Testimony of the New York Democratic Lawyers Council (NYDLC)

Hearing on Ensuring the Integrity of Elections.

Submitted to the New York State Assembly Standing Committee on Election Law, Subcommittee on Election Day Operations and Voter Disenfranchisement

Nov 29th, 2016

Co-Chairs: Doug Dunham John Nonna, Carol Schrager, Ekow Yankah
Hal Hodes, NYDLC Legislative Affairs Co-Chair, NYDLCLegislativeAffairs@gmail.com

Thank you to the New York State Assembly Standing Committee on Election Law, Subcommittee on Election Day Operations and Voter Disenfranchisement for holding this important hearing to examine the condition of New York's election infrastructure with a focus on measures in place—and those additional measures needed—in order to protect the integrity of the election administration system against cyber-infiltration, tampering, or other attack.

For over 10 years, NYDLC has protected the rights of voters by deploying trained attorneys and advocates as election monitors in poll sites on Election Day. NYDLC uses this "front line" experience to advocate for pro-voter legislative and operational reforms that would modernize our election registration and administration systems, and alleviate common problems that arise each cycle, and in this case, identify and address threats to the integrity of our democratic process, and thus, the sanctity of the core civil rights of New York voters.

In an effort to respond to the evolving threats that are the subject of today's hearing, to continue to effectively safeguard the effectiveness of the fundamental right to vote, and to improve the public trust in our democracy, NYDLC is proud to announce the formation of a Joint-Subcommittee on the Integrity of Elections, as a forum to conduct appropriate research, develop expertise, and propose constructive solutions to these issues.

Election Systems Should Be Considered Critical Infrastructure

Putting aside the deleterious effects on the public trust that arise from baseless, high-profile claims about the integrity of U.S. registration and election processes, all Americans should be concerned about the very real threat to our democratic infrastructure posed by cyber-infiltration, physical or digital tampering, or other attack.

As an illustration of the imminence of this threat, and how seriously state actors and stakeholders view the potential for election-related hacking/tampering, the U.S. Intelligence Community is confident that over the course of the 2016 Presidential campaign cycle, the Russian Government directed several compromises of e-mails from U.S. persons and institutions, including from U.S. political organizations. The U.S. Department of Homeland Security (DHS) has convened an Election Infrastructure Cybersecurity Working Group with experts across government to raise awareness of cybersecurity risks to election infrastructure and the elections process.[1] In 2016, DHS offered "cyber hygiene scans", among other assistance, to help states identify vulnerabilities in voter registration and election night reporting systems. As a preventative measure to identify vulnerabilities, Ohio even asked the National Guard to attempt to penetrate its databases.[2]

Due to the critical infrastructure and fundamental rights at stake, this threat represents a legitimate, if *sui generis*, threat to national security, that can be greatly reduced via adequate

[1] Department of Homeland Security, *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*, Oct. 7, 2016, https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-

[2] Marshall Cohen and Tom LoBianco, *Hacking the Election? Feds Step In As States Fret Cyber Threats*, CNN Politics, Sept. 23, 2016, www.cnn.com/2016/09/23/politics/ohio-pennsylvania-election-2016-hack/

funding, registration and administration modernization, and the adoption of an evolving set of uniform best practices.

NYDLC believes that New York should address this threat head on, building upon existing measures like the 3% voter verifiable audit process, to reduce the adversarial and political elements from what should really be seen as a ministerial, "internal-affairs" or "ombudsmen" style state function. In short, guaranteeing the accuracy of our voting systems should be considered an aspect of critical state infrastructure, and should not be policed by the whims, dynamics, and financial capacity of losing or winning candidates in any given election or their parties.

State and County BOEs Must Be Cyber Secure in Order to Protect the Franchise

New York must ensure that our voter registration databases are secure and that there are database backups in place (the accuracy of which has been verified) and poll site and registration lookup redundancies ahead of an election event, to prevent hacking or tampering.

As the State commences the budgeting process, State BOE will require adequate funding to provide for appropriate levels of technology-focused staff, in order to implement a regional liaison model that would work with county BOEs to ensure that each county in New York is able to analyze local or systemic threats and quickly implement safeguards.

As mentioned, DHS offers a variety of services to local election officials to assist in their cybersecurity, including cyber hygiene scans on Internet-facing systems, risk and vulnerability assessments, access to expertise via the NCCIC (National Cybersecurity and Communications Integration Center), information sharing and best practices, and access to cybersecurity advisors.[3]

Additionally, the Governor's Cyber Security Advisory Board could be tapped to help coordinate the response or the reforms needed to continue to meet these evolving threats. That body was created and designed specifically to advise on developments in cyber security and make recommendations for protecting New York's critical infrastructure and information systems, which includes the operations that ensure the credible functioning of our democracy. In any event, an overarching framework should be used avoid blind spots and duplication, while independently assessing agency implementation.

The 3% audit statute (Election Law §9-211) is a useful step toward ensuring that paper ballots cast match the electronic results. However, the legislature should review the Election Law to determine which modernization proposals to registration, voter roll maintenance, and operational security would be useful to addressing these evolving threats far in advance of an election. Additional safeguards should be proactive in nature, in addition to the bright-line (though post-hoc) provisions of §9-211. The legislature, with advice from public and private sector security and election experts, should consider model legislation from other states, with the goal of ensuring that the accuracy and legitimacy of election results is verified in a non-adversarial way,

[3] Department of Homeland Security, *Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election Systems*, Sept. 16, 2016, https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation's-election-systems#

as part of routine administrative due diligence. Now, at the beginning of the next four-year cycle, is the ideal time to constructively address these real threats to the functioning of our democracy, as oppose to in the run-up to an election, or worse, after a catastrophic attack.

An Opportunity for NYS to Lead on Voting Rights

When it comes to modernizing our voter registration and election administration systems, New York has notably and notoriously lagged behind the curve. However, the issues raised during this hearing present an opportunity for New York to lead. Much has been written elsewhere[4] about the many residual "election integrity" benefits that would flow from adopting automatic registration, registration portability, and other modernization reforms, which would clean up the voter rolls, and create a smoother voting process for millions of eligible voters. These come with costs and require systemic changes to the way we have historically administered elections. Appropriate cyber security protections should be viewed as indispensible to putting these much-needed proposals into practice, and vice versa.

Conclusion

Thank you again for convening this important hearing. NYDLC stands ready to serve as a resource to help New York State address these threats with innovative pro-voter policies, as part of our mission to improve our democracy by ensuring that the ballots of every eligible voter be counted accurately, by systems that are transparent, efficient and fair.

[4] E.g. Myrna Perez, *Election Integrity: A Pro-Voter Agenda*, Brennan Center for Justice (2016), https://www.brennancenter.org/sites/default/files/publications/Election_Integrity.pdf.