Letter to ABA Task Force on for American Democracy Co-Chairs

Judge Michael Luttig
Hon. Jeh Johnson
Vice-Chair William Ide III

We are specialists in cybersecurity, computer science, and election security who have spent many decades studying and engineering the security of computerized voting systems. We are writing to urge the ABA Task Force for American Democracy to appoint independent technical experts with recognized cybersecurity credentials to help the Task Force understand election integrity and security issues and assist in making recommendations to defend against the foreign and domestic threats facing the nation's computerized voting infrastructure.

Although we have often raised alarms about serious security vulnerabilities in voting systems, we are acutely aware of the dangers of false allegations of election security breaches. On November 16, 2020, many of us posted a jointly signed letter[1] on public websites stating there was no credible evidence of technical election fraud in the 2020 election anywhere in the U.S. Our letter was reported widely in national media[2], and we believe it did much to bolster confidence in the outcome of that election. We rebutted unsubstantiated and technologically fantastic claims by self-anointed "experts" and poorly informed election deniers that the results were rigged or manipulated. In many cases, these claims were promoted by lawyers and policymakers whose formal training and prior experience did not equip them with the requisite knowledge and skills to draw and communicate meaningful conclusions regarding the security of electronic voting systems. We advised policymakers to work with real experts to improve public confidence in the American election system.

We and other scientists have warned for many years that there are security weaknesses in existing voting systems. This is a view held by The National Academy of Sciences, Engineering, and Medicine—the most authoritative voice available to the federal government on science and technology—whose 2018 report, "Securing the Vote,"[3] concluded, *"There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats."* This is reflected in President Biden's 2021 Executive Order on Improving Cybersecurity[4] and the 2023 National Cybersecurity Strategy,[5] which focus on resilient systems that can withstand attacks, not on the impossible goal of perfectly secure systems. Even more pertinent to the ABA mission

---

[1]https://www.mattblaze.org/papers/election2020.pdf
[2]https://www.nytimes.com/2020/11/16/business/election-security-letter-trump.html?unlocked_article_code=1.ck0.6ENv.xZfPPOf2fNeO&smid=url-share
[3] https://doi.org/10.17226/25120
[4]https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
[5]https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

are the recent relevant federal court rulings documenting the factual basis for concern about unresolved, persistent cybersecurity risks affecting many existing voting systems.

We were buoyed by the announcement of the ABA Task Force for American Democracy and its promise to emphasize election integrity, public education, and tools to help election officials navigate the sometimes-confusing cyber threat landscape. We were also pleased by the “Listening Tour" information-gathering format, allowing policymakers, technical experts, and legal experts to work together. However, after the first session in Atlanta, we became concerned that in this listening tour the Task Force was not hearing from the scientific community. Particularly alarming were unchallenged statements from senior state election officials denying the possibility of intrusion and using demonstrably false claims of security to reject common sense measures to be employed should a catastrophic breach take place. When security experts hear that election officials believe their systems are immune from attack, images of icebergs looming over an “unsinkable” ship come immediately to mind. We applaud the support and praise for sincere, hard-working state and local election officials. However, election officials inadequately trained in cyber security are in no position to anticipate, recognize, and respond to the foreign and domestic threats facing us in 2024 and beyond. Worse, they may be bound by interpretations of the law that prevent them from adopting secure voting systems and strong security practices.

A Task Force goal is to “Assess the role cyberspace can play in either promoting or corrupting the American democratic process.”[6] Legitimate, well-respected scientific and technical experts are critical for navigating the complex threat landscape to support the ABA Task Force mission. There are authoritative resources grounded in textbook principles outlining accepted election security practices, including awareness training, threat assessment, ballot protection, incident response, data gathering, cyber clinics for election staff, post-election audits, and other measures to increase assurance in election outcomes and protect the individual right to vote and the rule of law. Administrative tasks have become complex and technical in the age of computerized elections. Credibility and competency in managing that complexity will go a long way toward building public confidence that our underlying systems can withstand cyber-attacks. We urge you to heed our advice to work with technical experts to “restore voter confidence in the integrity of elections.”[7] The ABA Task Force is uniquely positioned to provide objective, nonpartisan support for protecting the upcoming November election and help earn and restore voter confidence. Still, genuine collaboration among lawyers, election officials, and the technical community will be necessary for success. Appointing a sufficient number of technical advisors with the requisite cybersecurity and election security expertise will help the task force recognize

[6]https://www.americanbar.org/groups/leadership/office_of_the_president/american-democracy/our-work/#:~:text=Assess%20the%20role%20cyberspace%20can%20play%20in%20either%20promoting%20or%20corrupting%20the%20American%20democratic%20process.

[7]https://www.americanbar.org/groups/leadership/office_of_the_president/american-democracy/our-work/#:~:text=Endeavor%20to%20restore%20voter%20confidence%20in%20the%20integrity%20of%20our%20elections.

the real threats, weigh them properly, recommend effective protections, and avoid recommendations that might be harmful. We would be pleased to share recommendations for qualified candidates with you.

Signed (Affiliations are for identification purposes only; listed alphabetically)

1. Mustaque Ahamad, Professor and Regents Entrepreneur, School of Cybersecurity and Privacy, Georgia Tech
2. David A. Bader, Distinguished Professor, New Jersey Institute of Technology
3. Michael Bailey, Chair, School of Cybersecurity and Privacy, Georgia Tech
4. Josh Benaloh, Sr. Principle Cryptographer, Microsoft Research (and co-author referenced NASEM report)
5. Matt Blaze, McDevitt Chair of Computer Science and Law, Georgetown University
6. Duncan Buell, Chair Emeritus, NCR Chair in Computer Science and Engineering Dept. of Computer Science and Engineering, University of South Carolina
7. Richard DeMillo, Professor and Charlotte B. and Roger C. Warren Chair in Computing, School of Cybersecurity and Privacy, Georgia Tech
8. David Dill, Donald E. Knuth Professor, Emeritus, in the School of Engineering, Stanford University
9. Susan Greenhalgh, Senior Advisor on Election Security, Free Speech for People
10. Andrew Grossman, Association for Computing Machinery
11. J. Alex Halderman, Bredt Family Professor of Engineering, University of Michigan
12. Hari Hursti, co-founder Nordic Innovation Labs and Election Integrity Foundation
13. David Jefferson, Lawrence Livermore National Laboratory (retired)
14. Douglas Jones, University of Iowa Department of Computer Science, retired
15. Joseph Kiniry, Principal Scientist, Galois and CEO and Chief Scientist, Free & Fair
16. Wenke Lee, Professor, School of Cybersecurity and Privacy, Georgia Tech
17. Rhonda Martin, Coalition for Good Governance
18. Walter Mebane, Professor of Political Science and of Statistics, University of Michigan.
19. Gregory Miller, Open Software Election Technology Foundation
20. Peter Neumann, Chief Scientist, SRI International Computer Science Lab
21. Eddie Perez, Open Software Election Technology Foundation
22. Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology
23. Alex Schwarzmann, Dean, School of Computer and Cyber Sciences, Augusta University
24. Bruce Schneier, Berkman Klein Center for Internet & Society, Harvard University
25. John Sebes, Chief Technologist, Open Software Election Technology Foundation
26. Barbara Simons, IBM Research (Retired); Past President, Association for Computing Machinery

27. Eugene Spafford, Professor, Computer Science, Purdue University
28. Drew Springall, Assistant Professor, Computer Science, Auburn University
29. Michael Specter, Assistant Professor, School of Cybersecurity and Privacy, Georgia Tech
30. Philip Stark, Professor of Statistics and Associate Dean of Mathematical and Physical Sciences, University of California, Berkeley