Writing Assignment 2

Ethan Heeter

CYSE 406 - Cyber Law

11/30/2023

One of the most pressing issues facing the United States when it comes to the world of cybersecurity is the glaring weak points of our country, and that is the critical infrastructure responsible for maintaining our everyday way of life. Our critical infrastructure is vulnerable to cyber attacks, and when these attacks do happen, they can be utterly devastating to large portions of our country. There has been legislation proposed to congress to attempt to fix the issues of cyber vulnerabilities in critical infrastructure, with some failing and some passing. One such example is the Cybersecurity Vulnerability Identification and Notification Act of 2020, which is currently stuck on the legislative calendar since 2020. This bill seeks to allow the Department of Homeland Security, and more specifically the Cybersecurity and Infrastructure Security Agency or CISA, the power to compel both public and private critical infrastructure companies to supply them with information in regards to cybersecurity vulnerabilities in their systems.

This bill would allow for the federal government to know what vulnerabilities exist in the critical infrastructure keeping America running, which in turn leads to a better, more secure nation. The overwhelming threat of cyber attacks on the critical infrastructure of the US have never been as apparent as the infamous Colonial Pipeline attack that occurred in May 2021, the largest cyber attack to ever hit American critical infrastructure. The Colonial Pipeline is a massive pipeline on the east coast, “The Colonial Pipeline comprises more than 5,500 miles of pipeline. It starts in Texas and moves all the way up through New Jersey, supplying nearly half of the fuel for the East Coast.”(Kerner, 2022). The Pipeline was hacked by a hacking group known as DarkSide, a group of hackers primarily from Eastern European countries, and was shut down from May 7th to May 12th. The lack of gasoline to the east coast caused a state of panic in the general public, as the people rushed to get gasoline before it ran out, only serving to exacerbate the issue of dwindling oil supplies in affected areas. The pipeline was restored, but not before the ransom of 4.4 million dollars was paid, of which about half was later recovered by the Department of Justice, but the damages that were caused by the shutdown of the pipeline itself were far greater, with sectors such as the airline industry being disrupted.

As the Colonial Pipeline attack of 2021 has clearly shown us, the cybersecurity of critical infrastructure is of paramount importance not only to the national security of the US, but to the way of life that American citizens are accustomed to. This is why a bill that properly addresses the inherent weaknesses of critical infrastructure cybersecurity is so important, an issue that is properly addressed by this bill through the use of CISA to find any potential vulnerabilities, though it could be improved. This bill allows for the CISA to identify vulnerabilities in the cybersecurity of critical infrastructure, but the bill would be substantially better at defending the United States if it also allowed CISA to compel the companies to fix said vulnerabilities. The Cybersecurity Vulnerability Identification and Notification Act of 2020 only allows CISA to identify the vulnerability and then notify them about it, but if this was changed to allow CISA to both identify vulnerabilities and then force the company to fix them then critical infrastructure would be substantially more secure. Under the vigilance of CISA, fixes would be implemented that would solve these vulnerabilities facing critical infrastructure and America would be more secure for it.

Forcing those in charge of critical infrastructure to take more precautions when it comes to the cybersecurity of said infrastructure that is crucial to the entire country is a measure that should absolutely be taken, and one that will be very popular. The people of the United States rely upon this infrastructure for their daily lives, so improving the cybersecurity of critical infrastructure would also be improving the security of the American people. This would also have absolutely no negative effects on the public, only adding some restrictions to the companies and groups that operate this infrastructure, and thus would be nothing but a boon to the general public. This is one of the reasons why improving the security of critical infrastructure is a bipartisan issue, which also would serve to garner more popularity from both the left and right leaning populace. The implementation of a bill similar to the Cybersecurity Vulnerability Identification and Notification Act of 2020, yet strengthened such that it allows for the compelling of change would not only protect America, but also gain the popularity of the American people.

References:

S.3045 - 116th Congress (2019-2020): Cybersecurity Vulnerability Identification and Notification Act of 2020. (2020, July 29). https://www.congress.gov/bill/116th-congress/senate-bill/3045

Kerner, Sean&nbsp; Michael. “Colonial Pipeline Hack Explained: Everything You Need to Know.” WhatIs.Com, TechTarget, 26 Apr. 2022, www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

J. Beerman, D. Berent, Z. Falter and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), Bangalore, India, 2023, pp. 8-15, doi: 10.1109/CCGridW59191.2023.00017. https://ieeexplore.ieee.org/document/10181159