MEMORANDUM

To: Representative Tito Canduit

From: Aide EJ Corpus

Date: April 20, 2023

Subject: Cybersecurity Law for Consideration

Dear Representative Tito Canduit,

As you prepare for your reelection bid, it is important to demonstrate your commitment to cybersecurity legislation that protects the American people from threats that can affect their identity or steal sensitive information. I have conducted research on recently enacted and proposed U.S. and state cybersecurity laws and identified a law that is important for your consideration. A recent law that I found was the CISA Act which could very much benefit your bid and the overall wellness of cybersecurity in the United States.

The Cybersecurity and Infrastructure Security Agency Act of 2018 (CISA Act) is a recently enacted U.S. law that establishes the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) to lead the national effort to protect and enhance the security and resilience of the nation's critical infrastructure. The law was signed by President Donald Trump on November 16, 2018. The act allows United States government agencies and non-government entities to share information with each other as they investigate cyberattacks. This is called threat intelligence where they can work together to help understand an attacker’s motives and behaviors.

The CISA Act is designed to address the systems and assets vital to national security, economic security, public health and safety, and the well-being of the nation. This law is a major step forward in securing the nation's infrastructure against a wide range of cybersecurity threats, including those from foreign adversaries and hackers. Before the enactment of the CISA Act, DHS's cybersecurity responsibilities were divided among several different offices, making it difficult to coordinate cybersecurity efforts across the federal government. The creation of CISA consolidates these responsibilities into a single office, providing a more unified and coordinated approach to cybersecurity.

The CISA Act also strengthens the partnership between the federal government and the private sector, recognizing that the majority of the nation's critical infrastructure is owned and operated by private companies. The law establishes a framework for information sharing between the government and private sector entities to better identify and mitigate cyber threats to critical infrastructure. Although this law attends to cybersecurity threats, it does not deal with the problem of the government attempting to gain access to encrypted communications.

While the CISA Act is a significant step forward in securing the nation's critical infrastructure against cybersecurity threats, there are opportunities to improve the law. For example, the law could be amended to provide additional funding for cybersecurity research and development and enhance cybersecurity education and training programs for federal employees and private sector stakeholders. Cloud security is important and the CISA Act supports improving and developing strategies to strengthen the cloud. Another way to improve the act would be to include other outside resources that have crucial information instead of limiting it to private sector agencies and the federal government. Keep in mind, the CISA Act does not fix the problem since the cybersecurity world evolves every day, this means hackers also improve. The law will only help mitigate and improve security in businesses and agencies.

One provision in the CISA Act that voters might relate to is the requirement for CISA to develop and maintain a cybersecurity workforce strategy. The strategy is designed to ensure that CISA has the necessary expertise and resources to protect the nation's critical infrastructure against cybersecurity threats, including by developing a comprehensive cybersecurity workforce plan. It would be good to emphasize the threats that can be made to people and their families due to the internet. People can relate to social engineering attacks where they receive an email that look suspicious but common sense helps them notice that the email is malicious. These threats are exactly why the CISA Act was created, to help protect the people.

Your Aide,

EJ Corpus

References

CISA. (2023, April 20). *Cybersecurity and infrastructure security agency: CISA*. Cybersecurity and Infrastructure Security Agency CISA. Retrieved April 20, 2023, from https://www.cisa.gov/news-events/alerts/2018/11/19/cybersecurity-and-infrastructure-security-agency

CISA. (n.d.). *Executive order on improving the nation's cybersecurity: CISA*. Cybersecurity and Infrastructure Security Agency CISA. Retrieved April 20, 2023, from https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity

Office, U. S. G. A. (n.d.). *Cybersecurity and infrastructure security agency: Actions needed to ensure organizational changes result in more effective cybersecurity for our nation*. Cybersecurity and Infrastructure Security Agency: Actions Needed to Ensure Organizational Changes Result in More Effective Cybersecurity for Our Nation | U.S. GAO. Retrieved April 20, 2023, from https://www.gao.gov/products/gao-21-236

Contributor, T. T. (2016, February 23). *What is Cybersecurity Information Sharing Act (CISA)?: Definition from TechTarget*. WhatIs.com. Retrieved April 20, 2023, from https://www.techtarget.com/whatis/definition/Cybersecurity-Information-Sharing-Act-CISA#:~:text=Cybersecurity%20Information%20Sharing%20Act%20(CISA)%20is%20proposed%20legislation%20that%20will,participating%20organizations%20outside%20the%20government.