ANGUS S. KING, JR.
MAINE

133 HART SENATE OFFICE BUILDING
(202) 224-5344
Website: http://www.King.Senate.gov

United States Senate
WASHINGTON, DC 20510

COMMITTEES:
ARMED SERVICES
BUDGET
ENERGY AND
NATURAL RESOURCES
INTELLIGENCE
RULES AND ADMINISTRATION

9 May 2017

The Honorable John Boozman
Chairman, Subcommittee on Homeland Security Appropriations
131 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Jon Tester
Ranking Member, Subcommittee on Homeland Security Appropriations
128 Dirksen Senate Office Building
Washington, DC 20510

Chairman Boozman and Ranking Member Tester:

I write to request that you include $160,000,000 in the FY 2018 Homeland Security Appropriations Bill, for state and local governments to provide for the cybersecurity of infrastructure for federal elections through the purchase of auditable election systems and for the conduct of audits.

As you may know, in the emerging age of cyberwar, election equipment is a very attractive targets. Rational analysis concludes that our voting equipment will certainly be subject to sophisticated cyberattacks that are likely to change election outcomes without detection.

Most computer security experts agree that the threat cannot be resolved by conventional computer security methods. Organizations with great in-house expertise and large security budgets are routinely penetrated. There are regular reports of breaches or attempted breaches at the Department of Justice, Department of Homeland Security, the Office of Personnel Management, the Federal Bureau of Investigation, Google, Yahoo, Target, health insurance companies, banks, and all sorts of state and local governments. Local election offices, many of which have only part-time staff, have vastly less computer security expertise and funding with which to try to defend their systems. Computer scientists agree that even if we could somehow successfully detect tampering, under current conditions we will never know whether there have been successful undetected attacks. After every controversial election, charges of undetected tampering will grow until there is no longer faith in our elections.

Internet voting, allowed in some manner in more than 30 states, is even more vulnerable than electronic polling place voting. Every Internet voting system subjected to independent expert security review has been found to have fatal security weaknesses or privacy vulnerabilities or both. In a 2010 open public test of an online voting system in Washington, D.C., Russian hackers fully compromised the system within 36 hours and votes were changed without detection by the D.C. Board of Elections and Ethics. Attempted intrusions from China and Iran were also found.

A simple and effective solution to the cybersecurity vulnerability of our voting systems is available immediately: audit the results of elections instead of trying to secure computer systems. Risk limiting audits can provide a check on computer tallies to solve for malicious tampering (as well as inaccuracy from other sources like software bugs and clerical errors) and provide authoritative confirmation about the outcome. However, audits can't take place if state and local governments do not have auditable systems or funding to perform audits.

You can begin to help us to take hold of our elections and secure the integrity of one of our most important civic actions. We must ensure that votes cast are counted accurately and that we have the backup of an audit in the case of potential election meddling. To fail to cybersecure this foundation stone of our representative democracy will undermine our own people's faith in the integrity of our political system as well as to diminish the example we set for the nations of the world.

Thank you for your consideration of this critical request.

Sincerely,

Angus King

Angus S. King, Jr.