

White House mulls move as cybersecurity bill fails (Update)

November 15 2012, by Rob Lever



The White House said it was considering an executive order on cybersecurity after legislation on infrastructure protection failed again in the Senate.

The White House said Thursday it was considering an executive order on cybersecurity after legislation on infrastructure protection failed again in the Senate.

"The president is determined to protect our nation against cyber threats,"

said Caitlin Hayden, spokeswoman for the White House National Security Council after Wednesday's failure in the Senate of a bill aimed at protecting US "critical infrastructure" from cyber attacks.

Hayden said the White House was exploring ways "to more effectively secure the nation's critical infrastructure by working collaboratively with the private sector" and that this may result in an executive order.

She said such an order "is not a substitute for new legislation" and "doesn't create new powers or authorities (but) it does set policy under existing law."

In the lame-duck session, the bill backed by President Barack Obama failed to get the 60 votes needed to proceed under Senate rules. It was backed by a 51-47 vote.

The failure of the bill for the second time in three months prompted political sniping from supporters and detractors.

"Once again, Senate Republicans have chosen to filibuster much-needed cybersecurity legislation and, in so doing, have ignored the advice of the country's most senior military and national security officials," said Senator Jay Rockefeller, a key backer of the measure.

"Republican members have once again sided with the Chamber of Commerce, and not our military officials, on a national security issue."

Republican Senator Charles Grassley, however, claimed the bill was "flawed" and failed to see adequate debate.

"No one disputes the need for Congress to address cybersecurity," Grassley said.

"However, members do disagree with the notion this problem requires legislation that increases the size of the federal government bureaucracy and places new burdens and regulation on businesses."

The measure was blocked amid opposition from an unusual coalition of civil libertarians—who feared it could allow too much government snooping—and conservatives who said it would create a new bureaucracy.

US military officials have argued that legislation is needed to protect infrastructure critical to safeguarding national defense, including power grids, water systems and industries ranging from transportation to communication.

Senator Susan Collins, a Republican who supported the bill, said the issue remains of critical importance.

"Every day that we wait, our country becomes more vulnerable to a serious cyber attack, indeed a catastrophic attack," she said in a statement.

"Experts have also repeatedly warned that the computer systems that run our critical infrastructure—our electric grid, pipelines, water systems, financial networks, and transportation systems—are vulnerable to a major cyber attack."

Some industry leaders expressed disappointment on the failure of the bill.

"Stalemate doesn't make the issue go away," said Software Alliance president Robert Holleyman.

"There is no getting around the fact that we need to bolster America's

cybersecurity capabilities. We urge both parties to put this issue at the top of the agenda in the next Congress."

The Electronic Frontier Foundation, which promotes online freedoms, called the Senate bill "dangerously vague" and a threat to privacy.

"We're looking forward to having a more informed debate about cybersecurity next session, and hope Congress will bear in mind the serious privacy interests of individual Internet users," said EFF attorney Lee Tien.

"We don't need to water down existing privacy law to address the challenges of cybersecurity."

In a related matter, the White House confirmed reports this week that Obama signed a directive which can help the US military thwart cyber attacks.

"This step is part of the administration's focus on cybersecurity as a top priority. The cyber threat has evolved since 2004, and we have new experiences to take into account," a senior US official said.

"The directive itself is classified, so we cannot discuss all of the elements contained in it," the official said, adding that it "establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools we have at our disposal."

(c) 2012 AFP

Citation: White House mulls move as cybersecurity bill fails (Update) (2012, November 15) retrieved 12 May 2024 from <https://phys.org/news/2012-11-sniping-cybersecurity-bill.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.