TESTIMONY PRESENTED TO THE SENATE EDUCATION, HEALTH AND ENVIRONMENTAL AFFAIRS COMMITTEE

SENATE BILL 1036 – MARYLAND EMERGENCY MANAGEMENT AGENCY – CYBERSECURITY COORDINATION AND OPERATIONS OFFICE -ESTABLISHMENT

MAJOR GENERAL (RET) LINDA SINGH
POSITION: SUPPORT

MARCH 12, 2020

First, I would like to introduce myself, I am Major General(retired) Linda Singh. I served as the Adjutant General for Maryland from January 2015 until August 2019. At that time, I had the largest number offensive and defensive cyber resources in the National Guard. My past experience at the federal, state and local level uniquely positions me appear before you today.

If you have not been a victim to ransomware attack, you likely know someone or an agency that has been affected in the last year. In 2017 there were more than 200,000 individuals and more than 300,000 computers that were affected by cyber-attacks. These numbers have continued to climb each year and no matter how much we seem to prepare, the coordination across organizations to mitigate such attacks has remained a significant challenge. In 2017, cybercrime cost the global economy $600 billion. In 2018, the global financial damage exceeded $1 trillion, a 50% annual increase. Cyberattacks are the fastest growing crime in the U.S., and they are increasing in size, sophistication and cost.

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

Given that social engineering attacks (scareware, baiting, phishing and spear phishing) remain the most commonly used techniques, it becomes obvious that hackers focus on exploiting the human factor as a weakness. Even the well-designed security systems could be undermined via a single malicious act aimed at the human factor.

According to the National Preparedness Report, Cybersecurity is the lowest rated core capability and the capability in greatest danger of decline. Malicious cyber actors threaten critical infrastructure, essential services, and sensitive information. We are still hearing that states consistently rate cybersecurity as their least proficient core capability in their State Preparedness Reports.

The best protection against cyberattacks is prevention. While no one may ever be completely safe from a cyberattack, there are several actions we can take to protect our infrastructure and it begins with establishing a Cybersecurity Coordination and Operations Office. Taking preventative measures will help us avoid significant losses from cyberattacks. Implementing preventative measures, on average, saves several million dollars per cyberattack when compared to reactionary measures.

The conceptual model for the Cybersecurity Coordination and Operations Office, is based on other models throughout the United States. It is designed to use regional coordinators like the Cybersecurity and Infrastructure Security Agency's regional offices. This model has been proven to strengthen the coordinated delivery of vital resources and services—training, exercises, and programs—to our Nation's critical infrastructure owners and operators. The Cybersecurity Coordination and Operations Office creates a similar structure focused on assisting with more direct coordination with the counties and municipalities, outreach and engagement tailored to regional needs, improved response to counties and municipalities for information and services, coordinated support and expertise on incident prevention, resilience and recovery and coordinated cyber threat mitigation.

The largest cyberattacks in history exploited vulnerabilities in software, and therefore revealed the importance of maintaining it up to date. The poorly monitored network means that a malicious attack can be performed through your network's back door without being noticed. The weak links in your organization's cybersecurity system can come in many forms but it doesn't mean that the system can't be protected effectively.

I urge a favorable report on Senate Bill 1036.

POC: Linda L Singh, PhD, Major General (Retired), linda.singh@verizon.net