RESEARCH MEMO

DATE: November 12, 2023

TO: Tito Canduit

FROM: Kendal Taylor

SUBJECT: Potential Cybersecurity Laws and Regulations

Good afternoon Tito. I have written a research memorandum to you to assist with your reelection bid. This research highlights a recently proposed cybersecurity law that highlights protecting the people from cybersecurity threats. This will help you to roll out letters regarding potential cybersecurity proposals to strengthen our nation's cybersecurity, as well as your reelection bid.

Proposed Law

After conducting research, I have come across a bill that is underconsideration. It was presented on June 6th, 2023 entitled "*Advancing Cybersecurity Diagnostics and Mitigation Act"*. In summary, this bill seeks to require the CISA (Cybersecuirty and Infrastructure Security Agency of the Department of Homeland Security) to create a campaign program designed to raise awareness of cybersecurity in the United States. The findings within this bill state that, "the presence of ubiquitous internet-connected devices in the everyday lives of citizens of the United States has created opportunities for constant connection and modernization." It emphasizes that due to the connected nature of our society, we are more vulnerable to cybersecurity threats. The issue of interconnected critical infrastructure is also addressed, as well as the dangers that can occur if they are compromised. According to the White House's memorandum for critical infrastructure cybersecurity, "Protecting our Nation's critical infrastructure is a responsibility of

the government at the Federal, State and local levels, as well as of the owners and operators of that infrastructure." (The White House, 2021). Though the government plays a significant role in cybersecurity, developing a knowledgeable society is a critical tool. This proposal also states that cybersecurity awareness cannot fall into the cracks of a "once-a-year" activity, such a cybersecurity awareness month. Rather it should be a sustained, consistent effort among the citizens and the government.

They have established standards regarding these cybersecurity awareness campaigns. They include: establishing Federal cybersecurity awareness campaigns no later than 90 days after the enactment of the National Cybersecurity Awareness Act. In addition to this, the director of the campaign program should: "inform non-federal entities of best cyber hygiene practices, such as how to prevent cyberattacks and mitigate risks." The director should also consult with private sector entities, state, local, civil society and more to promote these best practices. To understand this, they have also defined what proper cybersecurity hygiene is. This is described as: "maintaining strong passwords and using a password manager, multi factor authentication, regular software updates, using caution with email attachments and links." (National Cyber Security Awareness Act, 2023). In addition to this, Jay P. Kesan and Carol M. Hayes states that an "ongoing analysis of threats, incidents and potential risks." can provide a near real-time awareness of cybersecurity in organizations (Kesan & Hayes, 2019).

The Issue the Bill is Addressing

This bill addresses the current issue of a lack of awareness when it comes to cybersecurity. Sure, many voters hear about it in the news and on the radio, but what does it actually entail? Many voters likely think that they aren't a valuable target for cybercriminals, when the reality is that anyone who has money to their name is a valuable target to

cybercriminals. This bill works to accomplish this by establishing response protocol and guidelines for good security posture. This law can fix the lack of awareness problem by helping voters to understand that hackers aren't just after the local and federal governments, they are out there after you too. This bill gives guidelines and provides strategies for continued awareness; voters may have a smaller chance of being victimized by cybercriminals.

Conclusion & Observations

In conclusion, this law possesses the ability to make cybersecurity more than just an issue voters see on the news. It makes cybersecurity a continuous effort through collaboration and guidance. I would recommend emphasizing the inclusiveness of this act, given it is not a strictly governmental cybersecurity act. It is worried about the citizens of the nation, this includes your voters. Making them feel as included as possible in this act will help to maintain their online safety, as well as their confidence in maintaining good cybersecurity posture. Thank you for your time.

References

National Cyber Security Awareness Act, 118th Congress, S. 1835 (2023). https://www.congress.gov/bill/118th-congress/senate-bill/1835/text?s=1&r=11&q=%7B%22search%22%3A%22cybersecurity+laws%22%7D

Kesan, J. P., & Hayes, C. M. (2019). Cybersecurity and Privacy Law in a Nutshell. *West Academic Publishing.*

The White House. (2021, July 28). National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems. *The White House.* https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/