

Background Research Memorandum

Carmen Taylor

12/2/2023

Cyse406 Cyber Law

To: Rep. Canduit

From: Carmen Taylor

Date: 12/2/23

Subject: Memorandum of Background Research Regarding Cybersecurity Legislation

Dear Rep. Canduit,

After hearing about you preparing for your 2022 reelection campaign in the fall, I was happy to help you secure the win when it comes to understanding these related laws. After spending some time and completing this important research, one law that can be included in your letters to the residents is “the Cybersecurity Enhancement Act of 2014”.

What is it: The Cybersecurity Enhancement Act of 2014 is a bill intended to improve the US government’s cybersecurity posture. It was passed to maintain the increasingly complex and aggressive cyber threats that the country is always at risk of facing.

How does it fix the issue: The law allows for resources, such as funds, and the creation of programs that enhance the research and development of the bill. It requires the cooperation of government agencies, private businesses, and academic institutions, to ensure the evolution of cybersecurity solutions. When thinking about the education and workforce development aspect, the law emphasizes the fact that education and training play an important role in combating cyber-attacks. It allows for the creation of a strong workforce, asking for employees to work together to educate themselves on cyber competitions, creating a national cyber awareness and education program, and introducing a cyber scholarship-for-service program. Some areas of skill the employees will have to undergo when combating the cyber challenges include “ethical hacking, penetration testing, and the continuity of system operations”(Sec 301). Then when the public-private partnerships, come into play, the law highlights why these partnerships are beneficial when protecting against the country’s cybersecurity protection performance. The act promotes communication and cooperation between both public and private sector organizations. One way to ensure their improvement in this area is the law amends the NIST for organizations to “consult with the heads of agencies with national security responsibilities, sector-specific agencies, and other appropriate agencies”. NIST stands for the National Institute of Standards and Technology, and it is a framework that provides for common and repeated use, rules, guidelines, or characteristics for activities that are created to achieve the “optimum degree of order in a given context”. The Framework of the NIST is mandated by this law to establish and maintain a cybersecurity framework that offers the best standards and guidelines. When these are put in place correctly, it will ensure that many organizations, agencies, and people have reduced cybersecurity risks. The Act requests that federal agencies have organized obligations when trying to protect their data and internal systems. The law proposes that government entities handle cybersecurity in a systematic and coordinated manner. One way the government interacts on a federal level from this law is for

the National Science and Technology Council and the Networking and Information Technology Research and Development Program, must update their Federal cybersecurity research and development strategic plan “every 4 years”. (sec.201)

Effect: Since this Act was created the country has had a stronger defense against cyber-attacks and challenges. The act allowed for major advancements in research, education, and teamwork between the private and public sectors. Cyberspace is stronger and safer than it ever has been before.

Letters: In the letters to the constituents, highlight the results of how this Act improved the cyber workforce size, breakthroughs in technologies, and more effective collaboration strategies. Also focus on the value of presenting a unified front when confronting cyberthreats, and state your intention to support the government that protects the interests of the American people in the digital era.

Today's issues: Today many people of today need help against fraud, which includes identity theft, or bank fraud where money is stolen. This act will help combat this in one way, where sec 201, states that Federal cyber research must be updated every four years, meaning that ways to combat this shall be included in that research. One way the research will combat this is to include a safe way to secure your bank info and private info, such as using Two- authentication sources when logging into accounts.

Citations:

<https://www.govinfo.gov/content/pkg/COMPS-12455/pdf/COMPS-12455.pdf>

<https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework#:~:text=NIST%20is%20the%20National%20Institute,the%20U.S.%20Department%20of%20Commerce.>