19 de marzo 2020

Hon. Wanda Vázquez Garced (via correo electrónico)
Gobernadora de Puerto Rico
La Fortaleza
San Juan, Puerto Rico

RE: Veto Proyecto del Senado 1314, "El Codigo Electoral de Puerto Rico 2020" Voto por Internet

Estimada Hon. Gobernadora Vázquez Garced,

Nosotros, Verified Voting, los abajofirmantes científicos en computación, y los expertos en seguridad cibernética, le escribimos para pedirle su VETO al PS 1314 que propone implementar un sistema de voto por Internet en Puerto Rico. Bajo las secciones de esta ley, Puerto Rico incluiría, por medio de fases, el voto por Internet para que éste sea el único disponible para los ciudadanos en Puerto Rico. Como explicamos en detalle en esta carta, el voto por Internet no se puede llevar a cabo con seguridad y de manera que se pueda verificar bien que las computadoras capturaron o contaron los votos correctamente. Este concepto es ciencia cierta, no empece los esfuerzos de algunas jurisdicciones de incluir el voto por Internet. En el contexto histórico que vivimos, en que países han querido interferir en las elecciones de otras naciones, este proyecto de ley de Puerto Rico es una movida riesgosa y peligrosa. El año pasado, el Informe de la Comisión Senatorial sobre Inteligencia de Estados Unidos rindió recomendaciones bipartidistas, entre las cuales incluyó que "los estados deben resistir el deseo" a mover sus elecciones a el Internet porque, en sus propias palabras, "no existe sistema de voto en línea que se haya presentado a sí mismo como seguro".

Expertos en seguridad cibernética coinciden en que, con la tecnología actual, no existen métodos que ofrezcan seguridad, privacidad o verificabilidad para efectuar cualquier material electoral por Internet. Esto significa que los votos se pueden manipular o borrar en la misma computadora del elector sin que el elector lo sepa. Y, los oficiales electorales no tendrán manera de verificar que, en efecto, el voto de la persona hecho por medio de el Internet, era la intención electoral de dicha persona. No es verificable. Este tipo de Sistema violaría las garantías al voto secreto expuesto en la Seccion 2 del Articulo II de la constitución.

El Proyecto del Senado 1314 hace referencia a un método "seguro" de voto por Internet. Sin embargo, no existe este sistema en el comercio actual a pesar del uso de métodos inseguros de voto por Internet que se usan en otros estados y países. Para que Puerto Rico intente desarrollar un Sistema seguro por su propia iniciativa seria exponencialmente caro y prohibitivo. El Departamento de Defensa y el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) ha gastado millones de dólares en su intento de crear un sistema de voto por Internet seguro, y han tenido que abandonar el programa al ser meridianamente claro que no existe método seguro para voto por Internet. Específicamente, el NIST dijo:

> El estudio concluyó que los sistemas de voto por Internet disponibles no pueden auditarse al nivel de confianza de los resultados de auditorías llevados a cabo para los sistemas de comicio electoral. Malware en la computadora personal de los electores presenta una amenaza sería que podria comprometer la integridad y confidencialidad de las papeletas de los electores. Y, los Estados Unidos ahora mismo arece de la infraestructura publica para proveer autenticación segura de electores por internet. Así que, los resultados de la investigación de NIST indican que se requiere investigación y desarrollo adicional para sobrepasar estos retos antes de que el voto por internet sea una opción viable.

Las Academias Nacionales de Ciencia, Ingeniería y Medicina publicaron un informe en 2018 llamado "Securing the Vote: Protecting American Democracy" en el que ofrecen las siguientes recomendaciones:

> 5.11 En el presente, el Internet (o cualquier sistema conectado a el Internet) no se debe utilizar para enviar o efectuar papeletas marcadas. Además, el voto por Internet no se debe usar en el futuro, al menos que existan garantías sumamente robustas de seguridad y verificabilidad desarrolladas y funcionales, contrario a la tecnología que existe al presente sin garantías de confidencialidad, seguridad y verificabilidad de una papeleta marcada enviada por Internet.

En resumidas cuentas, cualquier plan para desarrollar un sistema de voto por Internet sería contrario a las recomendaciones nacionales, incurriría en gastos significativos y garantizaría el fracaso de la seguridad electoral.

El Voto por Internet es la más vulnerable de ejercer el voto

Cualquiera en el mundo, incluyendo naciones foráneas, organizaciones criminales o nuestros partidarios domésticos pueden atacar el Sistema de voto por internet, buscar cambiar los votos, violar la privacidad o impedir las elecciones—posiblemente de manera totalmente indetectable. Los tipos de ataques que crean una amenaza creíble y eleven el riesgo del voto por internet son:

- Ataques a la autenticación del elector (ie. Credenciales electorales falsificados)
- Malware en la tecnología de los electores (ie. Virus, caballos de Troya, códigos maliciosos en actualizaciones de software) que pueden modificar los votos sin detección
- Ataques de negación de servicio (dilatar alguna parte del sistema a lentitud absoluta o a que se caiga, o por medio de mucho tráfico o algún virus)
- Ataques que penetren servidores (que entren y controlen el servidor electoral remotamente)
- Ataques de "spoofing" (dirigiendo a electores a una página de Internet falsa en vez de la real)

- Violación a la privacidad colectiva (por medio de diversos métodos, aprovechándose de que los electores tienen que proveer su nombre para efectuar su voto en línea)
- Esquemas de compra y venta de votos automatizada (con pagos en "cryptocurrency", ie, bitcoin, en intercambio de votos)

Más importante aún, la seguridad de los aparatos que los electores utilicen para efectuar su voto se desconoce. El aparato ya puede tener un virus o malware que interfiera con la transmisión de la papeleta o hasta riegue el virus a la computadora de le la oficina electoral que recibe el voto.

Los ataques no se pueden prevenir, detectar, ni de los que se puede recuperar

Expertos de seguridad cibernética coinciden en que prevenir los ataques es imposible, aun utilizando las mejores prácticas de seguridad cibernética. La resiliencia, la capacidad de recuperarse de un ataque o error, es un elemento crítico de la protección de seguridad cibernética. Con el inseguro voto por internet, no existe un record confiable de las opciones electorales, así que es imposible llevar a cabo una auditoria confiable o recuperar de un ataque o "hackeo".

Alternativas más seguras de deben explorar

Aunque somos sensibles a los temas descritos en esta legislación, le solicitamos enfáticamente que explore opciones más seguras para atender estos temas; por ejemplo, extender la fecha límite para recibir papeletas enviadas por correo.

Puerto Rico no debe embarcarse en este ejercicio costoso de introducir el voto por Internet al sistema electoral. Este sistema elevará los riesgos a niveles inaceptables para los ciudadanos en Puerto Rico. Endosamos la carta enviada por ACLU Puerto Rico el 29 de enero 2020 a usted, Honorable Gobernadora Wanda Vázquez Garced, y enfatizamos la carga e intromisión que el voto por Internet le colocará al derecho fundamental al voto. Si Puerto Rico convierte esto en ley, debe esperar litigación al respecto retando la legalidad y la carga al derecho al voto impuesto por dicha legislación.

Respetuosamente, le solicitamos que vete el Proyecto del Senado 1314 para, así, proteger el derecho fundamental al voto de los puertorriqueños.

Respetuosamente sometido,

Marian K. Schneider, Presidente
Verified Voting

cc: Steven Liong Rodriguez (*via* correo electrónico sliong@fortaleza.pr.gov)
Alex Lopez (*via* correo electrónico *ajlopez@fortaleza.pr.gov*)
Lcdo. Pabon (*via* correo electrónico *apabon@fortaleza.pr.gov*)

Verified Voting es una organización nacional de información y defensa sin fines de lucro, no partidista, enfocada exclusivamente en garantizar la seguridad, integridad y confiabilidad de la tecnología electoral computarizada. Nuestra misión es fortalecer la democracia para todos los votantes mediante la promoción del uso responsable de la tecnología en las elecciones. Buscamos garantizar que los estadounidenses puedan estar seguros de que sus votos se emiten según lo previsto y se cuentan como emitidos.

Los siguientes signatarios agregan sus nombres instando al Gobernador a vetar el proyecto de ley. Las afiliaciones institucionales se proporcionan solo con el propósito de identificación y no implican respaldo o aprobación institucional de esta carta.

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