MEMO

To: Tito Canduit
From: Evan Schranz
Date: June 19, 2021
Subject: Cybersecurity Legislation

Dear Mr. Canduit,

I am writing to inform you that after carefully analyzing both enacted cybersecurity laws and cybersecurity law proposals that are still under consideration, I have come up with a professional decision on what bill should be further reviewed.

H.R. 4237 or the Advancing Cybersecurity Diagnostics and Mitigation Act is a federal bill that was proposed in the House on September 6, 2019. It was passed by the Committee of the Department of Homeland Security (DHS) but is still awaiting future consideration by the House Oversight and Reform Committee. In broader terms, H.R. 4237 was an introduced bill in 2019 and is still pending by the House. The bill is currently waiting for further evaluation to be either approved or declined as a U.S. law. (See link below for more information)

https://www.congress.gov/bill/116th-congress/house-bill/4237

Advancing Cybersecurity Diagnostics and Mitigation Act was introduced by John Ratcliffe to amend the Homeland Security Act of 2002. If approved, this law will obligate the Department of Homeland Security (DHS) to create a program that will primally assist agencies in mitigating and deterring any oncoming cyber threats/vulnerabilities. By doing so, the Department of Homeland Security will meet four standard requirements. The first being that they will develop a program with the competency to efficiently detect, collect, analyze, and visualize any information/security data relating to incoming cybersecurity risk at any given organization or agency. Secondly is to make the cybersecurity program available to any agency. That being at either a local, state, or civilian level. Thirdly is for the DHS to help assist with setting up priority security information within an agency. The fourth and last requirement is for the DHS to develop new policies and standard procedures when in the process of reporting potential cybersecurity risks or incidents. The DHS must also keep up to date on developing new technologies to improve the program.

As hackers continue to find alternative ways on infiltrating large government and civilian agencies/organizations, it is key to find ways to counter these attacks. For example, the recent cyberattack by a gang called DarkSide was aimed at paralyzing one of the biggest North American petroleum pipelines. The result was catastrophic. The company Colonial Pipeline had

to shut down for days causing a gas shortage within a number of states. However, if H.R. 4237 is passed as a U.S. Law, any agency, whether it be a civilian or government agency, will have access to resources and equipment needed to prevent such a national crisis from ever happening. Although this bill may not successfully stop cyber hacking entirely, it will provide cybersecurity aid which could greatly reduce the chances of hackers successfully penetrating any agency's private security systems.

Analyzing how issues such as the national gas shortage affects thousands of American lives, it is clear that cyber hacking does not only interfere on a corporate or government level, but it affects the individual everyday person as well. Enacting H.R. 4237 as a law will help create a more secure environment for both the government and corporations to ensure that America's infrastructures which people rely on run smoothly. With the cyber resources provided by the DHS, America as a whole will be better prepared and more capable of implementing preventative measures if a crisis ever arises. With that said, if passed, H.R. 4237 will benefit every aspect of what makes America a secure and functioning country.

In conclusion, I highly advise you, Mr. Canduit, to review and consider going over the H.R. 4237- Advancing Cybersecurity Diagnostics and Mitigation Act and implementing it towards future voter campaigns. As technology becomes a much more prevalent source within agencies all across the world, informing the general public about H.R. 4237 will help them grasp a better understanding about the necessary cybersecurity implementations that are needed.

Sources

https://www.bloomberg.com/news/articles/2021-05-09/u-s-fuel-sellers-scramble-for-alternatives-to-hacked-pipeline

https://www.govinfo.gov/app/details/BILLS-116hr4237ih

https://docs.house.gov/meetings/HM/HM00/20191023/110141/BILLS-1164237ih.pdf

https://www.congress.gov/bill/116th-congress/house-bill/4237

https://www.csoonline.com/article/3512043/2020-outlook-for-cybersecurity-legislation.html