Memo on Cybersecurity Vulnerability Remediation Act (R.3710)

Janae Craig

Old Dominion University

CYSE 406

Professor Cheney

April 21, 2023

Cybersecurity Vulnerability Remediation Act (R.3710)

Cybersecurity Vulnerability Remediation Act (R.3710) was sponsored by Representative Jackson Lee, a homeland security and governmental affairs committee member, in 2019. Cybersecurity Vulnerability Remediation Act (R.3710), already passed into the Senate, was successfully deliberated but has yet to begin its operations. The bill underwent both readings and was subjected to discussions from the various political divides on the floor of the Senate.

Cybersecurity Vulnerability Remediation Act (R.3710) has expanded the Department of homeland security by granting it more responsibilities related to cybersecurity. The Department is, therefore, responsible for managing cybersecurity vulnerability issues within the United States, a step that is of great importance to all residing there. The bill empowers the National Cybersecurity and Communications Integration Center, a Department of Homeland Security unit, to establish and implement protocols for counteraction against cybersecurity in various sectors of the country. These interactions also include individual organizations whose software and hardware components are at risk of cybersecurity threats. The bill also empowers the Science and Technology directorate to develop and implement remedies that can competitively help curb cybersecurity issues. It, therefore, means that this bill grants cybersecurity issues more weight. As a result, when an organization receives a cybersecurity threat, the Science and Technology directorate can quickly assist in solving this problem promptly without delays (Brumfield, n.d).

The Cybersecurity Vulnerability Remediation Act (R.3710) established a Cybersecurity and Infrastructure Security Agency (CISA). CISA is a new component, a federal agency established to protect the United States' critical infrastructure. This component is also responsible for protecting against physical attack in some dimensions. However, its sole aim for the establishment was to increase the nation's capacity to handle cybersecurity issues.

Cybersecurity issues are increasing day by day in the United States. Therefore, the bill is of great help to the constituents. The increased responsibility of the Department of Homeland Security enables the constituents to anchor their trust in the nation's efforts to curb cybersecurity. Also, Cybersecurity issues have been of significant threat to business activities. The bill ensures maximum protection of these businesses to mitigate fraudulent actions and hacking of business databases (Brumfield, n.d).

The Cybersecurity Vulnerability Remediation Act (R.3710) also enables the Department of Homeland Security to conduct competitions on cybersecurity issues. These programs are intended to instill cybersecurity knowledge and data protection skills in the local citizen and promote local skills who may get chances of employment when they compete favorably. This is an excellent chance for the district's unemployed youths to train in cybersecurity and use the available platforms to compete and gain more skills. Shortly, almost everyone will know about the management of cybersecurity threats (Brumfield, n.d).

Cybersecurity Vulnerability Remediation Act (R.3710) is also cost-effective for ordinary citizens. However, unfortunately, managing cybersecurity threats is often expensive. Sometimes, one has to bear many losses when they cannot, for example, pay malware attackers. They, therefore, end up losing their well-established and costly business. The efforts of the members of the Senate were to ensure that these services could be provided for free and that the attackers could be traced and arrested afterward.

Cybersecurity issues often come up in every electioneering period. Sometimes unscrupulous deals lead to deleting voters' details from the voter register. In other cases, many system failures lead to delays in the voting processes. Through cyber attackers, some candidates

have lost elections because these elections were rigged in favor of other candidates. Therefore, this bill seeks to help the common constituents and the country

Reference

Brumfield, C. (n.d.). 2020 outlook for cybersecurity legislation. CSO Online. https://www.csoonline.com/article/3512043/2020-outlook-for-cybersecurity-legislation.html

Cybersecurity Vulnerability Remediation Act (R.3710)

https://www.cbo.gov/publication/55508