SUSAN C. LEE
Legislative District 16
Montgomery County

MAJORITY WHIP

Judicial Proceedings Committee

Joint Committee on
Cybersecurity, Information Technology,
and Biotechnology

Chair Emeritus
Maryland Legislative Asian American
and Pacific Islander Caucus

President Emeritus
Women Legislators of the
Maryland General Assembly, Inc.

THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

James Senate Office Building
11 Bladen Street, Room 223
Annapolis, Maryland 21401
410-841-3124 · 301-858-3124
800-492-7122 *Ext.* 3124
Susan.Lee@senate.state.md.us

February 25, 2021

Senate Judicial Proceedings Committee

Senate Bill 623 - Criminal Law - Crimes Involving Computers - "Ransomware"

Senate Bill 623 mitigates the growing threat of cybercrime in Maryland by defining the crime of ransomware and applying that crime to the unlawful possession of ransomware software with the intent to deploy the technology for malicious purposes. Ransomware is software or a program that prevents victims from accessing computer systems or records until the victim makes a payment to the perpetrator, usually involving untraceable Bitcoin transactions.

Maryland State and local government agencies have fallen victim to high-profile ransomware attacks in recent years. In May of 2019, Baltimore City employees were unable to access online accounts and city payment systems were down for weeks, resulting in some $18 million in restoration and repair costs for the City. These attacks are not only costly, they also threaten public safety. In 2018, a separate ransomware attack rendered Baltimore City's computer-assisted 9-1-1 dispatcher system inoperable for almost a full day.

It's not just big city governments that are targeted with ransomware, local police departments, public and private educational institutions, hospitals and other critical infrastructure face attacks on a daily basis across our State. Some public institutions are targeted not only because they will pay the ransom, but so that the attack itself will generate interest in the software. If an attack garners enough media attention, the software can be marketed and sold on the dark web either as a contract hire or transfer of the ransomware program itself. Private institutions are much more likely to pay to avoid embarrassment, but public institutions have more transparency

requirements that make the damage more severe as they have a greater disincentive to pay off the extortionists.

No business, organization, or industry, no matter the size, is safe from ransomware attacks today. It doesn't take a sophisticated crime syndicate to perpetrate an attack. Any individual connected to the internet has the power to access and utilize crippling ransomware. As the software is disseminated more widely, opportunists like disgruntled employees will deploy these weapons with greater frequency. We must snip this supply growth by fighting demand.

Let me be clear: ransomware is a weapon. This software is a loaded gun with no possible defensive purpose; we shouldn't have to wait for someone to pull the trigger to take decisive action. Law enforcement should be empowered to act against individuals and organizations who possess such weapons without a legitimate purpose *before* they are unleashed to wreak havoc on our schools, hospitals, police departments and businesses. That is exactly what this bill does.

Under SB 623, persons who possess ransomware with an intent to use it for anything other than a lawful purpose are guilty of a misdemeanor offense and will face penalties of up to 3 years (down from 10 in last year's version) and/or a $10,000 maximum fine. Additional tweaks to the penalties reflect feedback we received from the chair last session, and I believe it to be well balanced. In addition to the change of the penalty for possession of ransomware with intent to use it, I have brought back some provisions from previous versions of this bill. The private right of action provision is restored, and local school systems as well as hospitals are added to the critical infrastructure category. After the attack on Baltimore County schools this seems reasonable in the age of COVID and remote learning. Going forward systems for schools are going to be that much more important to protect.

Iterations of this bill have been introduced in prior sessions with the support of the Maryland Cybersecurity Council, on which I serve, and this version continues to enjoy the support of the Council. In past years, this legislation has failed to move forward due to minor technical concerns expressed by the former Chairman. SB 623 has been adjusted to confront those concerns in order to create the best conditions for passage.

While we have a lot more work to do as a committee, as a legislature, and as a State to address ransomware attacks and other cybercrime, this bill is a step in the right direction towards strengthening our cybercrime deterrence. Prosecutors and investigators who discover ransomware and the intent to use it, should not be prohibited from preventing a harmful crime from occurring. There is no lawful purpose to have ransomware if you are not doing research, and we should not allow individuals to trade these weapons online until we create weapons of mass destruction without a deterrence structure.

The private sector should also be more transparent about their attacks, and they should expect future legislation to prevent their payment of ransoms to support organized criminals or opportunists. However, SB 623 is a first step toward preventing access to dangerous weapons that have already been targeted against our democratic institutions and the services government provides to citizens and residents. Most of these services now contain a digital component that can be compromised far too easily with this technology that proliferates unabated.

For these reasons, I respectfully request a favorable report on SB 623.