Poorvi L. Vora
Professor, Department of Computer Science
The George Washington University

Micah Sherr
Provost's Distinguished Associate Professor, Department of Computer Science
Director, Georgetown Institute for Information Assurance
Georgetown University

House Bill 1331
Election Law – Cybersecurity
SUPPORT

Ways and Means
February 27, 2018

I am Poorvi L. Vora, a tenured Professor of Computer Science at The George Washington University. Micah Sherr, tenured Provost's Distinguished Associate Professor, Department of Computer Science, Georgetown University, is a co-signatory on my submitted written testimony, and has reviewed and approved the text of my oral testimony, which I present today on our behalf as he is out of town on an academic sabbatical. We have both published extensively on the subject of voting system security. We support this Bill.

In September last year, I testified at a joint hearing on cybersecurity of the House Ways and Means Committee and the Senate Education, Health and Environmental Affairs Committee. I spoke then of the need to protect online databases and election services, and I consider this Bill's notification requirements—of the election administrator and internet service providers—to be a step in the right direction.

I would like to add that, while these changes are necessary for election security, they are not sufficient. Particularly since the Mueller indictment of 16 February, the use of "information that is not generally available to the public but is readily available to the applicant" is not sufficient as a means of preventing voter impersonation. While such information is better than voter address, it is not a member of the general public that we are primarily worried will impersonate the voter. We are up against an entity with great technical skill, deep pockets, hundreds of employees and a commitment to interfering in US elections. The bad actors in cybersecurity can no longer be resisted by simply hardening the security of servers or using social security numbers for credentials.

The only approach available to us is to limit our use of entirely virtual transactions which are easy to fake. The addition of physical parts to the transactions—such as physical delivery of unfilled ballots—makes faking them considerably harder. Incorporating physical components into the voting process also makes it far more difficult for attackers to conduct large-scale attacks. It is far easier to give the appearance of thousands of computers requesting virtual ballots than it is to receive mail at thousands of physical addresses.

I also support this Bill's requirement of clear notifications to the voter of the integrity risks of online ballot delivery because the returned ballot will be duplicated manually once it is received by the local boards, and of the privacy risks of online ballot marking tools because computer viruses on the voter's machine can determine how the voter voted, regardless of whether the computer is connected to the internet at that time or not.