MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Fourteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

August 8, 2016

The Honorable Jeh C. Johnson
Secretary
Department of Homeland Security
Washington, DC 20528

Dear Secretary Johnson:

In recent weeks, a spate of hacking incidents against national political institutions have brought into sharp focus that cyber hackers, possibly at the direction of a foreign government, are engaged in a campaign to exploit cyber vulnerabilities to impact the forthcoming national election. Your recent acknowledgement that high-level discussions are underway about our nation's election cybersecurity[1] and designating our nation's electronic ballot-casting system as "critical infrastructure" for the November Presidential election is under consideration[2] reflects an appreciation of the risk that cyber weaknesses in certain voting equipment could be exploited by nefarious actors to alter the results of the election.

While attribution for these attacks is still the subject of ongoing Federal investigation, ignoring the risks to our electoral process presented by this campaign of cyber attacks is not an option. With precincts in at least 28 States, including jurisdictions in Ohio and Florida, expected to utilize digital touch screen voting machines,[3] there is an urgent need for the Department of Homeland Security (DHS) to provide a coherent, quick, and thorough response to needs of State and local officials who want to address the cyber vulnerabilities in their election equipment but may lack the resources and expertise.

---

[1] U.S. Seeks to Protect Voting System from Cyberattacks. Julie Hirschfeld Davis. New York Times. 3 August 2016.

[2] Id.

[3] "How to Hack an Election in 7 Minutes," Ben Wofford. Politico Magazine. 5 August 2016.

The Department must act swiftly to prevent even the suggestion that our electoral processes are vulnerable or under attack and ensure the public confidence of one of our most sacred treasures—the right to vote—is not affected by the prospect of malicious cyber and information technology intrusions. Local, county, and state officials must be able to call on the Federal government to defend the integrity, reliability, and validity of our free and democratic elections. DHS, as the Federal government lead for working with State, local, tribal, and territorial governments to secure critical infrastructure and information systems, is the natural partner for efforts to address cyber vulnerabilities in the nation's electoral system.

I believe that DHS could assist jurisdictions in need by (1) increasing its outreach and awareness effort to State and local officials to educate them about the cybersecurity resources available through the United States Computer Emergency Readiness Teams (US-CERT); and (2) prioritizing the provision of assistance to any jurisdiction that requests assistance to help to secure an at-risk voting systems; and redoubling its efforts to produce actionable information for distribution to State, local, tribal and territorial governments through the National Cybersecurity and Communications Integration Center (NCCIC). The Department is uniquely-situated and has the capabilities to help make a fundamental difference and protect a bedrock of our democratic process in a meaningful way.

It is in our Nation's best interest for DHS to move quickly for the benefit of all of state and local election officials whose systems are vulnerable and to protect the integrity of one of our most precious democratic institutions—our democratic, free, and unfettered voting process.

Again, I appreciate your attention to this critical homeland security issue, and I encourage you to strengthen your efforts to address this matter. If you have any questions, please contact Hope Goins, Chief Counsel for Oversight at hope.goins@mail.house.gov or 202-226-2616.

Sincerely,

Bennie G. Thompson
Ranking Member