

A thick dark blue vertical bar runs down the left side of the page. A medium blue arrow points to the right, overlapping the bar, with the date '6/17/2022' written inside it in white.

6/17/2022

# Writing Assignment 2

CYSE 406 – Cyber Law

Several thin, curved lines in dark blue and light grey originate from the bottom left corner and sweep upwards and to the right, creating a dynamic, abstract design.

Garrett Moison

# Memo

## **District 26**

To: Tito Canduit  
From: Garrett Moison  
Date: June 17, 2022  
Re: Advancing Cybersecurity Diagnostics and Mitigation Act

I am writing to inform you of a potential cybersecurity bill that, if backed by you, could potentially help you secure more voters in the upcoming election this Fall. Likewise, this bill will benefit our government by improving our government's system and network security and preventing future cyberattacks from affecting our Federal agencies.

The Advancing Cybersecurity Diagnostics and Mitigation Act is an amendment to the Homeland Security Act of 2002. It is supposed to codify the Continuous Diagnostics and Mitigation (CDM) program, providing a program for state and local governments to deploy the CDM's cybersecurity technologies. In addition, this bill would authorize the Secretary of Homeland Security, acting through the Director of Cybersecurity and Infrastructure Security, to deploy, operate, and maintain a continuous diagnostics and mitigation program for agencies.

There are several different responsibilities that this bill will give the Secretary, and I will do my best to mention the critical points to you. Firstly, this bill will allow the Secretary to assist agencies in diagnosing and mitigating cyber threats and vulnerabilities continuously. Moreover, the bill allows the Secretary to collect, analyze, and visualize information relating to security and cybersecurity risks at agencies. These permissions allow agencies to receive assistance from the Department of Homeland Security (DHS), including any programs available to the DHS, on any issues they have with identifying and preventing cyber threats. Additionally, the Secretary can employ shared services and any economic or procurement models to determine the most efficient, cost-saving methods for implementing an information system. Finally, the Secretary will be able to assist agencies in setting security priorities and managing cybersecurity risks, as well as developing policies and procedures for reporting cybersecurity risks and potential incidents based on collected data.

Cyberattacks pose a severe threat to our economy and national security, and attacks on our government have increased in frequency and complexity. An example of one of these devastating attacks was a data breach our government was hit by in 2020. This breach was one of the worst cyber-espionage incidents in the U.S. during a presidential transition and a public health crisis. To make matters worse, Russian hackers were behind the attack and have compromised thousands of other organizations and unclassified networks operated by our government. With no logical conclusion as to who in Russia was behind the attack, we can only assume that it was the Russian government, creating a problematic international conflict. Furthermore, a necessary resolution to the attack required the replacement of entire enclaves of computers and network hardware, costing our government a considerable amount of money.

Therefore, our federal agencies can better thwart these attacks by updating our cybersecurity tools and programs. In addition, by codifying the CDM with congressional oversight, we can ensure that our government is better prepared for potential cyber threats.

Cyberattacks on our government systems are demoralizing to the people of the United States, so backing this law should garner you a significant amount of support. Cybersecurity is a growing prospect in our nation, with data breaches growing in numbers, requiring us to improve our networks and systems. In addition, our government holds vast quantities of data on our citizens, meaning any breaches to our government are very concerning to them. In conclusion, backing this bill and giving the Department of Homeland Security more responsibility and resources to assist other Federal agencies will prevent further devastating cyberattacks and help you win voters in the upcoming election.

## **References**

- Curran, J. (2022, March 24). Senate Bill Aims to Codify Federal CDM Program, Pilot SLG Deployments. *MeriTalk*. <https://www.meritalk.com/articles/senate-bill-aims-to-codify-federal-cdm-program-pilot-slg-deployments/>
- H.R.4237 - Advancing Cybersecurity Diagnostics and Mitigation Act. *Congress.gov*. (2019). <https://www.congress.gov/bill/116th-congress/house-bill/4237/text>
- Riotta, C. (2020, December 17). US under major active cyberattack from Russia, Trump's former security adviser warns. *The Independent*. <https://www.independent.co.uk/news/world/americas/russia-cyber-attack-us-trump-b1775632.html>