

Panel urges better cybersecurity to President-elect Trump (Update)

December 2 2016, by Tami Abdollah And Darlene Superville



In this Feb. 17, 2016, file photo, President Barack Obama, joined by from left, Commerce Secretary Penny Pritzker, former IBM CEO Sam Palmisano, former National Security Adviser Tom Donilon, and Homeland Security Secretary Jeh Johnson, talks to media in the Oval Office of the White House, in Washington. Donilon, and Palmisano, are being appointed as the Chair and Vice Chair, respectively, of the Commission on Enhancing National Cybersecurity. A national commission is delivering urgent recommendations to improve the nation's cybersecurity, weeks before President-elect Donald Trump takes office. The report follows the worst hacking of U.S. government systems in history and the Obama administration accusing Russia of meddling in the U.S. presidential election by hacking Democrats. (AP Photo/Carolyn Kaster, File)

A presidential commission on Friday made 16 urgent recommendations to improve the nation's cybersecurity, including creating a nutritional-type label to help consumers shop wisely and appointing a new international ambassador on the subject—weeks before President-elect Donald Trump takes office.

The release of the 100-page report follows the worst hacking of U.S. government systems in history and accusations by the Obama administration that Russia meddled in the U.S. presidential election by hacking Democrats.

The Presidential Commission on Enhancing National Cybersecurity urged immediate action within two to five years and suggested the Trump administration consider acting on some proposals within its first 100 days.

The commission recommended that Trump create an assistant to the president for cybersecurity, who would report through the national security adviser, and establish an ambassador for cybersecurity, who would lead efforts to create international rules. It urged steps, such as getting rid of traditional passwords, to end the threat of identity theft by 2021 and said Trump's administration should train 100,000 new cybersecurity workers by 2020.

Other ideas included helping consumers to judge products using an independent nutritional-type label for technology products and services.

"What we've been doing over the last 15 to 20 years simply isn't working, and the problem isn't going to be fixed simply by adding more money," said Steven Chabinsky, a commission member and the global chair of the data, privacy and cybersecurity practice for White & Case LLP, an international law firm.

He said the group wanted the burden of cybersecurity "moved away from every computer user and handled at higher levels," including internet providers and product developers who could ensure security by default and design "for everyone's benefit."

The White House requested the report in February and intended it to serve as a transition memo for the next president. The commission included 12 of what the White House described as the brightest minds in business, academia, technology and security. It was led by Tom Donilon, Obama's former national security adviser.

The panel studied sharing information with private companies about cyber threats, the lack of talented American security engineers and distrust of the U.S. government by private businesses, especially in Silicon Valley. Classified documents stolen under Obama by Edward Snowden, a contractor for the National Security Agency, revealed government efforts to hack into the data pipelines used by U.S. companies to serve customers overseas.

One commissioner, Herbert Lin of Stanford University, said some senior information technology managers distrust the federal government as much as they distrust China, widely regarded as actively hacking in the U.S.

President Barack Obama said in a written statement after meeting with Donilon that his administration will take additional action "wherever possible" to build on its efforts make progress before he leaves office next month. He urged Trump and the next Congress to treat the recommendations as a guide.

"Now it is time for the next administration to take up this charge and ensure that cyberspace can continue to be the driver for prosperity, innovation, and change both in the United States and around the world,"

Obama said.

It was not immediately clear whether Trump would accept the group's recommendations. Trump won the election on promises to reduce government regulations, although decades of relying on market pressure or asking businesses to voluntarily make their products and services safer have been largely ineffective.

Trump's presidential campaign benefited from embarrassing disclosures in hacked emails stolen from the Democratic National Committee, Hillary Clinton's campaign staff and others, and Trump openly invited Russian hackers to find and release tens of thousands of personal emails that Clinton had deleted from the private server she had used to conduct government business as secretary of state. He also disputed the Obama administration's conclusion that Russia was responsible for the Democratic hackings.

Though Trump is a prolific user of online social media services, especially Twitter, he is rarely seen using a computer. His campaign manager, Kellyanne Conway, tweeted a photograph Monday of Trump working on an Apple laptop inside his office at Trump Tower. He testified in a deposition in 2012 that he did not own a personal computer or smartphone, and in another deposition earlier this year said he deliberately does not use email.

Trump has already promised his own study by a "Cyber Review Team" of people he said he will select from military, law enforcement and private sectors. He said his team will develop mandatory cyber awareness training for all U.S. government employees, and he has proposed a buildup of U.S. military offensive and defensive cyber capabilities that he said will deter foreign hackers.

The new report suggested that the government should remain the only

organization responsible for responding to large-scale attacks by foreign countries.

Obama has a mixed legacy on cybersecurity.

Under Obama, hackers stole personal data from the U.S. Office of Personnel Management on more than 21 million current, former and prospective government employees, including details of security-clearance background investigations for federal agents, intelligence employees and others. The White House also failed in its efforts to convince Congress to pass a national law—similar to laws passed in some states—to require hacked companies to notify affected customers.

But the Obama administration also became more aggressive about publicly identifying foreign governments it accused of hacking U.S. victims, arrested some high-profile hackers overseas, successfully shut down some large networks of hacked computers used to attack online targets, enacted but never actually used economic sanctions against countries that hacked American targets and used a sophisticated new cyberweapon called Stuxnet against Iran's main nuclear enrichment facilities.

Congress passed a new law in late 2015 to encourage companies and the government to share information about online threats.

More information: www.nist.gov/sites/default/files/2016/12/eport-final-post.pdf

© 2016 The Associated Press. All rights reserved.

Citation: Panel urges better cybersecurity to President-elect Trump (Update) (2016, December 2) retrieved 26 April 2024 from

<https://phys.org/news/2016-12-white-house-broad-cybersecurity-effort.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.