The IoT Cybersecurity Improvement Act of 2020

CYSE 406

Jordan Sustarsic

December 1st, 2023

Considering how quickly cybersecurity threats are changing, protecting the country's digital infrastructure must come first. It is critical to inform voters about the proactive steps being taken to address cybersecurity concerns as the upcoming reelection bid draws near. As per your request, I have located a noteworthy legislative measure called the "IoT Cybersecurity Improvement Act of 2020" that not only highlights our dedication to cybersecurity but also offers an engaging story for voter participation.

Introduction

Enacted as Public Law No: 116-207, the IoT Cybersecurity Improvement Act is a vital countermeasure to the growing risks associated with the extensive utilization of Internet of Things (IoT) devices in federal agencies.

Summary of the Law

This law provides a thorough framework for improving the security of IoT devices used by the federal government. The law, which can be found here, provides federal agencies with guidelines regarding the need for particular security measures, vulnerability management, and the reporting of vulnerabilities related to Internet of Things devices.

The Problem and Background

Because IoT devices are so commonplace—from smart home appliances to vital infrastructure parts—cyber threats now face a whole new level of competition. Because many of these devices don't have strong security safeguards, they can be easily exploited. Recognizing the possible effects of compromised IoT devices on national security, the law addresses the urgent need to strengthen the cybersecurity posture of federal agencies.

Effectiveness and Potential Improvements

An admirable step toward reducing the risks connected to IoT devices is the IoT Cybersecurity Improvement Act. The law aims to stop bad actors from taking advantage of holes in federal systems by creating a baseline of security requirements. To ensure the law stays effective in the face of changing cybersecurity landscapes, it will be essential to conduct ongoing evaluations and updates.

Constituents may find the law's emphasis on transparency to be relatable. Federal agencies are mandated to keep an inventory of IoT devices along with information on the security measures that have been put in place. Voters may be greatly impacted by our commitment to transparency and accountability in government operations, which is why we are communicating this provision.

The statute also emphasizes how crucial it is for industry and governmental stakeholders to work together. In addition to being essential, this cooperative strategy is a prime example of how bipartisan efforts can be used to tackle the intricate problems in the field of cybersecurity.

Conclusion

In conclusion, our commitment to cybersecurity is demonstrated by the IoT Cybersecurity Improvement Act of 2020. We may effectively communicate to constituents our proactive approach to safeguarding the country's digital infrastructure by conveying its transparent approach, collaborative nature, and dedication to tackling emerging threats. This legislation offers a strong basis, and its story line is consistent with our dedication to working across party lines and promoting openness in public policy. Highlighting these points will certainly resonate with voters as we get ready for the election and demonstrate our commitment to bolstering national security through legislative action.

Works Cited

U.S. Congress. (2020). IoT Cybersecurity Improvement Act of 2020. Link.