

To: Rep. Tito Canduit
From: Vincent Saunders
Subject:

This memorandum examines a recently approved cybersecurity law that I believe is crucial. The Hack Your State Department Act is the name of this legislation. Although this legislation has not yet become law, it has been approved in the House and forwarded to the Senate as of January 2019. Regrettably, it was never passed by the Senate. This is an act that permits individuals, businesses, or organizations to hack or attempt to hack into the Department of State in order to detect and research any potential weaknesses.

The Brumfield law mandates the creation of a Vulnerability Disclosure Process (VDP) by the Department of State to enhance cybersecurity. The VDP requires the State Department to determine the digital technologies that will be included, the types of security vulnerabilities that may be targeted, and provide a readily available form and means of reporting. The law also includes the bug bounty pilot program that allows approved individuals, organizations, or companies to identify and report vulnerabilities on the State Department website. Participants in the program will be compensated, which makes it similar to ethical hacking and a potential job opportunity.

The VDP is an important step toward improving cybersecurity in the government sector. By establishing clear guidelines for identifying and reporting vulnerabilities, the State Department can stay ahead of potential cyber-attacks. The bug bounty pilot program is a proactive approach that incentivizes individuals and organizations to search for vulnerabilities and report them, rather than exploit them for personal gain. Additionally, compensating individuals for their participation in the program provides a tangible incentive for individuals to take part, potentially attracting skilled professionals to participate.

Overall, the Brumfield law and the bug bounty pilot program demonstrate the importance of proactive measures to enhance cybersecurity. By incentivizing individuals and organizations to report vulnerabilities, the State Department can stay ahead of potential cyber-attacks and improve its overall cybersecurity posture.

The bug bounty pilot program has specific requirements that must be met to ensure its success. One key requirement is the provision of compensation for previously unidentified security risks found in the department's public-facing websites, applications, and other technologies. Another important requirement is the ability to award contracts to companies to administer and repair discovered security flaws if needed. To ensure the protection of individuals, organizations, or companies participating in the program, a meeting with the attorney general is required to guarantee they will not be prosecuted.

The pilot program should be short-term and not last more than a year. After its completion, the Secretary must submit a report detailing the program's success. This report should include information such as the number of approved individuals, organizations, or companies involved, the number of registered participants, the number of approved participants, the number of security vulnerabilities identified, and the number of participants compensated for their findings. The report should also include details about the number and severity of security vulnerabilities identified and resolved as part of the program, the current status of outstanding security vulnerabilities, and the Department's remediation plans. Additionally, the report should highlight the types of compensation provided under the program and the lessons learned.

The bug bounty pilot program's specific requirements provide clear guidelines for its success. Compensation incentivizes individuals and organizations to participate, while contracts ensure the program's effective administration and timely remediation of security flaws. The Attorney General's involvement helps protect participants from potential prosecution, while the reporting requirements provide a clear evaluation of the program's effectiveness. Overall, these requirements provide a clear framework for a successful bug bounty pilot program.

This act aims to enhance the Department of State's security measures and protect against hackers penetrating its database. Many non-governmental organizations conduct similar practices, calling them penetration testing. As digital attacks have grown more complex, organizations' internal security capabilities have been surpassed, leading to the emergence of "bug bounties." These contests incentivize developers to stress test systems and identify vulnerabilities.

Foreign countries such as China, North Korea, and Russia have a history of attempting and succeeding in hacking into government databases. The State Department suffered major computer break-ins in 2006, targeting its headquarters and offices dealing with China and North Korea. Hackers accessed sensitive US information and passwords, leading to limited internet access at many Department locations and a decrease in employee productivity. In 2022, suspected Russian hackers stole thousands of State Department officials' emails, accessing emails in the Bureau of European and Eurasian Affairs and the Bureau of East Asian and Pacific Affairs. These incidents highlight the importance of effective security measures to protect sensitive government information.

I don't believe this legislation will solve the problem because I don't believe it can be solved. The rate at which technology is rapidly advancing corresponds to the rate at which new hacking techniques are developed. There will always be hackers, but perhaps this act will make it simpler to keep up with them. Constantly attempting new techniques to breach the Department's security system is prudent because this is exactly what hackers do, therefore being proactive can assist the department in discovering new ways to reinforce its security system. I believe the law is great as

it is. Personally, I believe that this law is vital and that it may benefit both the United States as a whole and its inhabitants individually.

Work Cited

Brumfield, Cynthia. "2020 Outlook for Cybersecurity Legislation." CSO Online. CSO, 06 Jan.2020. Web. 21 April 2023.

"H.R.328 - 116th Congress (2019-2020): Hack Your State Department Act."Congress.gov, Library of Congress, 23 January 2019,<https://www.congress.gov/bill/116th-congress/house-bill/328/summary/53>.

"State Department Computers Hacked." CBS News. CBS Interactive, 12 July 2006. Web. 21 April 2023.

Swan, Betsy Woodruff, and Natasha Bertrand. "Russia Suspected of Stealing Thousands of State Department Emails." POLITICO. POLITICO, 30 Mar. 2021. Web. 21 April 2023.

"Text - H.R.328 - 116th Congress (2019-2020): Hack Your State Department Act."Congress.gov, Library of Congress, 23 January 2019, <https://www.congress.gov/bill/116th-congress/house-bill/328/text>.

Varrock. "The Government Wants You...to Hack It?" Technology and Operations Management. 13 Nov. 2018. Web. 21 Aprile 2023

Alcott, Hillary J. Cleckler, author. Recent developments in cybersecurity / writers, Hillary J. Cleckler Alcott, Tyler Allard. Annapolis, Maryland : Department of Legislative Services, Office of Policy Analysis, [2022]

S.536 - 115th Congress (2017-2018): Cybersecurity Disclosure Act of 2017. (2018, June 28). <https://www.congress.gov/bill/115th-congress/senate-bill/536>

Congressional Record. (2023, April 21). <https://www.congress.gov/congressional-record/volume-166/issue-127/house-section/article/H3114-2>