House Bill 1331
Election Law – Cybersecurity
SUPPORT

Ways and Means
February 27, 2018

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

This Bill makes valuable necessary improvements to Maryland's current approach to election cybersecurity. We support it.

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

We 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[1], 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[2]. 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,

[1] U.S. v. Internet Research Agency, et al (1:18-cr-32, District of Columbia), 16 February, 2018. https://www.justice.gov/file/1035477/download

[2] "In or around 2016, Defendants and their co-conspirators also used, possessed, and transferred, without lawful authority, the social security numbers and dates of birth of real U.S. persons without those persons' knowledge or consent. Using these means of identification, Defendants and their co-conspirators opened accounts at PayPal, a digital payment service provider; created false means of identification, including fake driver's licenses; and posted on ORGANIZATION-controlled social media accounts using the identities of these U.S. victims. Defendants and their co-conspirators also obtained, and attempted to obtain, false identification documents to use as proof of identity in connection with maintaining accounts and purchasing advertisements on social media sites", page 16, para 41, *ibid*.

hundreds of employees and a commitment to interfering in US elections[3]. 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.

We 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, whether the computer is connected to the internet at that time or not.

We urge you to pass this Bill.

Respectfully,

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

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

Note: affiliations are included for identification only

[3]"Defendants and their co-conspirators also registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names so as to appear to be U.S. persons and groups", pg 16, para 40, *ibid*. "The ORGANIZATION [Internet Research Agency] employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The ORGANIZATION's annual budget totaled the equivalent of millions of U.S. dollars", page 5, para 10(a), *ibid*.

Poorvi L. Vora is Professor of Computer Science at The George Washington University. Her research focus has been on end-to-end independently verifiable (E2E) voting systems which enable voters and observers to audit election outcomes without requiring them to rely on the trustworthiness of election technology or unobserved election processes. Prof. Vora was a member of the team that deployed polling-place, paper-ballot-based, E2E voting system Scantegrity II in the Takoma Park elections of 2009 and 2011, and of the team that developed remote voting E2E system Remotegrity and accessible voting variant Audiotegrity, used in 2011. She has worked with the National Institute of Standards and Technology (NIST) on definitions of desired properties of E2E systems, and on information-theoretic models and measures of voting system security properties. She obtained her Ph.D. from North Carolina State University.
poorvi@gwu.edu

Micah Sherr is Provost's Distinguished Associate Professor in the Computer Science Department at Georgetown University and director of the Georgetown Institute for Information Assurance. His academic interests include privacy-preserving technologies, electronic voting, wiretap systems, and network security. He participated in two large-scale studies of electronic voting machine systems, and helped to disclose numerous architectural vulnerabilities in U.S. election systems. His current research examines the security properties of legally authorized wiretap (interception) systems and investigates methods for achieving scalable, high-performance anonymous routing. Micah received his B.S.E., M.S.E., and Ph.D. degrees from the University of Pennsylvania. He is a recipient of the NSF CAREER award.
msherr@cs.georgetown.edu