COMMON CAUSE
Holding Power Accountable

To: The National Institute of Standards and Technology (NIST)

From: Common Cause

Responsive comments for developing a Framework for Improving Critical Infrastructure Cybersecurity

April 8, 2013

COMMON CAUSE
Holding Power Accountable

Common Cause is a not for profit, citizens advocacy organization committed to improving civic engagement and strengthening democracy. We are grateful for the opportunity to provide comments for the development of a Framework for Improving Critical Infrastructure Cybersecurity.

Common Cause has a long history of pressing for reforms to make the voting process accessible to all voters. In addition, our advocacy is dedicated to ensuring that every citizen has an opportunity to vote, that every vote is counted as cast and cast as intended. To that end, we advocate for election technology that can be audited and recounted. We strongly support the use of a voter-verified paper audit trail and post-election audits to ensure that the election outcomes are correct.

The administration of U.S. elections is the responsibility of state governments, but the federal government also has a role in ensuring our elections are fair, accessible and trustworthy. Healthy democracies are constituted of more than just elections outcomes; the legitimacy and credibility of the election itself is necessary for the peaceful transfer of power that we repeatedly enjoy.   The stability, continuity and security of our government are a function of the integrity of our election system.

As termed in 42 U.S.C. 5195c(e), for the purposes of developing the Framework for Improving Critical Infrastructure Cybersecurity, “critical Infrastructure” is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”   We believe our election systems cannot be excluded from the protections afforded our critical infrastructure.

Despite NIST's active involvement in setting standards for voting technologies, election systems and voting machines have been conspicuously absent from recent cyber security recommendations and policy proposals. With the passage of the Help America Vote Act of 2002 (HAVA), nearly every ballot in the U.S. is now counted by computer. Voter registration systems have been put online as have absentee balloting tools. But most concerning, in the last decade thirty states have passed laws to allow voted ballots to be sent electronically, by facsimile, email or direct Internet portal.   State election officials and legislators have adopted these laws and policies with no guidance or counsel from the national cyber security agencies and experts.

NIST has conducted research into voting systems for the U.S. Election Assistance Commission and concluded that secure Internet voting is not feasible at this time.[1] However, NIST's conclusion has not been incorporated into a national cyber security policy or guidelines. While NIST has identified the very serious threat of cyber attacks against online voting systems, these risks have not yet been recognized as threats against our national critical infrastructure.

We believe this constitutes a "high priority gap" in the cyber security framework where guidelines are non-existent. We urge NIST to draw on its existing research to develop guidelines and best practices for state officials and afford our voting systems the expertise and guidance essential to safeguarding our national critical infrastructure.

We thank you for the opportunity to provide these comments. We hope to cooperate with NIST and other stakeholders in developing guidance for voting systems.

Bob Edgar

Bob Edgar

President

[1] http://www.nist.gov/itl/vote/uocava.cfm