

Title: **Branstad: Iowa needs cybersecurity**  
 Author: MATTHEW PATANE AND WILLIAM PETROSKI MPATANE@DMREG.COM  
 Size: 44.33 square inch  
 Des Moines, IA Circulation: 151448



# Branstad: Iowa needs cybersecurity

Governor signs executive order calling on state agencies to devise a plan for response to cyberattack

**MATTHEW PATANE  
AND WILLIAM PETROSKI**

MPATANE@DMREG.COM

Iowa Gov. Terry Branstad has ordered state officials to develop a strategy that would improve the state's cybersecurity awareness and response in case of a cyberattack.

Branstad signed an executive order Monday calling on the Office of the Chief Information Officer and

other state agencies to develop the plan and deliver a public report to his office by July 1.

Among other work, Branstad's order calls for the strategy to:

» Address high-risk cybersecurity areas of Iowa's infrastructure and develop plans to "better identify,

protect, detect, respond and recover" from cybersecurity incidents.

» Establish a process to regularly assess Iowa's cybersecurity infrastructure and activities.

» Provide recommendations on

**See SECURITY, Page 11A**

## SECURITY

Continued from Page 10A

how to secure networks, systems and data, and develop best practices to prevent unauthorized access, theft and destruction of state data.

Implement cybersecurity awareness training for state government.

Recommend science, technology, engineering and math (STEM) education and training in Iowa schools to "foster an improved cybersecurity workforce pipeline."

Establish data breach reporting and notification requirements.

Have Iowa Homeland Security update Iowa's emergency response plan to deal with the physical consequences of a cyberattack.

Jeff Franklin, Iowa's chief security information officer, will lead the effort.

The CIO's office will work

with the Iowa Homeland Security and Emergency Management Department, the Iowa Communications Network, the Iowa National Guard, the Department of Public Safety and others to develop the report.

Asked during a press conference Monday if there have been credible plots and threats foiled to date, Iowa Public Safety Commissioner Roxann Ryan said: "None that we can talk about."

Branstad said there are a lot of things that are top secret, and officials can't talk publicly about some matters.

"We just need to be very vigilant and update our systems so we can be as effective as possible in fighting these cyberattacks," Branstad said.

Some of their concerns involve law enforcement and public safety, as well as protecting

Iowa's electrical and natural gas systems, financial institutions and government agencies such as the Iowa Department of Revenue, Branstad said.

"We need to be aware of and prepared for all kinds of cyberattacks," Branstad said.

Cybersecurity experts have said state governments can make great targets for cyberattacks due to the wealth of information they hold about citizens.

Numerous recent cyberattacks have focused on private companies, but government agencies are not immune.

In 2010, hackers accessed the Iowa Racing & Gaming Commission's computer systems, compromising the information of 80,000 people. A data breach hit South Carolina's Department of Revenue in 2012.

Last year, Iowa State University said a hacker compromised

its servers in an attempt to generate enough computing power to mine bitcoins.

Earlier this year, the federal government said hackers breached the U.S. Office of Personnel Management resulting in the theft of more than 20 million records.

Branstad said he is especially aware of cybersecurity because he is co-chair of the Council of Governors, which is made up of 10 governors who work to strengthen state and federal ties relating to national security.

They will be drafting a state strategy to increase the state's resiliency to cyberattacks and will be updating the state's homeland security emergency response plan to better deal with the physical consequences of a cyberattack.



Terry  
Branstad