

Top News

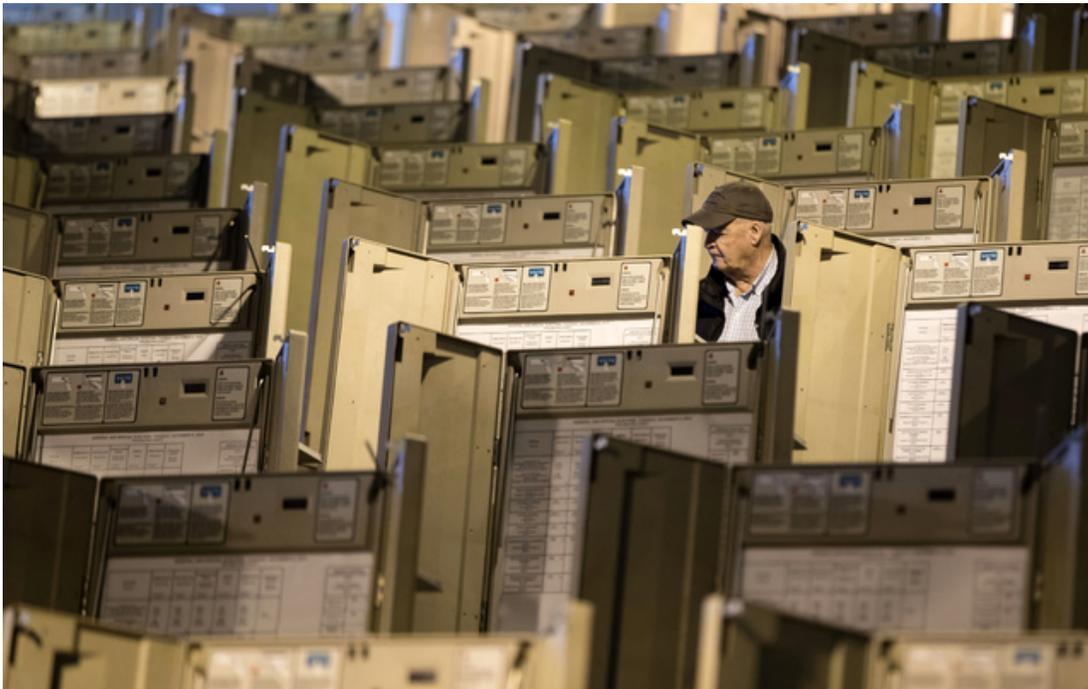
State election systems to get more federal aid for security

Associated Press

Posted January 06, 2017

January 6, 2017

Updated January 6, 2017 9:30pm



ASSOCIATED PRESS / OCT. 14

A technician worked to prepare voting machines to be used in the presidential election in Philadelphia.

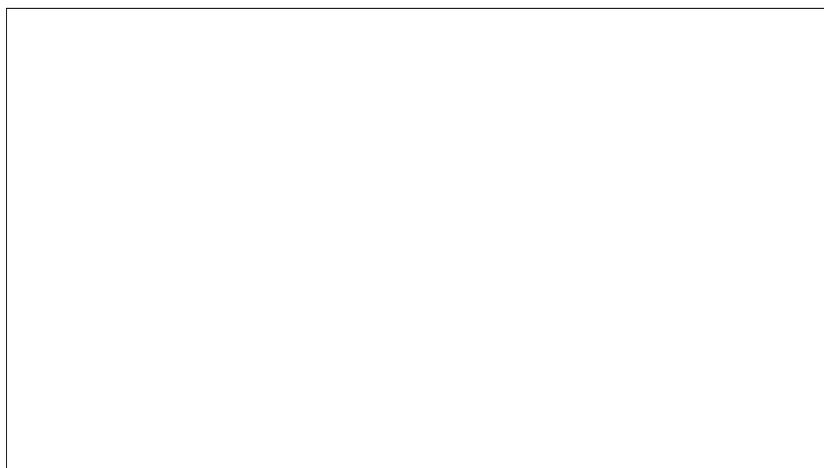
WASHINGTON >> Citing increasingly sophisticated cyber bad actors and an election infrastructure that's "vital to our national interests," Homeland Security Secretary Jeh Johnson is designating U.S. election systems critical infrastructure, a move that

provides more federal help for state and local governments to keep their election systems safe from tampering.

“Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law,” Johnson said in a statement today. He added: “Particularly in these times, this designation is simply the right and obvious thing to do.”

The determination came after months of review and despite opposition from many states worried that the designation would lead to increased federal regulation or oversight on the many decentralized and locally run voting systems across the country. It was announced on the same day a declassified U.S. intelligence report said Russian President Vladimir Putin “ordered” an influence campaign in 2016 aimed at the U.S. presidential election.

ADVERTISING



inRead invented by Teads

The declassified report said that Russian intelligence services had “obtained and maintained access to elements of multiple U.S. state or local electoral boards.” None of the systems targeted or compromised was involved in vote tallying, the report said.

A 2013 presidential directive identified 16 sectors as critical infrastructures, including energy, financial services, health care, transportation, food and agriculture and communications.

The designation announced today places responsibilities on the Homeland Security secretary to identify and prioritize those sectors, considering physical and cyber threats against them. The secretary is also required to conduct security checks and provide information about emerging and imminent threats.

Such a change does not require presidential action, and only requires the secretary to first consult with the assistant to the president for homeland security and counterterrorism.

Discussions about whether to designate elections systems as critical infrastructure surfaced after hackers targeted the voter registration systems of more than 20 states in the months prior to the November election.

While the designation puts responsibilities on the Department of Homeland Security, it does not require entities that are determined “critical infrastructure” to participate. Much of the nation’s critical infrastructure is in the private sector.

Johnson said election infrastructure included storage facilities, polling places and vote tabulation locations, plus technology involved in the process, including voter registration databases, voting machines and other systems used to manage the election process and report and display results.

The designation allows for information to be withheld from the public when state, local and private partners meet to discuss election infrastructure security — potentially injecting secrecy into an election process that’s traditionally and expressly a transparent process. U.S. officials say such closed door conversations allow for frank discussion that would prevent bad actors from learning about vulnerabilities. DHS would also be able to grant security clearances when appropriate and provide more detailed threat information to states.

The Obama administration has proposed international cyber rules for peacetime that would expressly note that countries shouldn’t conduct online activity targeting critical infrastructure, which will now also include election systems.

President Barack Obama used sanctions last week to retaliate against Russian efforts to interfere in the U.S. election process by expanding a prior executive order that allows for their use in the case of cyberattack on critical infrastructure to entities “interfering with or undermining election processes or institutions.” With election infrastructure designated as critical, an attack that takes the system down would also qualify for a response of sanctions.

Rep. Bennie G. Thompson of Mississippi, who is the ranking Democrat on the House Homeland Security Committee, commended Johnson’s action and said, “In the long term, this will put our electoral systems on a more secure footing and maintain public confidence in our elections.”

Rep. Jim Langevin, a Rhode Island Democrat and co-chairman of the Congressional Cybersecurity Caucus, said in a statement that the decision “demonstrates the vital need to ensure votes can’t be tampered with. We must also act as a nation to build our resilience against future information warfare attacks.”

Georgia Secretary of State Brian P. Kemp, who is a member of the U.S. Election Infrastructure Cybersecurity Working Group run by DHS, is among those who have opposed the designation. Testifying in September to a House Oversight subcommittee, Kemp said more federal oversight could make systems more vulnerable and could make protected records more accessible.

When Johnson discussed the likelihood of the designation in a conference call with state officials on Thursday, Kemp called the action “a federal overreach into a sphere constitutionally reserved for the states.” According to a copy of his comments released by his office, Kemp told Johnson on the phone that “this smacks of partisan politics” given the dwindling days left in the Obama administration.

Kemp has appealed to President-elect Donald Trump to investigate “failed cyberattacks” on the Georgia secretary of state’s network that traced to the Department of Homeland Security, calling the department’s technical explanations insufficient.

 **Get the latest news by email** [Sign Up](#)