

117TH CONGRESS
1ST SESSION

S. RES. 410

Supporting the goals and ideals of National Cybersecurity Awareness Month to raise awareness and enhance the state of cybersecurity in the United States.

IN THE SENATE OF THE UNITED STATES

OCTOBER 7, 2021

Mr. PETERS (for himself, Mr. CASSIDY, Ms. ROSEN, Mr. ROUNDS, Mr. CORNYN, Mr. KING, and Ms. HASSAN) submitted the following resolution; which was referred to the Committee on Homeland Security and Governmental Affairs

NOVEMBER 2, 2021

Committee discharged; considered and agreed to

RESOLUTION

Supporting the goals and ideals of National Cybersecurity Awareness Month to raise awareness and enhance the state of cybersecurity in the United States.

Whereas internet-based devices are present in every aspect of life for many people in the United States, with constant connection providing opportunities for innovation and modernization;

Whereas the COVID–19 pandemic forced daily aspects of societal life to online environments that are vulnerable to cyber attacks;

Whereas the number of cellular Internet of Things (commonly referred to as “IoT”) connections is expected to reach 3,500,000,000 in 2023, increasing at an annual growth rate of 30 percent;

Whereas a connected society is subject to cybersecurity threats that can compromise even the most personal and sensitive of information;

Whereas connected critical infrastructure is subject to cybersecurity threats that can compromise fundamental economic and health and safety functions;

Whereas malware is any malicious software that can be used to compromise the integrity of an electronic device, including the various types of software that give cyber criminals unique methods to monitor and control online activity or steal personal information or other sensitive data, such as—

- (1) adware;
- (2) botnets;
- (3) ransomware;
- (4) rootkits;
- (5) spyware;
- (6) Trojans;
- (7) viruses; and
- (8) worms;

Whereas the Federal Bureau of Investigation received more than 2,000 ransomware complaints in 2020 accounting for nearly \$30,000,000 in losses;

Whereas social engineering to trick individuals to give up their credentials, often through phishing attacks, can allow attackers to access personal information and accounts, leading to substantial harm;

Whereas public Wi-Fi hotspots can be convenient, but are not always secure, and may expose anyone connected to the network to a malicious cyberattack;

Whereas there were more than 2,000,000 cybercrimes reported to the Federal Bureau of Investigation in 2020 equating to more than \$4,000,000,000 in losses;

Whereas everyone can take simple steps to minimize the chance of a cybercrime, including—

- (1) setting strong passwords;
- (2) using multi-factor authentication;
- (3) installing updates;
- (4) understanding privacy settings;
- (5) backing up data; and
- (6) thinking critically and carefully about online offers;

Whereas National Cybersecurity Awareness Month is a collaborative effort between government and industry—

- (1) to raise awareness about the importance of cybersecurity;
- (2) to provide education to public and private sector partners through events and initiatives;
- (3) to ensure that public and private sector partners, and all people of the United States, have the tools and resources needed to be safer and more secure online; and
- (4) to increase the resilience of the United States in the event of a cyber incident;

Whereas, in 2021, National Cybersecurity Awareness Month will emphasize personal accountability and the importance of taking proactive steps to enhance cybersecurity at home and in the workplace, focusing on key areas such as—

- (1) cyber hygiene;

- (2) phishing scams; and
- (3) cybersecurity trainings;

Whereas the theme of National Cybersecurity Awareness Month in 2021 is “Do Your Part. #BeCyberSmart.”;

Whereas there are approximately 500,000 unfilled cybersecurity jobs in the United States; and

Whereas the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security works with public sector, private sector, and government partners—

- (1) to share information;
- (2) to build greater trust; and
- (3) to lead the national effort to protect and enhance the resilience of the physical and cyber infrastructure of the United States: Now, therefore, be it

1 *Resolved*, That the Senate—

2 (1) supports the goals and ideals of National
3 Cybersecurity Awareness Month;

4 (2) commits to continuing to work with Federal
5 agencies, State, local, tribal, and territorial govern-
6 ments, businesses, educational institutions, and
7 other organizations to enhance the state of cyberse-
8 curity in the United States; and

9 (3) recognizes October as National Cybersecu-
10 rity Awareness Month in 2021, with the theme “Do
11 Your Part. #BeCyberSmart.”, as an opportunity—

12 (A) to provide education to the people of
13 the United States about cybersecurity; and

1 (B) to help all people of the United States
2 be safer, more secure, and more aware while
3 online and using connected devices.

○