To: Rep. Gomer Pyle Independent Virginia's 26th District

From: Chris Evans, UIN: 01206431, Cyber Law 406 Prof. Mann

Subject: Writing Assignment 2, Background Research Memo for Rep. Pyle

Date: June 13, 2023

A. Overview

H.R.3710- The Cybersecurity Vulnerability Remediation Act (CVRA). Sponsored by Rep. Sheila Jackson Lee Democrat of Texas 18 District on July 11, 2019. CVRA has passed the House on September 26, 2019. The bill currently is stalled in the Senate Homeland Security and Government Affairs Committee. CVRA empowers the Department of Homeland Security to address cybersecurity concerns in two ways first by disseminating protocols that counter vulnerabilities in software and hardware and second by allowing the Science and Technology Directorate of DHS to establish an open competition of subject matter experts which will provide crowdsourced solutions to the cybersecurity vulnerabilities. Cybersecurity is a key issue for national security and part of keeping America safe and functioning, cyber attacks and ransomware attacks cause damage and disruption to the tune of billions and only increase every year. Strengthening public private partnerships increases national security and strengthens private infrastructures cybersecurity defenses. This legislation also builds on the goals and directions of the White House's National Cybersecurity Strategy. Voters benefit from leveraging crowdsourced best talent to continuously improve the security of the federal governments computer systems, and from the DHS creating protocols that secure software and hardware. CVRA also addresses growing national security concerns about cyberwarfare and threating attacks from rival nations or groups.

B. Summary of H.R.3710- The Cybersecurity Vulnerability Remediation Act (CVRA)

H.R.3710- The Cybersecurity Vulnerability Remediation Act (CVRA) is sponsored by Rep. Sheila Jackson Lee Democrat of Texas 18 District on July 11, 2019, and passed the House on September 26, 2019. The Senate Homeland Security and Government Affairs Committee currently is reviewing CVRA. H.R. 3710 would amend the Homeland Security Act of 2002 and add two major components. First it would establish the ability of the Department of Homeland Security to, *"identify, develop, and disseminate actionable protocols to mitigate cybersecurity vulnerabilities, including in circumstances in which such vulnerabilities exist because software or hardware is no longer supported by a vendor."*. This would allow DHS to begin to develop and share remedies to hardware and software vulnerabilities discovered it their or member agencies computer networks. This will allow more sharing of cybersecurity solutions and increases the effectiveness of cybersecurity personnel as they won't work independently on the same vulnerabilities. The second piece of the legislation would allow the Science and

Technology Department under the DHS to create an incentive-based competitive program that would allow industry experts, threat researchers, and individuals to create solutions to vulnerabilities. This would be crowdsourcing cybersecurity, and leverage industry and expert knowledge from the private sector and researchers to develop and implement cybersecurity solutions.

https://www.congress.gov/bill/116th-congress/house-bill/3710

C. Background Context

-US Government stepping up security in wake of cyberattacks

The US government has been increasing its cyber defenses in the wake of the Russian invasion of Ukraine and increased cyberattacks online. The Cybersecurity and Infrastructure Security Agency's (CISA) Shields Up campaign is trying to help organizations prepare for, respond to, and mitigate the effects of cyberattacks on their networks and critical infrastructure. This is done by sharing guidance and resources on threats, vulnerabilities, and best computer practices.

https://www.cisa.gov/shields-up

-Sharing threat information is common and beneficial in cybersecurity

The sharing of threat information and vulnerabilities is a common technique in cybersecurity and has had great success bringing together the work of academic researchers, industry experts, and government. The rapid dissemination of information concerning types of malware, attack techniques, or other indicators or compromise all allow organizations to better strengthen their cybersecurity posture. A major success in sharing cybersecurity information is the CVE catalog or common vulnerability and exploit reporting framework which is maintained by public private partnerships and uses a reporting network to create a public catalog of vulnerabilities for organizations to use to strengthen their cybersecurity.

https://www.cve.org/About/Overview

D. Benefits and Improvements to H.R.3710- The Cybersecurity Vulnerability Remediation Act (CVRA).

-Crowdsourcing Pro's and Con's

One of the strongest benefits of the CVRA is the use of contests to solve vulnerabilities in government computer systems. These contests will be open to individuals and cybersecurity subject matter experts as they compete to solve computer vulnerabilities first in government computer systems. Crowdsourcing is good for solving highly technical complex problems, such as cybersecurity problems. While crowdsourcing is a powerful tool, it does require diligent review of the information released to the crowd, and government will need to monitor that privileged information is not disclosed, and that adversaries do not gain from the information shared in competitions.

-Benefits to sharing information and supporting White House's National Cybersecurity Strategy

The CVRA attempts to support the initiatives in the White House National Cybersecurity Strategy and copy existing programs that use collaboration with the private sector. Sharing information on vulnerabilities and threats between private sector and governments is common in the cybersecurity industry and has shown immense benefits. A recent example is Microsoft alerting the US government to compromise in their computer networks in Guam by Chinese hackers.

https://grahamwaters.medium.com/h-r-3710-cybersecurity-vulnerability-remediation-act-9344182e8c77

https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html

E. Voter Appeal

-Why we need to strengthen cybersecurity, Chinese and Russian cyberattacks

Russia's military operations against Ukraine began with cyber-attacks attempting to disrupt military and civilian infrastructure and communications, thus securing our government computer infrastructure is a defensive measure against any possible military attacks. The government of Ukraine has been working with international cybersecurity companies and foreign cybersecurity experts to protect their government systems and has had big success limiting scope and impact of Russian cyber-attacks. China continuously launches cyberattacks at American industry and government computer networks in attempts to steal information or compromise operations. Recently Microsoft discovered and alerted the US government that China had hacked critical infrastructure in Guam, a key US ally with a strong US Navy presence. The partnership between the private sector and the US government strengthened US national security as it alerted to the vulnerabilities. CVRA will create more partnerships with the private sector and collaboration between agencies in DHS to spread actionable good intelligence quickly and repair vulnerabilities limiting cyberattacks.

https://thehill.com/opinion/cybersecurity/4049481-the-guam-hack-should-be-a-cybersecurity-wakeup-call/

https://www.washingtonpost.com/politics/2023/02/16/what-we-learned-year-russian-cyberattacks-ukraine/

-How it helps voters

Voters need to be able to rely on the government to fulfill essential functions and respond during times of crises. The computer infrastructure the government uses must become reliable and resistant to attacks from adversarial nations or cyberhackers. By securing our federal computer networks we help increase national security, keeping America safe at home and strong abroad.

-Rep. Pyle the independent continues to work across the aisle with both Republicans and Democrats

Rep. Pyle as a member of the Independent party has been working across the aisle his whole career and continues to support good legislation regardless of party affiliation. Americas cybersecurity and national security should not be up for partisan debate, as our adversaries continually seek to attack us. Rep. Pyle calls for passing the CVRA and for congress to stop playing games with Americans and our security.

SOURCES

https://www.congress.gov/bill/116th-congress/house-bill/3710

https://grahamwaters.medium.com/h-r-3710-cybersecurity-vulnerability-remediation-act-9344182e8c77

https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html

https://thehill.com/opinion/cybersecurity/4049481-the-guam-hack-should-be-a-cybersecurity-wakeup-call/

https://www.washingtonpost.com/politics/2023/02/16/what-we-learned-year-russian-cyberattacks-ukraine/

https://www.cve.org/About/Overview

https://www.cisa.gov/shields-up