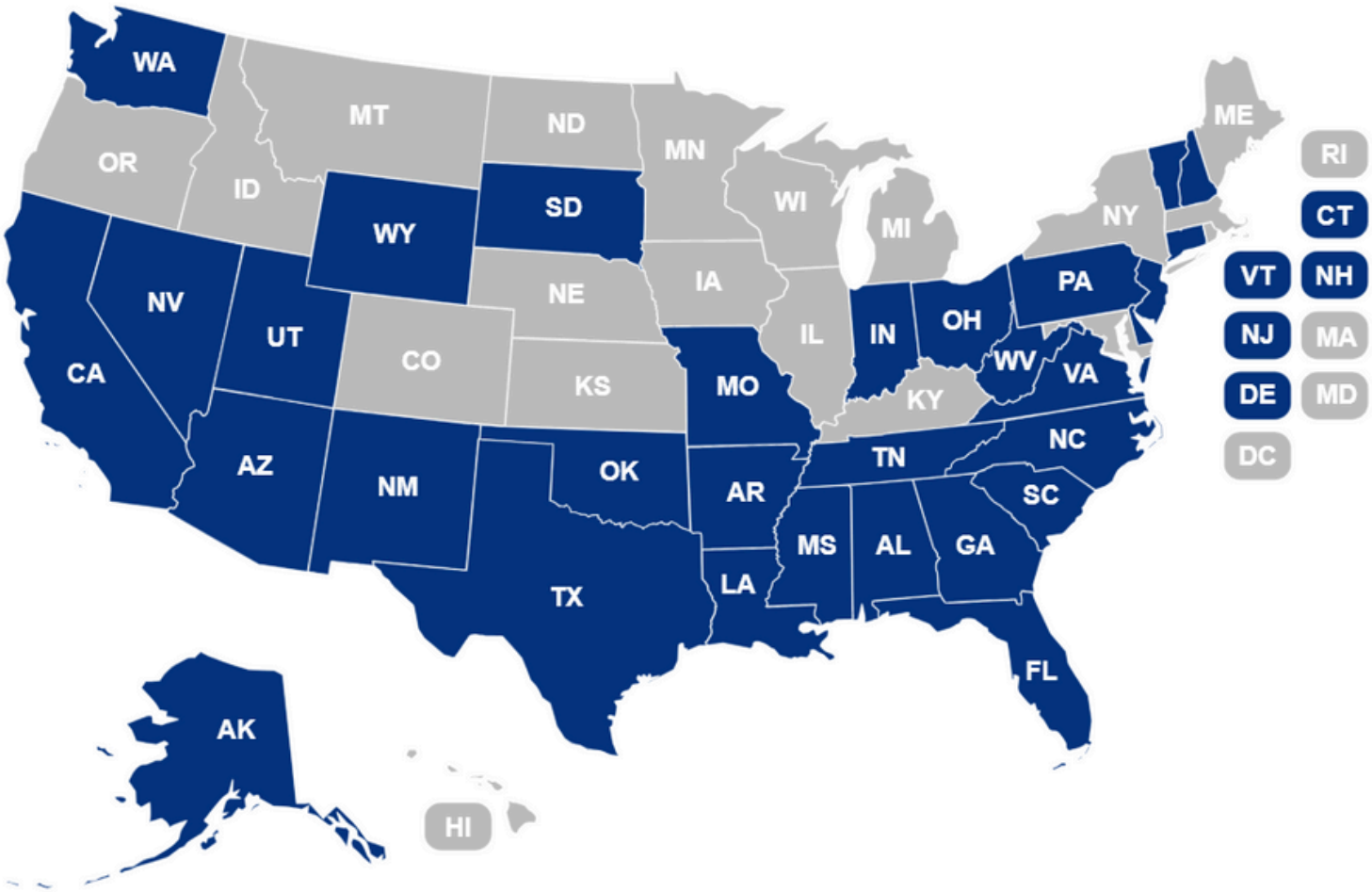
CYBERSECURITY LAWS BY STATE

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 444 (DDOS) 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 – HB444 CRIMINAL LAW – PUBLIC SAFETY – INTERFERENCE WITH CRITICAL INFRASTRUCTURE OR PUBLIC SAFETY ANSWERING – PENALTIES

February 4, 2025

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

HB444 strengthens existing protections of the broad range of critical communications infrastructure against the increasing number of cyber and other threats, by creating specific penalties for those who seek to undermine these systems by intentional actions aimed at disrupting or impairing their function. **HB444**, a recommendation of the Next Gen 9-1-1 Commission and a 2022 Judiciary and Judicial Proceedings Workgroup, informed by prior local and national cyberattacks, aims to deter future bad actors and improve accountability. It broadens the type of digital systems subject to penalties beyond 9-1-1 systems known as Public Service Answering Points (PSAPs), which is the subject of a separate bill, HB445, which passed this committee and the House 135-0 in 2023 and 141-0 in 2024.

In Maryland, the 2019 Baltimore ransomware attack disabled city systems for weeks, disrupting essential services and costing $18 million in recovery efforts. A Baltimore County Public Schools 2020 attack halted remote learning for 115,000 students, highlighting the vulnerabilities of our educational systems. In 2023, a Microsoft outage stemming from vulnerabilities in cloud-based systems disrupted critical operations globally for hours, delaying over 3,500 flights, temporarily disabling airline communication systems, and causing widespread service interruptions for banks, airlines, and major corporations. The 2021 Colonial Pipeline ransomware attack disrupted East Coast fuel supplies for almost a week, costing over $4 million and sparking widespread economic and public safety concerns. The cost of the ransomware attack on the Maryland Department of Health, for which there was a rapid response that preserved data security took nearly two years for system recovery at immeasurable human cost. These incidents exemplify the profound impact cyberattacks can have on government operations, communities, and individuals.

HB444

- defines “CRITICAL INFRASTRUCTURE” as both physical or virtual systems and assets, vital to the state, county, or municipality for which incapacitation or destruction of one or more components would have a debilitating impact on public security, economic security, public health, or public safety.
- explicitly targets modern cyber threats, including ransomware and denial-of-service attacks, ensuring that Maryland's laws remain aligned with current and emerging risks.
- creates a felony with clear, enforceable penalties of up to **5 years and up to $25,000** or both for actions **intending** to and **up to 10 years and up to $50,000** or both for actions which succeed in interrupt or impair the functioning of critical infrastructure with malicious intent.

While federal initiatives like CISA and companies like CrowdStrike have advanced cybersecurity, they do not and cannot ensure security to these systems. In fact, CrowdStrike software update was itself subject to

a July 2024 attack causing a widespread IT outage that affected millions of Windows computers worldwide.

HB444 is an essential deterrence, response, and accountability tool needed to protect Maryland's critical infrastructure and better safeguard the health, safety, and security of our residents.

I ask for a favorable report on **HB444**.

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.*

FirstEnergy FAV HB-444 - Critical Infrastructure.p
Uploaded by: Timothy Troxell
Position: FAV

Timothy R. Troxell, CEcD
Senior Advisor, Government Affairs
301-830-0121
ttroxell@firstenergycorp.com

10802 Bower Avenue
Williamsport, MD 21795

SUPPORT – House Bill 0444
Criminal Law – Interference with Critical Infrastructure or a Public Safety Answering Point – Penalties
Judiciary Committee
Tuesday, February 4, 2025

Potomac Edison, a subsidiary of FirstEnergy Corp., serves approximately 285,000 customers in all or parts of seven Maryland counties (Allegany, Carroll, Frederick, Garrett, Howard, Montgomery, and Washington). FirstEnergy is dedicated to safety, reliability, and operational excellence. Its ten electric distribution companies form one of the nation's largest investor-owned electric systems, serving customers in Ohio, Pennsylvania, New Jersey, New York, West Virginia, and Maryland.

Favorable

Potomac Edison / FirstEnergy strongly supports House Bill 0444 - *Criminal Law – Interference with Critical Infrastructure or a Public Safety Answering Point – Penalties*. This legislation addresses threats to actions intended to obstruct the access to, or operation of, critical infrastructure by codifying both its definition as well as the penalty for violations.

Potomac Edison / FirstEnergy requests a Favorable report on HB-444. Enhancing the security and reliability of Maryland's critical infrastructure, particularly the electric grid that serves our communities, is crucial.

The electric grid is a vital component of Maryland's critical infrastructure. It ensures the continuous delivery of electricity to homes, businesses, government agencies, and other essential services. Any intentional interference with the network could lead to significant disruptions – which can then affect public safety, economic stability, and the well-being of our customers.

House Bill 0444 aims to strengthen the legal protections against actions that intentionally disrupt or impair critical infrastructure operations. By prohibiting such actions and establishing penalties for violations, the bill serves as a deterrent against malicious activities targeting essential services. The proposed legislation also aligns with industry efforts to safeguard critical infrastructure. It complements existing measures by providing a legal framework to address intentional disruptions, thereby supporting our ability to maintain reliable electric service.

Potomac Edison / FirstEnergy believes House Bill 0444 takes a necessary step toward ensuring the security and resilience of Maryland's critical infrastructure. Given the sensitive nature of utility critical infrastructure, the need to deter actions that may harm it, and the benefits of having clearly defined penalties for taking such actions, we urge the committee to support this bill. We appreciate your consideration of our perspective on this issue and believe that protecting the essential services upon which our communities depend is vital.

For the above reasons, Potomac Edison / FirstEnergy respectfully request a Favorable vote on HB-444.

Letter on MD HB444 re cybersecurity.pdf
Uploaded by: Matthew Bohle
Position: INFO

February 4, 2025

TO: House Judiciary Committee
FROM: Colonial Pipeline
RE: HB 444
POSITION: Informational only

To Chair Clippinger, Vice Chair Bartlett, Committee members and Delegate Hill,

The purpose of this letter is to provide information and recommendations regarding HB 444 related to penalties for interference with critical infrastructure.

Colonial Pipeline Company operates an interstate pipeline system that delivers refined products such as gasoline, jet fuel, and diesel fuel into 14 States, including Maryland. Colonial maintains over 300 miles of pipeline in Maryland; operates a major storage and distribution facility in Carroll County; and directly serves BWI airport.

Colonial generally supports initiatives like HB 444 that increase penalties for interfering with critical infrastructure, but we believe HB 444 could be improved. HB 444 contains a definition of "critical infrastructure" that differs from language adopted just last year through SB No. 474. While the law passed last year was focused on certain generating units or facilities, the definition of critical infrastructure was significantly broader than that contained in HB 444. It accomplished this by encompassing in its critical infrastructure definition "…assets, systems and networks, whether physical or virtual, *considered by the U.S. Department of Homeland Security* to be so vital to the United States…." [Emphasis added.] Colonial believes that bringing the definition in HB 444 into alignment with what was enacted last year would reduce the possibility of interpretative confusion or conflicts in the future.

Colonial appreciates your introducing HB 444 and raising awareness of this issue. We look forward to working with you and the Committee on this topic in the future.

Sincerely,

/Philip A. Squair/

Philip A. Squair
Senior Government Affairs Advisor
psquair@colpipe.com
470-330-5099 (m)