March 19, 2020

Hon. Wanda Vázquez Garced *(via email)*
Governor of the Commonwealth of Puerto Rico
La Fortaleza
San Juan, Puerto Rico

RE: Veto of Senate Bill 1314, "Puerto Rico Electoral Code of 2020" - Internet Voting

Dear Governor Vázquez Garced,

We, Verified Voting, the undersigned computer scientists and cybersecurity experts, write to urge you to veto Senate Bill 1314 which proposes implementing a system of internet voting in Puerto Rico. Under the provisions of this bill, Puerto Rico would phase in internet voting as the sole option for Puerto Rican citizens. As explained more fully below, internet voting cannot be accomplished securely and provides no meaningful way to verify that the computers captured or counted votes accurately. This concept is settled science, notwithstanding efforts to increase internet voting use in some areas. In the current climate when nation states have sought to interfere in other nations' elections, Puerto Rico's bill is a risky move. Indeed, last year the Report of the Select Committee on Intelligence of the United States Senate made bipartisan recommendations, among them that "states should resist pushes" to move their elections online because in their words, "no system of online voting has yet established itself as secure."[1]

Cybersecurity experts agree that under current technology, no practically proven method exists to securely, verifiably, or privately return voted materials over the internet. That means that votes could be manipulated or deleted on the voter's computer without the voter's knowledge, local elections officials cannot verify that the voter's ballot reflects the voter's intent, and the voter's selections could be traceable back to the individual voter. Such a system could violate protections guaranteeing a secret ballot, as outlined in Section 2, Article II of the Puerto Rico Constitution.

The pending legislation references a "secure" method of voting. No such system is commercially available despite the use of insecure internet voting methods in some other states and countries. For Puerto Rico to attempt to develop such a system on its own would be prohibitively expensive. The Department of Defense and National Institute for Standards and Technology (NIST) spent millions of dollars attempting to do just that and abandoned the program when it became clear that no secure method of voting is available.[2] Specifically, NIST stated:

---

[1] *See* Report of The Select Committee On Intelligence United States Senate On Russian Active Measures Campaigns And Interference In The 2016 U.S. Election, Vol. 1: Russian Efforts Against Election infrastructure with Additional Views, at 59 (July, 2019) available here: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

[2] NIST Activities on UOCAVA Voting; http://www.nist.gov/itl/vote/uocava.cfm

> The study concluded that Internet voting systems cannot currently be audited with a comparable level of confidence in the audit results as those for polling place systems. Malware on voters' personal computers poses a serious threat that could compromise the secrecy or integrity of voters' ballots. And, the United States currently lacks a public infrastructure for secure electronic voter authentication. Therefore, NIST's research results indicate that additional research and development is needed to overcome these challenges before secure Internet voting will be feasible.

The National Academies of Science, Engineering, and Medicine in 2018 released the report entitled *Securing the Vote: Protecting American Democracy*[3] which gives the following recommendation:

> 5.11 At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.

In short, any plan to develop a system of internet voting goes against recommendations, would incur significant costs, and would be guaranteed to fail to secure votes.

Internet voting is the most vulnerable method of voting

Anyone in the world, including foreign nation states, criminal organizations, or our domestic partisans, can attack any Internet voting system, attempt to change votes, violate privacy, or disrupt the election – possibly in a completely undetectable way. The kinds of attacks that are credible threats and elevate the risk of voting via the internet include the following:

- Voter authentication attacks (i.e. forged voter credentials)
- Malware on voters' devices (e.g., viruses, Trojan horses, malicious code embedded in software updates) that can modify votes undetectably
- Denial of service attacks (slowing some key part of the system to a crawl, or crashing it, either by overwhelming it with traffic or taking advantage of a bug)
- Server penetration attacks (remote break-in and control of the election server)
- Spoofing attacks (directing voters to a fake voting site instead of the real one)
- Widespread privacy violation (by any of several methods, taking advantage of the fact that online voters must transmit their names with their votes)
- Automated vote buying and selling schemes (with cryptocurrency payments, e.g. Bitcoin, in exchange for votes)

[3] National Academies Press https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

More importantly, the security of the device that voters use to cast their votes is unknowable. The device may already be corrupted with malware or viruses that could interfere with ballot transmission or even spread that malware to the computer at the elections office on the receiving end.

Attacks cannot be prevented, recovered from, or even reliably detected

Cyber security experts agree that completely preventing attacks is impossible despite the use of best practices in cybersecurity. Resiliency, namely the capability to recover from an attack or error, is a critical component of cybersecurity protection. With insecure internet voting, no trustworthy record of the voter's choices exists, and therefore it is impossible to perform meaningful audits or recover from an attack or a hack.

Safer alternatives should be explored

While we are sensitive to the issues described in the legislation, we strongly urge you to explore more secure policy choices to address these issues, i.e. extending the deadline for receipt of voted ballots sent through the mail.

Puerto Rico should not embark on a costly exercise to introduce internet voting that will increase the risk to unacceptable levels for the citizens of Puerto Rico. We endorse the ACLU of Puerto Rico's January 29, 2020 letter to you and emphasize the burden internet voting will place on the fundamental right to vote. Should Puerto Rico enact this bill, certainly litigation challenging its legality and burden on the right to vote will follow.

We respectfully urge you to veto Senate Bill 1314 to protect the fundamental right to vote of Puerto Ricans.

Respectfully submitted,

Marian K. Schneider, President
Verified Voting

cc: Steven Liong Rodriguez (*via email*)
Alex Lopez (*via email)*
Lcdo. Pabon (*via email)*

Verified Voting is a national, non-profit non-partisan information and advocacy organization focused exclusively on ensuring the security, integrity, and trustworthiness of computerized election technology. Our mission is to strengthen democracy for all voters by promoting the responsible use of technology in elections. We seek to ensure that Americans can be confident their votes are cast as intended and counted as cast.

The following signatories add their names urging the Governor to veto the bill.
Institutional affiliations are provided only for the purpose of identification and do not imply institutional endorsement or approval of this letter.

David L. Dill
Founder and Member, Board of Directors, Verified Voting
Donald E Knuth Professor, Emeritus,
School of Engineering, Stanford University

David Jefferson. Ph.D.
Member, Board of Directors, Verified Voting
Computer Scientist, Lawrence Livermore National Laboratory

Ronald Rivest
Institute Professor
Professor of Electrical Engineering and Computer Science
Co-inventor, RSA public key encryption algorithm
Massachusetts Institute of Technology, MIT

Kevin Shelley
Member, Board of Directors, Verified Voting
Former California Secretary of State

Barbara Simons
Chair, Verified Voting Foundation
IBM Research (retired)
Former President, Association for Computing Machinery (ACM)
Member, Board of Advisors to the U.S. Election Assistance Commission (EAC)

Ron Bandes
Network Security Analyst
President, VoteAllegheny
Director, League of Women Voters of Greater Pittsburgh

Alex Blakemore
Computer Scientist
Virginia Verified Voting

Matt Blaze
McDevitt Professor of Computer Science and Law
Georgetown University

Jeff Bleich
United States Ambassador to Australia (ret.)

Duncan Buell
NCR Professor of Computer Science and Engineering
Dept. of Computer Science and E
University of South Carolina

Larry Diamond
Senior Fellow, Hoover Institution
Senior Fellow, Center on Democracy, Development & the Rule of Law, Freeman Spogli Institute for International Studies
Bass University Fellow in Undergraduate Education, Stanford University

Michael J. Fischer
Member, Verified Voting Board of Advisors
Professor of Computer Science
Yale University

John Gage
Member, Verified Voting Board of Advisors
Former Vice President and Chief Researcher
Sun Microsystems

Martin Hellman
Member, US National Academies of Sciences, Engineering, and Medicine
Professor Emeritus of Electrical Engineering
Stanford University

Candice Hoke
Founding Co-Director, Center for Cybersecurity and Privacy Protection

Douglas W. Jones
Associate Professor of Computer Science
Past Chair, Iowa Board of Examiners for Voting Machines and Electronic Voting Systems
Coauthor of Internet Voting in the United States
University of Iowa

Lou Katz
Privacy Advisory Commission
Oakland CA

Joseph Kiniry
Principled CEO and Chief Scientist, Free & Fair
Principal Scientist, Galois

Carl E. Landwehr
Visiting Professor
Electrical and Computer Engineering
University of Michigan

Collin F. Lynch
Assistant Professor of Computer Science
North Carolina State University

Neal McBurnett
Member, Verified Voting Board of Advisors

John L. McCarthy
Member, Verified Voting Board of Advisors
Computer Scientist (retired), Lawrence Berkeley National Laboratory

David Mussington, Ph.D., CISSP
Director of the Center for Public Policy and Private Enterprise
University of Maryland

Peter G. Neumann
Chief Scientist, SRI International Computer Science Lab

Morris Pearl
Member, Verified Voting Board of Advisors

Alexa Raad
Member, Verified Voting Board of Advisors
Alexa Raad, LLC.

Mark Ritchie
Member, Verified Voting Board of Advisors
Former Secretary of State, Minnesota

John E. Savage
An Wang Professor of Computer Science
Brown University

Bruce Schneier
Fellow, Berkman Center for Internet and Society
Fellow, Belfer Center, Kennedy School of Government
Harvard University

Kevin Skoglund
Chief Technologist, Citizens for Better Elections

Phillip Stark
Professor of Statistics and Associate Dean of Mathematical and Physical Sciences
University of California, Berkeley

Susan Dzieduszycka-Suinat
President and CEO
U.S. Vote Foundation

Eugene H. Spafford
Professor of Computer Science
Director Emeritus
Purdue University CERIAS

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

Dan Wallach
Professor of Computer Science
Rice University

Daniel M. Zimmerman
Principled Computer Scientist, Free & Fair
Principal Researcher, Galois