

113TH CONGRESS
1ST SESSION

H. RES. 399

Supporting the goals and ideals of National Cyber Security Awareness Month and raising awareness and enhancing the state of cybersecurity in the United States.

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 30, 2013

Mr. LANGEVIN submitted the following resolution; which was referred to the Committee on Science, Space, and Technology

RESOLUTION

Supporting the goals and ideals of National Cyber Security Awareness Month and raising awareness and enhancing the state of cybersecurity in the United States.

Whereas the use of the Internet in the United States to communicate, conduct business, or generate commerce that benefits the overall United States economy is ubiquitous;

Whereas many people use the Internet in the United States to communicate with family and friends, manage finances and pay bills, access educational opportunities, work remotely, shop at home, participate in online entertainment and games, and stay informed of news and current events;

Whereas the exponential growth of these services has led to a concomitant increase in the amount of personal data stored electronically;

Whereas the avenues to attack repositories holding these data have correspondingly increased and led to significant financial and personal privacy losses through theft and fraud;

Whereas the intellectual property, including proprietary information, copyrights, patents, trademarks, and related information, of business, academic institutions, government, and individuals are vital to the economic security of the United States;

Whereas the theft of intellectual property in the United States likely results in the loss of over \$300,000,000,000 per year, according to the Commission on the Theft of American Intellectual Property;

Whereas this massive illicit activity is facilitated by advanced persistent threats and other state and non-state cyber actors;

Whereas United States small businesses, which employ a significant fraction of the private workforce, increasingly rely on the Internet to manage their businesses, expand their customer reach, and enhance the management of their supply chain;

Whereas studies have shown that small businesses are frequently the target of cyberattacks due to their less comprehensive defenses and that small businesses incur a significantly higher per capita cost per cyber incident than do larger companies;

Whereas critical infrastructure systems in the United States rely on the secure and reliable operation of information

networks to support the United States Armed Forces, civilian government, energy, telecommunications, financial services, transportation, health care, and emergency response systems;

Whereas critical infrastructure owners and operators face a growing threat of cyberattack as evidenced by increasingly sophisticated and destructive attacks and the denial of service attacks perpetrated on financial institutions;

Whereas research tools continue to reveal the large number of industrial control systems and other critical information infrastructure connected to the Internet;

Whereas nearly all public schools in the United States have Internet access to enhance education, with a significant percentage of instructional rooms connected to the Internet to provide access to educational online content and encourage self-initiative to discover research resources;

Whereas the number of children who connect to the Internet continues to rise, and teaching children of all ages to become good cyber-citizens through safe, secure, and ethical online behaviors and practices is essential to protect their computer systems and potentially their personal safety;

Whereas in addition to increasing personal safety and web hygiene, cybersecurity education initiatives can foster an interest in the discipline that may culminate in matriculation into a cybersecurity occupation helping to ease the shortage of qualified professionals;

Whereas national organizations, policymakers, government agencies, private sector companies, nonprofit institutions, schools, academic organizations, consumers, and the media recognize the need to increase awareness of cyber-

security and the need for enhanced cybersecurity in the United States;

Whereas coordination between the numerous Federal agencies involved in cybersecurity efforts is essential to securing the cyber infrastructure of the United States;

Whereas the National Strategy to Secure Cyberspace, published in February 2003, recommends a comprehensive national awareness program to empower all people in the United States, including businesses, the general workforce, and the general population, to secure their own parts of cyberspace;

Whereas the White House's Cyberspace Policy Review, published in May 2009, recommends that the United States Government initiate a national public awareness and education campaign to promote cybersecurity;

Whereas "STOP. THINK. CONNECT." is the national cybersecurity awareness campaign founded and led by the National Cyber Security Alliance and the Anti-Phishing Working Group as a public-private partnership with the Department of Homeland Security to help all digital citizens stay safer and more secure online;

Whereas the National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology, is the coordinating body for the Federal Government to establish a sustainable, operational, and continually improving cybersecurity education program to enhance the Nation's cybersecurity and support the development of a professional cybersecurity workforce and cyber-capable citizens; and

Whereas the National Cyber Security Alliance, the Multi-State Information Sharing and Analysis Center, the De-

partment of Homeland Security, and other organizations working to improve cybersecurity in the United States have designated October 2013 as the tenth annual National Cyber Security Awareness Month in order to educate the people of the United States about the importance of cybersecurity: Now, therefore, be it

1 *Resolved*, That the House of Representatives—

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

4 (2) continues to work with Federal agencies,
5 businesses, educational institutions, and other orga-
6 nizations to enhance the state of cybersecurity in the
7 United States;

8 (3) commends the work of the National Initia-
9 tive for Cybersecurity Education and all the Federal
10 agencies, nonprofits, educational institutions, busi-
11 nesses, and other organizations that support this ef-
12 fort;

13 (4) recognizes “STOP. THINK. CONNECT.”
14 as the national cybersecurity awareness campaign to
15 educate people of the United States and help all citi-
16 zens stay safer and more secure online; and

17 (5) congratulates the National Cyber Security
18 Alliance, the Multi-State Information Sharing and
19 Analysis Center, the Department of Homeland Secu-
20 rity, and other organizations working to improve cy-
21 bersecurity in the United States on the tenth anni-

- 1 versary of the National Cyber Security Awareness
- 2 Month.

