Scientists say no credible evidence of computer fraud in the 2020 election outcome, but policymakers must work with experts to improve confidence

16 November 2020

We are specialists in election security, having studied the security of voting machines, voting systems, and technology used for government elections for decades.

We and other scientists have warned for many years that there are security weaknesses in voting systems and have advocated that election systems be better secured against malicious attack. As the National Academies recently concluded, “There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats.” However, notwithstanding these serious concerns, we have never claimed that technical vulnerabilities have actually been exploited to alter the outcome of any US election.

Anyone asserting that a US election was “rigged” is making an *extraordinary* claim, one that must be supported by persuasive and verifiable evidence. Merely citing the existence of technical flaws does not establish that an attack occurred, much less that it altered an election outcome. It is simply speculation.

The presence of security weaknesses in election infrastructure does not by itself tell us that any election has actually been compromised. Technical, physical, and procedural safeguards complicate the task of maliciously exploiting election systems, as does monitoring of likely adversaries by law enforcement and the intelligence community. Altering an election outcome involves more than simply the existence of a technical vulnerability.

We are aware of alarming assertions being made that the 2020 election was “rigged” by exploiting technical vulnerabilities. However, in every case of which we are aware, these claims either have been unsubstantiated or are technically incoherent. To our collective knowledge, no credible evidence has been put forth that supports a conclusion that the 2020 election outcome in any state has been altered through technical compromise.

That said, it is imperative that the US continue working to bolster the security of elections against sophisticated adversaries. At a minimum, all states should employ election security practices and mechanisms recommended by experts to increase assurance in election outcomes, such as post-election risk-limiting audits.

If you are looking for a good place to start learning the facts about election security, we recommend the recent National Academies of Science, Engineering, and Medicine (NASEM) study, “Securing the Vote”, which is available for free download at https://doi.org/10.17226/25120.

Signed,

(Affiliations are for identification purposes only; listed alphabetically by surname.)

1. Tony Adams, Independent Security Researcher
2. Andrew W. Appel, Professor of Computer Science, Princeton University
3. Arlene Ash, Professor, University of Massachusetts Medical School
4. Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science; affiliate faculty, Columbia Law, Columbia University
5. Matt Blaze, McDevitt Chair of Computer Science and Law, Georgetown University
6. Duncan Buell, NCR Professor of Computer Science and Engineering, University of South Carolina
7. Michael D. Byrne, Professor of Psychological Sciences and Computer Science, Rice University
8. Jack Cable, Independent Security Researcher
9. Jeremy Clark, NSERC/Raymond Chabot Grant Thornton/Catallaxy Industrial Research Chair in Blockchain Technologies, Concordia Institute for Information Systems Engineering
10. Sandy Clark, Independent Security Researcher
11. Stephen Checkoway, Assistant Professor of Computer Science, Oberlin College
12. Richard DeMillo, Chair, School of Cybersecurity and Privacy and Warren Professor of Computing, Georgia Tech
13. David L. Dill, Donald E. Knuth Professor, Emeritus, in the School of Engineering, Stanford University
14. Zakir Durumeric, Assistant Professor of Computer Science, Stanford University
15. Aleksander Essex, Associate Professor of Software Engineering, Western University, Canada
16. David Evans, Professor of Computer Science, University of Virginia
17. Ariel J. Feldman, Software Engineer
18. Edward W. Felten, Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University
19. Bryan Ford, Professor of Computer and Communication Sciences, Swiss Federal Institute of Technology Lausanne (EPFL)
20. Joshua M. Franklin, Independent Security Researcher
21. Juan E. Gilbert, Banks Family Preeminence Endowed Professor & Chair, University of Florida
22. J. Alex Halderman, Professor of Computer Science and Engineering, University of Michigan
23. Joseph Lorenzo Hall, SVP Strong Internet, Internet Society
24. Harri Hursti, co-founder Nordic Innovation Labs and Election Integrity Foundation
25. Neil Jenkins, Chief Analytic Officer, Cyber Threat Alliance
26. David Jefferson, Lawrence Livermore National Laboratory (retired)
27. Douglas W. Jones, Associate Professor of Computer Science, University of Iowa

28. Joseph Kiniry, Principal Scientist, Galois, CEO and Chief Scientist, Free & Fair
29. Philip Kortum, Associate Professor of Psychological Sciences, Rice University
30. Carl E. Landwehr, Visiting Professor, University of Michigan
31. Maggie MacAlpine, co-founder Nordic Innovation Labs and Election Integrity Foundation
32. Bruce McConnell, former Deputy Under Secretary for Cybersecurity, Department of Homeland Security, (currently) President, EastWest Institute
33. Patrick McDaniel, Weiss Professor of Information and Communications Technology, Penn State University
34. Walter Mebane, Professor of Political Science and of Statistics, University of Michigan
35. Eric Mill, Chrome Security PM, Google
36. David Mussington, Professor of the Practice, School of Public Policy, University of Maryland College Park
37. Peter G. Neumann, Chief Scientist, SRI International Computer Science Lab
38. Lyell Read, Researcher at SSH Lab, Oregon State University
39. Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology
40. Aviel D. Rubin, Professor of Computer Science, Johns Hopkins University
41. Bruce Schneier, Fellow and Lecturer, Harvard Kennedy School
42. Alexander A. Schwarzmann, Dean of Computer and Cyber Sciences, Augusta University
43. Hovav Shacham, Professor of Computer Science, The University of Texas at Austin
44. Micah Sherr, Provost's Distinguished Associate Professor, Georgetown University
45. Barbara Simons, IBM Research (retired)
46. Kevin Skoglund, Chief Technologist, Citizens for Better Elections
47. Michael A. Specter, EECS PhD Candidate, MIT
48. Alex Stamos, Director, Stanford Internet Observatory
49. Philip B. Stark, Professor of Statistics and Associate Dean of Mathematical and Physical Sciences, University of California, Berkeley
50. Jacob Stauffer, Director of Operations, Coherent CYBER
51. Camille Stewart, Cyber Fellow, Harvard Belfer Center
52. Rachel Tobac, Hacker, CEO of SocialProof Security
53. Giovanni Vigna, Professor, Computer Science, University of California, Santa Barbara
54. Poorvi L. Vora, Professor of Computer Science, The George Washington University
55. Dan S. Wallach, Professor, Departments of Computer Science and Electrical & Computer Engineering, Rice Scholar, Baker Institute of Public Policy, Rice University
56. Tarah Wheeler, Cyber Fellow, Harvard Belfer Center
57. Eric Wustrow, Assistant Professor, Department of Electrical, Computer & Energy Engineering, University of Colorado Boulder
58. Ka-Ping Yee, Review Team Member, California Secretary of State's Top-to-Bottom Review of Voting Systems
59. Daniel M. Zimmerman, Principal Researcher, Galois and Principled Computer Scientist, Free & Fair