From the Office of Secretary of State John A. Gale

www.sos.ne.gov

For Release:
August 30, 2016

Contact: Laura Strimple
402-471-8408

Sec. Gale assures election security is highest priority

LINCOLN – Recent events of potential voter registration database attacks in Arizona and Illinois and the FBI Flash Alert about targeting activity against state election systems have brought national attention to the issue of election cyber security for the coming November election, according to Secretary of State John Gale.

"Election security has been a matter of close attention in my office for 10 years. Election cyber security is not something new that has suddenly become a crisis," said Gale. "It is an ongoing process."

Gale said that potential breaches in Arizona and Illinois are not the first time states have been attacked by hackers. Gale said that his office takes multiple steps in each election cycle to identify possible vulnerabilities.

"It is a high priority," Gale said, noting that election and IT specialists from his office have been involved with election vendors and state officials since January.

"Problems or gaps that have been identified over the years have been resolved and this year we have been proceeding with the same type of security assessment. Security has tightened each election cycle, and new steps are being taken this year."

Nebraska coordinates with a number of vendors and state agencies to carry out voter registration and Election Day reporting processes. The Secretary of State's office launched NEReg2Vote, an online voter registration system in September 2015. The Department of Motor Vehicles (DMV) also started taking voter

registrations online a few months later. Information is passed through secure networks to Election Systems and Software (ES&S), the election system provider for Nebraska and multiple other states.

"We have had a close working relationship with all of our vendors and have been working together this year to close any potential gaps that we can identify," explained Gale.

Gale said that discussions involving security have also included ensuring that electronic transmission of tabulated results are simply for election night reporting, and do not reflect final results. Such transmission is handled with the highest protocol possible.

"If any attack were to disrupt election night reporting, it's not a threat to the official election results. We have the paper ballots to check against. No results of an election are ever official until the counties, and then the state, certifies the results of paper ballot tabulation to the State Canvassing Board. Wireless transmission is not allowed in this process."

Prior to every statewide primary and general election, election equipment and software used by the counties are tested in a process called a mock election. Sample ballots are randomly marked by county officials and machine tabulated. Those results are compared to a hand tabulation of the same ballots to confirm that results are accurate. Mock election results are then posted to a closed website, to ensure that the published results match those reported by the counties.

"After the election, a certain number of counties carry out a random audit of results in their precincts, to further confirm the accuracy of the election," said Gale.

Each process that is undertaken is meant to tighten up all the ropes.

"One can never be over-confident, but we feel very comfortable with our initiatives as we work toward a smooth November general election."

###