112TH CONGRESS
1ST SESSION

H. RES. 446

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

IN THE HOUSE OF REPRESENTATIVES

OCTOBER 24, 2011

Mr. LANGEVIN (for himself, Mr. MCCAUL, Mr. DANIEL E. LUNGREN of California, Mr. STIVERS, Mr. CICILLINE, Mr. RUPPERSBERGER, Ms. RICHARDSON, Mrs. MYRICK, Ms. SPEIER, and Ms. CLARKE of New York) 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 cyber security 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 the United States technological knowhow, innovation, and entrepreneurship are all digitally connected and the pace of innovation has accelerated, so too have the methods to attack the Nation's economic prosperity and security, spawning new, high-tech challenges, from identity theft to corporate hacking to cyber bullying;

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

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 the cost of cyber crime to private businesses rose 56 percent from 2010, costing organizations on average $5,900,000 and that small businesses incur a significantly higher per capital cost than larger companies according to a report by the Ponemon Institute;

Whereas nearly all public schools in the United States have Internet access to enhance children's education, with a significant percentage of instructional rooms connected to the Internet to enhance children's education by providing access to educational online content and encouraging 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 physical safety;

Whereas the growth and popularity of social networking Web sites has attracted millions of teenagers, providing access to a range of valuable services, making it all the more important to teach young users how to avoid potential

threats like cyber bullies, predators, and identity thieves they may come across while using such services;

Whereas cyber security is a critical part of the United States national security and economic security;

Whereas to prepare the United States Armed Forces for emerging cyber threats, the Department of Defense developed a Cyber Strategy that is focused on treating cyberspace as an operational domain to organize, train, and equip forces, employing new defense operating concepts, partnering with United States Government departments, Federal agencies, and the private sector to enable a whole-of-government approach, building robust international partnerships to strengthen collective cybersecurity, and fully growing cyber work force talents and leveraging new technological innovations;

Whereas the United States critical infrastructures and economy 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 Internet users and information infrastructure owners and operators face an increasing threat of cybercrime and fraud attacks through viruses, worms, Trojans, and malicious programs such as spyware, adware, hacking tools, and password stealers, that are frequent and fast in propagation, are costly to repair, and may disable entire systems;

Whereas the intellectual property, including proprietary information, copyrights, patents, trademarks, and related information, of business, academic institutions, govern-

ment, and individuals are vital to the economic security of the United States;

Whereas millions of records containing personally identifiable information have been lost, stolen, or breached, threatening the security and financial well-being of United States citizens;

Whereas consumers face significant financial and personal privacy losses due to personally identifiable information being more exposed to theft and fraud than ever before;

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 cyber security in the United States;

Whereas coordination between the numerous Federal agencies involved in cyber security 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, the Anti-Phishing

Working Group as a public private partnership with the Department of Homeland Security, and a coalition of private companies, nonprofits, and government organizations 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 cyber security workforce and cyber-capable citizens;

Whereas the United States Cyber Challenge initiative is working to identify 10,000 of the Nation's best and brightest to fill the ranks of cybersecurity professionals where their skills can be of the greatest value to the Nation; and

Whereas the National Cyber Security Alliance, the Multi-State Information Sharing and Analysis Center, the Department of Homeland Security, and other organizations working to improve cyber security in the United States have designated October 2011 as the eighth annual National Cyber Security Awareness Month which serves to educate the people of the United States about the importance of cyber security: Now, therefore, be it

Resolved, That the House of Representatives—

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

(2) continues to work with Federal agencies, businesses, educational institutions, and other orga-

nizations to enhance the state of cybersecurity in the United States;

(3) commends the work of the National Initiative for Cybersecurity Education and all the Federal agencies, nonprofits, educational institutions, businesses, and other organizations that support this effort;

(4) recognizes ''STOP. THINK. CONNECT.'' as the national cybersecurity awareness campaign to educate people of the United States and help all citizens stay safer and more secure online; and

(5) congratulates the National Cyber Security Alliance, the Multi-State Information Sharing and Analysis Center, the Department of Homeland Security, and other organizations working to improve cyber security in the United States on the eighth anniversary of the National Cyber Security Awareness Month.

○