REPORT OF THE TASK FORCE TO STUDY THE PRACTICE KNOWN AS "SWATTING"

FEBRUARY 2023

ADL®
WASHINGTON, D.C.

February 9, 2023

Governor Wes Moore
State House
100 State Circle
Annapolis, MD 21401

Senate President Bill Ferguson
State House, H-107
100 State Circle
Annapolis, MD 21401

House Speaker Adrienne A. Jones
State House, H-101
100 State Circle
Annapolis, MD 21401

RE: Report of the Task Force to Study the Practice Known as "Swatting"

Governor Moore, Senate President Ferguson, and House Speaker Jones,

Attached you will find the final Report of the Task Force to Study the Practice Known as "Swatting." During the 2022 General Assembly, **Senate Bill 881, Task Force to Study the Practice Known as "Swatting"** passed unanimously in both the Senate and House and was signed by then Governor Hogan. Swatting has become a serious problem nationwide and Maryland has also seen an increase in incidents where there is a deliberate and malicious act of reporting a false violent crime or emergency. This has resulted in a grave misuse of government emergency response resources, serious bodily harm to targets, and severe emotional distress to victims.

The task force was directed to study the current laws applicable and make recommendations relating to legislative changes to prohibit the practice of swatting. Members of the task force met several times throughout the Fall and early Winter of 2022 to review current laws and came to the understanding that the law in Maryland has not kept pace nor does it have a swatting-specific law on the books. The task force went to great lengths in our discussions to consider how to address this problem by holding swatting perpetrators responsible, empowering victims, and establishing appropriate guidelines for criminal penalties that reflect the severity of incidents and future incidents.

ADL®
WASHINGTON, D.C.

Throughout the report you will find examples of Maryland based swatting incidents and why current laws must be updated. Starting on Page 10 you will find a set of recommendations on how Maryland can enact a freestanding swatting-specific criminal prohibition. Two cross-filed bills have now been introduced in the 2023 legislative session with these recommendations. Senate Bill 340/House Bill 745, Criminal Law – False Statements – Emergency or Commission of Crime (Antiswatting Act of 2023), which if passed will implement the task force recommendations. Task force members Senators Cheryl Kagan and Jeff Waldstreicher and Delegates Lesley Lopez, Sandy Bartlett and Rachel Muñoz are all co-sponsors on these bills.

As you may know, the ADL (the Anti-Defamation League) is a leading anti-hate organization founded in 1913 with a mission to "stop the defamation of the Jewish people and to secure justice and fair treatment to all." Today, ADL continues to fight all forms of antisemitism and bias, using innovation and partnerships to drive impact. A global leader in combating antisemitism, countering extremism and battling bigotry wherever and whenever it happens, ADL works to protect democracy and ensure a just and inclusive society for all.

Therefore, it has been my honor to serve as the Chair of this task force because the issue of swatting has been something ADL has seen ravaging our marginalized communities. We feel strongly that we must protect vulnerable groups against actions of online hate and harassment like swatting. 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.

The task force members listed on Page 19 brought together expertise from law enforcement, the legislature, the public defender, the Maryland state's attorney, and the ADL. Important discussions were held so that Maryland can continue to be a leader in the fight against hate.

Please do not hesitate to contact me with any questions related to the task force report. I look forward to robust discussions during the legislative

hearings on these bills. It is vital we work together to ensure that swatting becomes something perpetrators are held accountable for, and no one faces being a victim again.

Sincerely,

Meredith R. Weisel
ADL Washington, D.C. Regional Director
mweisel@adl.org
301-437-2554

TABLE OF CONTENTS

INTRODUCTION

"Swatting" is the deliberate and malicious act of reporting a false violent crime or emergency to evoke an aggressive response from a law enforcement agency to a target location.[1] The falsely reported threat is designed to be sufficiently alarming so as to prompt a heightened response from law enforcement, such as by a Special Weapons and Tactics (SWAT) team.[2]

Exploitation of the 911 emergency system via swatting places the target, emergency responders, and innocent bystanders at risk physically and emotionally. In addition to those risks, swatting diverts resources from legitimate emergencies. A single incident can cost a law enforcement agency an estimated $15,000 to $100,000.[3] Despite law enforcement's best efforts, swatting calls can be difficult to identify as false because the callers use

---

[1] Anti-Defamation League: Center for Technology and Society, *What is Swatting?* (Aug. 18, 2022), https://www.adl.org/resources/blog/what-swatting?gclid=EAIaIQobChMI9PXYnvmr_AIVSkpyCh3P6gUAEAAYASAAEgIXNPD_BwE (hereinafter "ADL"); *see also Dobbs v. Townsend*, 416 F. Supp. 3d 441, 445 (D. Md. 2019) (describing "swatting" as "the act of placing a 911 call in which a false report of a violent crime is made to elicit a police . . . [SWAT] response to the physical address of a targeted individual") (cleaned up).

[2] Federal Bureau of Investigation (FBI): Stories, *The Crime of 'Swatting': Fake 9-1-1 Calls Have Real Consequences*, (Sept. 3, 2013), https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences1 (hereinafter "FBI: Stories"); ADL, *supra* note 1.

[3] ADL, *supra* note 1.

technology, such as Caller Identification ("ID") spoofing, social engineering, and TTY to make it appear as though a call is coming from a legitimate source, like the target's phone.[4]

Swatting first gained notoriety in online communities.[5] One notable variation involved a gamer targeting a rival's residence while the rival was livestreaming. Because the target was mid-livestream, law enforcement's response to the false report was broadcast via the internet.[6]

Swatting, however, quickly moved beyond the online community.[7] The range of swatting targets has expanded to include public places, particularly schools.[8] Likewise, the motive behind swatting has expanded; it is now used to ambush

---

[4] FBI Las Vegas, *FBI Las Vegas Federal Fact Friday: The Dangers of Swatting* (Sept. 23, 2022), https://www.fbi.gov/contact-us/field-offices/lasvegas/news/press-releases/fbi-las-vegas-federal-fact-friday-the-dangers-of-swatting (hereinafter "FBI Las Vegas").

[5] Nathan Grayson, *Twitch streamers traumatized after four 'swattings' in a week,* THE WASHINGTON POST, Aug. 15, 2022, https://www.washingtonpost.com/video-games/2022/08/15/keffals-adin-ross-ishowspeed-swatting-twitch-youtube/ ("Swatting is not a new trend and has been deployed against numerous gamers, internet users and content creators for well over a decade."); Odette Yousef, *False calls about active school shooters are rising. Behind them is a strange pattern*, NPR: NATIONAL SECURITY (Oct. 7, 2022), https://www.npr.org/2022/10/07/1127242702/false-calls-about-active-shooters-at-schools-are-up-why.

[6] Grayson, *supra* note 5; ADL, *supra* note 1.

[7] FBI Las Vegas, *supra* note 4.

[8] *See*, *e.g.*, Martin Weil, *False Reports of violence Monday at area schools, authorities say*, THE WASHINGTON POST (Sept. 19, 2022), https://www.washingtonpost.com/local/public-safety/false-reports-of-violence-mondaty-at-area-schools-authorities-say/2022/09/19/bbc7a830-3877-11ed-9f55-b65f1323f2f_story.html.

individuals, often vulnerable ones, as a form of revenge,[9] harassment, or intimidation.[10] Regardless of the location or the motive, the common thread throughout swatting incidents is that the bad actor attempts to exploit law enforcement and weaponize it against the target.

Over the last decade, there has been a significant uptick in swatting incidents nationwide.[11] While there are no national statistics tracking how many swatting incidents occur yearly, it is estimated that the number has more than doubled, up from approximately 400 cases nationwide in 2011, to 1,000 incidents in 2019.[12] A National Public Radio investigation found 113 instances of "hoax calls targeting schools across 19 states" in September 2022 alone.[13]

Maryland has not been spared from this trend.

---

9 FBI: Stories, *supra* note 2.

10 FBI Las Vegas, *supra* note 4.

11 Ethan Ehrenhaft, *Officials say threats at River Hill High are hoax originating from outside the United States*, BALTIMORE SUN (Oct. 12, 2022), https://www.baltimoresun.com/maryland/howard/cng-ho-river-hill-threat-20221012-sbmaoelnrretnbrd7z7sg6bt6a-story.html.

12 ADL, *supra* note 1.

13 Yousef, *supra* note 5.

MARYLAND-BASED SWATTING INCIDENTS

Some examples of Maryland-related swatting incidents are highlighted below.

In 2015, a person seeking revenge against Tyran Dobbs falsely claimed to be armed and holding three hostages at Dobbs's home in Howard County, Maryland.[14] The Howard County Police Department responded to the call and evacuated the apartment building.[15] After speaking with a negotiator, an unarmed Dobbs went to the door, but failed to keep his hands up as ordered by the police.[16] When he attempted to retreat to his apartment, a police officer shot him with rubber bullets, hitting him in the torso and face.[17]

In 2019, Pulitzer Prize winning newspaper columnist Leonard G. Pitts was the target of a swatting incident in Bowie, Maryland.[18] The police received a call from a blocked number claiming that someone was "being murdered" in Pitts's house. The

---

14 *Dobbs*, *supra* note 1.
15 *Id.* at 445.
16 *Id.* at 446.
17 *Id.*
18 Martin Weil, *Columnist Leonard Pitts Jr. says hoax 911 call sent police to his Md. home*, WASHINGTON POST (July 9, 2019), https://www.washingtonpost.com/local/public-safety/columnist-handcuffed-in-bowie-after-police-get-false-information-authorities-say/2019/06/30/32ef85cc-9baa-11e9-85d6-5211733f92c7_story.html.

police ordered Pitts, who was sleeping when they arrived, out of the home and handcuffed him while they investigated.[19]

In October 2022, the Howard County Police Department received two false threats concerning River Hill High School in Clarksville, Maryland, which prompted the school to be locked down.[20] In one of the calls, the caller falsely reported that a student was armed with a gun and a bomb.[21] Four students, who were not responsible for the threat, were handcuffed in the school while the police investigated.[22]

Recently, in December 2022, a 17-year-old Marylander triggered three swatting incidents in Florida as retaliation against another minor in relation to an online dispute.[23] The Maryland teen falsely and repeatedly reported that violent crimes involving a firearm were occurring at an address he mistakenly believed corresponded to the target.[24] Each time, approximately ten to 12

---

19 *Id.*

20 Ehrenhaft, *supra* note 11.

21 *Id.*

22 *Id.*

23 Kate Hussey & Scott Sutton, *Maryland teen arrested after 3 'swatting' calls made in Port St. Lucie: Fake calls said there were violent crimes involving firearm*, WPTV (Dec. 27, 2022), https://www.wptv.com/news/treasure-coast/region-st-lucie-county/port-st-lucie/maryland-teen-arrested-after-3-swatting-calls-made-in-port-st-lucie.

24 *Id.*

officers responded to the innocent bystanders' home, expending a "substantial number of resources."[25] The teen was taken into custody and is facing charges in Maryland.[26]

CURRENT MARYLAND LAW

Currently, in Maryland, there are no swatting-specific laws. Under Maryland's current laws, a swatting-type situation would most likely constitute the misdemeanor offense of making a false statement to a public official concerning a crime or hazard under Section 9-503 of the Criminal Law Article. That statute prohibits a person from making, or causing to be made, "a statement or report that the person knows to be false as a whole or in material part to an official or unit of the State or of a county, municipal corporation, or other political subdivision of the State that a crime has been committed or that a condition imminently dangerous to public safety or health exists, with the intent that the official or unit investigate, consider, or take action in connection with that

[25] *Id.*
[26] *Id.*

statement or report."[27] This offense carries a maximum penalty of up to six months' incarceration and a fine of up to $500.[28]

Maryland also has a more general statute that prohibits false statements to a law enforcement officer. A person commits the offense of making a false statement to a law enforcement officer by making, or causing to be made, "a statement, report, or complaint that the person knows to be false as a whole or in material part, to a law enforcement officer of the State, of a county, municipal corporation, or other political subdivision of the State, or of the Maryland-National Capital Park and Planning Police with intent to deceive and to cause an investigation or other action to be taken as a result of the statement, report, or complaint."[29] This offense is also a misdemeanor punishable by up to six months' incarceration and a fine of up to $500.[30]

Often, swatting incidents are motivated by bias.[31] Effective October 1, 2022, false statements that violate Section 9-501 of the Criminal Law Article that are "[m]otivated either in whole or

---

27 Md. Code Ann., Crim. Law § 9-503(a) (2002).
28 *Id.*
29 Md. Code Ann., Crim. Law § 9-501(a) (2022).
30 Md. Code Ann., Crim. Law § 9-501(b) (2022).
31 Grayson, *supra* note 5; ADL, *supra* note 1.

substantial part by another person's or group's race, color, religious beliefs, sexual orientation, gender, gender identity, disability or national origin, or because another person or group is homeless" constitute a felony hate crime punishable by up to 10 years' incarceration and a fine of up to $10,000.[32] If, however, the bias-motivated false statement results in the death of the victim, the penalty is increased to a maximum sentence of 20 years' incarceration and a fine of up to $20,000.[33]

In some instances, swatting may involve the false report of a destructive device. In those cases, that conduct likely amounts to the crime of making a false report involving a destructive device or toxic material, which is classified as a freestanding felony offense under Section 9-504 of the Criminal Law Article, and is punishable by up to 10 years' incarceration and a fine of up to $10,000.

Although restitution is part of a criminal sentence,[34] Maryland's current restitution statute does not appear to give a governmental unit the ability to obtain restitution for the cost

---

[32] Md. Code Ann., Crim. Law § 10-304(1)(iv), 2(i) (2022); Md. Code Ann., Crim. Law § 10-306(b)(1) (2022).

[33] Md. Code Ann., Crim. Law § 10-306(b)(2) (2022).

[34] *Chaney v. State*, 397 Md. 460, 470 (2007).

incurred in responding to a swatting incident. A governmental unit can only obtain restitution for expenses incurred "in removing, towing, transporting, preserving, storing, selling, or destroying an abandoned vehicle"—circumstances that are typically absent in a swatting-related incident.[35]

Read collectively, these statutes illustrate that, unless the false report is bias motivated or concerns a purported destructive device or toxic material, swatting constitutes only a misdemeanor offense punishable by up to six months' incarceration and a $500 fine with limited pecuniary risk.

THE PURPOSE OF THE TASK FORCE

Senate Bill 881 created the "Task Force to Study the Practice Known as 'Swatting'" ("Task Force"), which has been assigned three tasks. First, it is required to study the laws applicable to, and otherwise relating to, swatting.[36] Second, it is required to "make recommendations relating to legislative changes to prohibit" swatting.[37] Lastly, it must report its findings and

---

35 Md. Code Ann., Crim. Pro. § 11-603(a)(4) (2002).
36 Senate Bill 881(f)(1) (2022).
37 *Id.*

recommendations to the Governor and the General Assembly on or before June 1, 2023.[38]

RECOMMENDATIONS

After studying the current laws pertaining to swatting, both nationwide and locally, it is the Task Force's recommendation that Maryland enact a freestanding swatting-specific criminal prohibition.

Specifically, the offense should prohibit a person from making a "knowingly false report that is reasonably likely to cause a heightened emergency response from a law enforcement agency or other emergency responder," with at least "reckless disregard of causing bodily harm to any individual as a direct result of an emergency response to the report." By requiring a "knowingly false report," the offense would exclude good Samaritans reporting crimes that they genuinely believe are occurring that, ultimately, turn out to be unfounded. This intent element further ensures that

[38] *Id.*

the offense is not perceived as a strict liability offense, as strict liability offenses are generally disfavored in Maryland.[39]

The range of outcomes in swatting incidents is vast, and the penalties provided should reflect that reality. In some cases, no injury results, while in others, individuals are seriously injured or die.[40] If the knowingly false report results in death or serious bodily harm to another, the offense should be classified as a felony punishable by up to 10 years' imprisonment with a fine of up to $20,000. All other swatting acts, i.e., those in which no death or serious bodily injury occurs, should be classified a misdemeanor punishable by up to three years' imprisonment and a fine of up to $2,000. These proposed sentences are consistent with recent legislative trends, such as the Justice Reinvestment Act,[41] in that they eschew a mandatory minimum sentence.[42] These varied punishments, which differ based on the injury inflicted, resemble

---

[39] *See*, *e.g.*, *State v. McCallum*, 321 Md. 451, 456 (1991) (quoting *Dawkins v. State*, 313 Md. 638, 650 (1988)) (explaining that "'the contemporary view disfavors strict liability offenses'") (ellipses omitted).

[40] ADL, *supra* note 1.

[41] 2016 Md. Laws ch. 515.

[42] Governor's Office of Crime Control & Prevention of Maryland, *Justice Reinvestment Initiative Fact Sheet*, http://goccp.maryland.gov/wp-content/uploads/Maryland-Justice-Reinvestment-Initiative-Fact-Sheet.pdf.

the type of scaled punishments used in the recently enacted hate crimes statute.[43]

The statute should indicate that the penalty for the freestanding swatting offense stands separate from any sentence imposed for an underlying offense. This can be achieved by including a provision that specifies that a sentence imposed under the freestanding swatting offense may be separate from and consecutive to or concurrent with a sentence for any crime based on the act establishing a violation the statute.

Because swatting incidents are often bias-based, the statute should include a cross-reference to the hate crimes statute, Section 9-501 of the Criminal Law Article.

Special consideration was given to potential juvenile offenders. If not diverted, by default, cases involving juveniles who commit an act that would constitute the crime of swatting will originate in the juvenile court. The swatting offense should not be listed among the offenses that divest the juvenile court of original jurisdiction.[44] Allowing swatting-based delinquent acts to

---

[43] Md. Code Ann., Crim. Law § 10-306(b) (2022).
[44] Md. Code Ann., Cts. and Jud. Proc., § 3-8A-03(d)(2022).

originate in the juvenile court system accounts for children's "lack of maturity" and "underdeveloped sense of responsibility, leading to recklessness, impulsivity, and heedless risk-taking."[45] The juvenile system provides the flexibility needed to balance the objectives of securing the public's safety, holding the child accountable, and assisting the child in becoming a responsible and productive member of society.[46] The possibility of diversion for juveniles may be expressly stated in the statute so as to indicate a preference for that course in cases where it is appropriate.

SWATTING-RELATED ISSUES: TDOS AND DDOS

The public voice network has likewise become the target of many attacks, including Telephony Denial of Service (TDoS) and Distributed Denial of Service (DDoS). TDoS attacks are attempts to make a telephone system unavailable to the intended user by preventing incoming and/or outgoing calls. This is accomplished when an attacker successfully consumes or "floods" all available telephone network resources, preventing legitimate incoming

---

[45] *Montgomery v. Louisiana*, 577 U.S. 190, 207 (2016) (quoting *Miller v. Alabama*, 567 U.S. 460, 471 (2012)) (cleaned up).

[46] Md. Code Ann., Cts. and Jud. Proc. 3-8A-02(a) (2002) (specifying the purposes of the Juvenile Justice System).

and/or outgoing call transactions from processing.[47] Common targets of TDoS include emergency public-safety response systems such as Public Safety Answering Points (PSAPs)[48], government entities, high-ranking officials, and law enforcement agencies. The objective of the attack is to make a significant number of calls and to keep those calls active for as long as possible, to overwhelm or at least "clog" all or a portion of the target's voice system, which may delay or block genuine calls for service. The resulting increase in time for emergency services to respond may have dire consequences, including loss of life.

Manual TDoS attacks use calling campaigns within social networks to encourage individuals to flood a particular number. An automated attack often presents as a "robocall" (an automated telephone call) using a software application to make numerous calls simultaneously or in rapid succession, including Voice Over Internet Protocol (VoIP) and Session Initiation Protocol (SIP). TDoS attacks could also be used in conjunction with a physical

---

[47] The Department of Homeland Security, Science and Technology (S&T) Directorate, *Telephony Denial of Service Fact Sheet*, (June 2016), https://www.dhs.gov/sites/default/files/publications/508_FactSheet_DDoSD_TDoS One Pager-Final_June 2016_0.pdf.

[48] PSAPs are also known as "9-1-1 Centers" and "Emergency Communication Centers."

attack, when calls to 911 and other emergency numbers would peak.[49] TDoS attacks may have a short duration or occur intermittently over several days. Occasionally, TDoS attacks are accidental, such as a mistake in a text message phishing (SMSishing) campaign that inadvertently directs respondents to call for emergency services.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks occur when a bad actor uses resources from multiple, remote locations to disrupt an organization's online operations. Typically, DDoS attacks focus on generating destruction that manipulate the default, or even proper workings, of network equipment and services. Similar to social engineering manipulating the default workings of human communication, a DDoS attacker manipulates the ordinary workings of network services. A DDoS attack is like

[49] FBI: Public Service Announcement, *Telephony Denial of Service Attacks Can Disrupt Emergency Call Center Operations*, (Feb. 17, 2021), https://www.ic3.gov/Media/Y2021/PSA210217.

an unexpected traffic jam clogging up the highway, preventing regular traffic from arriving at its destination.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources, such as Internet of Things (IoT)[50] devices, infected with malware[51], allowing them to be controlled remotely by an attacker. These individual devices are referred to as "bots"[52] (or "zombies"), and a group of bots is called a "botnet." When a target's server or network is pursued by the botnet, each bot sends requests to the target's Internet Protocol (IP) address, causing a crippling interruption in one or more of its services because the attack has flooded their resources with Hypertext Transfer Protocol (HTTP) requests and traffic, denying access to legitimate users. Since each bot is a valid Internet device, separating the attack traffic from

---

[50] "Internet of Things" is a catchall phrase for all the various Internet-connected devices and gadgets that are not traditional computers.

[51] Malware, a portmanteau from the words "malicious" and "software," is a general term which can refer to viruses, worms, Trojans, ransomware, spyware, adware, and other types of harmful software. Malware needs to be intentionally malicious; any software that unintentionally causes harm is not considered to be malware.

[52] A "bot" is a software program that operates on the Internet and performs repetitive tasks.

normal traffic can be complicated and time consuming, proving to be a top cybersecurity threat amongst social engineering, ransomware, and supply chain attacks.

Another method of misusing the 911 system is Caller ID manipulation, also known as "spoofing."[53] Caller ID spoofing is the process of changing the Caller ID to any number other than the actual calling number to disguise the number when making a phone call or sending a short message/messaging service (SMS) text. The number that displays on a Caller ID may look as though it's coming from a government agency or business to entice the recipient to answer a call they would otherwise decline. Numbers and call attributes can be easily spoofed, making it difficult to differentiate legitimate calls from malicious ones.

In 2017, the Federal Communications Commission (FCC) gave phone companies greater authority to block these types of calls.[54] Service providers can now block additional calls that are likely spams, such as numbers that begin with a 911 area code.

---

[53] FCC, *Caller ID Spoofing*, (Mar. 7, 2022), https://www.fcc.gov/spoofing.

[54] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls,* GC Docket No. 17-59, Report and Order and Further Notice of Proposed Rulemaking, 17 FCC Rcd 151, para. 10 (2017).

Bad actors are also spoofing Caller IDs to display "911" and making calls informing individuals that a relative has been in an accident. Between the false number and startling news, scammers are hoping the targets will be frightened enough to share personal information. PSAPs will not make outbound calls unless they are called initially. In the event an individual is receiving a call from a PSAP, the Caller ID will display a seven-digit administrative phone number, or in some cases "restricted," "unavailable" or "blocked." If there is confusion or concern, the non-emergency number for the local police department may assist the call recipient in confirming if the incoming call is legitimate.

911 continues to be vulnerable to security issues which may saturate the network and prevent individuals from receiving timely service. With limited resources and the need to answer every call, PSAPs continue to be vulnerable to TDoS, DDoS, and Caller ID spoofing. Although there are TDoS and DDoS mitigation mechanisms specified in Next Generation 9-1-1 (NG9-1-1) standards, they are not widely deployed. Parallel to swatting efforts, it is necessary to update Maryland's laws and increase penalties for these cyber and telephonic attacks.

TASK FORCE MEMBERS

Meredith R. Weisel, Chair and Regional Director of the Anti-Defamation League

Senator Cheryl C. Kagan

Senator Edward R. Reilly

Senator Jeffrey D. Waldstreicher

Delegate J. Sandy Bartlett

Delegate Lesley J. Lopez

Delegate Rachel P. Muñoz

Sergeant Michael Richardson

Deputy State's Attorney Brian Marsh

Assistant Public Defender Roberto C. Martinez

Detective Brian Donahoe

Staff: Assistant Attorney General Karinna M. Rossi

Thank you to Karyn Henry, J.D., of Mission Critical Partners for her contribution.