110TH CONGRESS
2D SESSION

H. CON. RES. 425

Expressing the sense of Congress regarding the need to pass meaningful legislation to protect commercial and government data from data breaches.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 24, 2008

Mr. BURGESS (for himself and Mr. GONZALEZ) submitted the following concurrent resolution; which was referred to the Committee on Science and Technology, and in addition to the Committee on Oversight and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

CONCURRENT RESOLUTION

Expressing the sense of Congress regarding the need to pass meaningful legislation to protect commercial and government data from data breaches.

Whereas over 225 million records have been subject to a data breach in the United States since 2005;

Whereas almost 8.4 million adults in the United States were victims of identity fraud in 2007;

Whereas 66 percent of breaches involve data that the victim was unaware existed on the system;

Whereas data breaches occur in a wide rage of institutions, including government, military, education, health care companies, banking, and credit and financial services;

Whereas, in 2007, the number of data security breaches at colleges and universities increased over 67 percent from 2006, and the number of educational institutions affected increased over 72 percent;

Whereas the Department of the Interior, the Nuclear Regulatory Commission, the Department of Treasury, the Department of Veterans Affairs, and the Department of Agriculture all scored an ''F'' on the 2007 Federal Security Report Card;

Whereas a data breach at the Department of Veterans Affairs in 2006 put 26.5 million veterans' names, addresses, and Social Security numbers at risk;

Whereas, in 2008, medical data of over 3,000 patients at the National Institutes of Health was stolen from an unencrypted government laptop;

Whereas, in 2006, three systems at the United States Department of Agriculture were compromised, potentially making available the names, Social Security numbers, and photos of 26,000 U.S.D.A. employees, contractors, and retirees;

Whereas, since 2001, the Department of Commerce previously reported to the House Committee on Government Reform that a total of 1,137 department laptops have been stolen, lost, or reported missing;

Whereas the Government Accountability Office found in 2008 that significant control weaknesses continue to threaten the confidentiality, integrity, and availability of the Securities and Exchange Commission's financial and sensitive information and information systems, and the S.E.C. has not consistently implemented effective controls to prevent,

limit, or detect unauthorized access to computing resources;

Whereas the requested fiscal year 2009 Federal budget across all agencies for information technology security of $7.2 billion, an increase of $600 million over the fiscal year 2008 budget, has yet to be enacted;

Whereas the Department of Homeland Security has the lead responsibility for assuring the security, resiliency and reliability of the Nation's information technology and communications infrastructure with only a requested budget of $247 million for the Office of the Chief Information Officer;

Whereas the Department of Homeland Security's Chief Information Officer, who has primary oversight of information technology projects and reviews and approves all information technology, currently has no established qualifications for appointment as authorized by Congress;

Whereas the Inspector General of the Department of Homeland Security reports that the department has not completed all the steps to produce a prioritized inventory of its internal cyber critical infrastructure and the department's Management Directorate has not been coordinating related efforts to secure these assets;

Whereas, in 2006, Congress suffered computer attacks from a foreign government where information was stolen;

Whereas data breaches are caused by a variety of sources, including 73 percent from external sources, 18 percent caused by insiders, 39 percent by business partners, and 30 percent where multiple parties are involved;

Whereas data breaches occur in a variety of ways, including 62 percent attributed to significant error, 58 percent re-

sulted from hacking and intrusions, 31 percent from malicious code, 22 percent exploited a vulnerability, and 15 percent were due to physical threats;

Whereas cyber crime is a growing international business that presents a fundamental threat to the Internet;

Whereas 36 States have recognized the threat that data breaches pose and have taken steps to pass their own data security legislation;

Whereas the total cost of the data security crisis to business and consumers is approaching $50 billion annually, with the average breach costing a consumer $1,200 and a business $5 million;

Whereas 87 percent of breaches are considered avoidable if reasonable controls had been in place; and

Whereas solutions to these threats exist in the marketplace for relatively low cost: Now, therefore, be it

Resolved by the House of Representatives (the Senate concurring), That it is the sense of Congress that Congress should—

(1) before final adjournment of the 110th Congress, pass meaningful legislation to protect commercial and government data, which includes a robust definition of encryption tied to National Institute of Standards and Technology standards and requires leadership at the top levels of an organization to take an active role in ensuring that their systems are secure; and

(2) encourage leaders of government agencies and private enterprises to take responsibility for the data collected and stored within their institution by making data security a top priority within the institution.

○