



cnsnews.com
THE RIGHT NEWS. RIGHT NOW.™

Legal Experts: Allowing DHS to Secure Elections Would Set a Dangerous Precedent

Barbara Hollingsworth

August 31, 2016

Homeland Security Secretary Jeh Johnson's suggestion that state and local voting systems be designated as “pieces of **critical infrastructure**” so that the U.S. Department of Homeland Security (DHS) can protect them from hackers is unconstitutional and would create a dangerous precedent, legal experts said.

“The Department of Homeland Security does not have the legal authority to interfere with states’ election systems without their permission,” **University of California/Berkeley School of Law Professor John Yoo** told CNSNews.com.

“While the federal government has the general power to protect the nation’s cyber infrastructure, it cannot intrude into areas of state sovereignty without clear constitutional mandate.

“Article I, Section 4 of the Constitution recognizes the authority of the states to regulate the times, places, manner of elections, subject to congressional regulation. As far as I am aware, Congress has not clearly decided to regulate the information systems of state electoral systems or delegated this authority to DHS,” Yoo noted.

“There is no federal power to control or secure elections. Each state administers its own elections, restricted only by constitutional protections for voting rights,” agreed **Ilya Shapiro**, senior fellow in constitutional studies at the **Cato Institute**.

“It may make sense for states to request federal support here, but it would set a dangerous precedent for a federal agency to unilaterally take over state electoral processes,” Shapiro said.

“It is unnecessary and uncalled for and potentially unconstitutional since the federal government doesn’t have the authority to administer elections, only to set the time, place, and manner of congressional elections,” **Hans von Spakovsky**, a senior legal fellow at **The Heritage Foundation**, told CNSNews.

The co-author of *Who’s Counting? How Fraudsters and Bureaucrats Put Your Vote at Risk*, said that “the realistic fear is that this is the first step towards nationalizing elections.”

“If Jeh Johnson wants to make recommendations to the states on improving security, he can do so without designating our election system as ‘critical infrastructure’ unless he wants to use that designation as a way of exerting control over our election administration process,” von Spakovsky told CNSNews.

The suggestion to designate voting systems as “critical infrastructure” was raised by Johnson at an August 3rd **breakfast conference** in Washington hosted by the *Christian Science Monitor*.

"We are actively thinking about election cybersecurity right now. The issue with the election process, as you know, there's no one federal election system. There are some 9,000 jurisdictions across this country involved in the election process, so when there's a national election for president, there are some 9,000 jurisdictions that participate and contribute to collecting votes, tallying votes, and reporting votes," Johnson told conference attendees.

“States, cities, counties who all have their own way of doing business, down to the nature of the ballots, the nature of how votes are collected and tabulated,” he said.

“We should carefully consider whether our election system, our election process, is critical infrastructure like the financial sector, like the power grid," Johnson continued. “There's a vital national interest in our election process, so I do think we need to consider whether it should be considered by my department and others critical infrastructure.”

An **August 15 press release** stated that “DHS is not aware of any specific or credible cybersecurity threats relating to the upcoming general election systems.”

White House spokesman Josh Earnest **told reporters** on Monday that designating voting systems as critical infrastructure would give federal technology experts at DHS “more of a role in assisting the administrators of those networks as they deter intrusions.”

On August 18, the FBI issued an alert, saying that it had found breaches in voter registration databases on State Board of Elections websites in **Arizona and Illinois**.

But von Spakovsky pointed out that the voting systems in those two states were vulnerable to hackers because they allow online registration.

“The problems in Arizona and Illinois were caused by implementing online voter registration, a very bad idea, since that gives hackers a road into the voter registration system,” he told CNSNews. “Stop online registration immediately and the problem is solved.”

Decentralization also makes the American election system impervious to large-scale hacking, another legal expert pointed out.

"Homeland security is critical, but it is also critical that the Department of Homeland Security knows and respects its limits," said **Capital University Law School Professor Bradley Smith**.

"One of the great strengths of the American election system is that there is no national network or infrastructure that can be taken down. Hacks of isolated local systems can occur, but the system is so thoroughly decentralized that it is all but immune to any system-wide or systematic attack," he pointed out.

Keeping the federal government out of elections will ensure that any problems “remain isolated and local,” Smith said.

Last July, the director of the federal Office of Personnel Management (OPM) **resigned** after cyberhackers got past **Einstein**, DHS’ multi-billion-dollar cyberhacker intrusion and prevention system, and stole the personal data of 21.5 million current and former federal employees -

including their addresses, Social Security numbers, financial and military records, and security clearances - from OPM's Central Personnel Data File.