Written Testimony of
Josh Benaloh

Senior Cryptographer
Microsoft Research
Microsoft Corporation

to the Subcommittee on Investigations & Oversight
and the Subcommittee on Research & Technology
of the House Committee on Science, Space, & Technology
to review Election Security: Voting Technology Vulnerabilities.

June 25, 2019

Chair Sherrill, Chair Stevens, Ranking Member Norman, Ranking Member Baird, and Members of the Committees, thank you for the opportunity to testify about the important issue of deploying technology to improve the security of U.S. elections.

My name is Josh Benaloh, I am the Senior Cryptographer at Microsoft Research[1]. Microsoft's research operations span 17 locations worldwide, employing well over 2,000 people conducting research and advanced development in computer science, electrical engineering, economics, physics, biology, and social science. These research operations are embedded in R&D operations across Microsoft that represent an annual investment of over $14 billion.

In addition to my position at Microsoft, I hold an Affiliate Faculty position in the Paul G. Allen School of Computer Science and Engineering at the University of Washington. I earned a degree in Mathematics from MIT and M.S., M.Phil., and PhD. Degrees in Computer Science from Yale University, where my 1987 doctoral dissertation was entitled "Verifiable Secret-Ballot Elections." I have spent the last 30 years working on the complex and intricate problems of election security and integrity.

[1]Microsoft Research, https://research.microsoft.com/

When individuals cast their ballots in a free and fair election, they experience democracy in its most personal form. They select leaders and provide direction for their communities, and in the United States they do so within the privileged protection of a secret ballot. When adversaries attempted to interfere in the 2016 U.S. elections their actions threatened more than just the integrity of the vote itself; they threatened to undermine our collective faith in the entire electoral process.

Building and maintaining voter confidence in elections is a multi-facetted task that cannot be accomplished by one organization or entity alone. Microsoft believes it will take extensive effort from the Federal government, state and local governments, election system vendors, the technology sector, academia, civil society, and voters themselves to come together and drive solutions.

For that reason, last year Microsoft formed the Defending Democracy Program, which works with a variety of governmental and non-governmental stakeholders in democratic countries globally to achieve the following goals: [2]

- **Protect campaigns from hacking** through increased cyber resilience measures, accessible and affordable security tools, and incident response capabilities;
- Explore technological solutions to **preserve and protect electoral processes** and engage with federal, state, and local officials to identify and remediate cyber threats; and
- **Defend against disinformation campaigns** in partnership with leading academic institutions and think tanks dedicated to countering state-sponsored computational propaganda and junk news.

National Academies Report

Recently, I had the privilege and pleasure of serving on the National Academies of Science, Engineering, and Medicine committee on the Future of Voting which spent nearly two years gathering and synthesizing information. The committee's

[2] "Defending Democracy Program", https://news.microsoft.com/on-the-issues/topic/defending-democracy-program/

report – "Securing the Vote: Protecting American Democracy" – was published in September of 2018[3].

The report included numerous findings and 41 specific recommendations, and it devoted an entire chapter to election integrity. With regard to cybersecurity, the report noted the asymmetric relationship between the thousands of electoral jurisdictions in the United States – most of which are very small – and the potential nation-state level attackers who may threaten these jurisdictions. The report concluded that the diversity of the U.S. election infrastructure weakens – rather than strengthens – the security of our elections, and that although we have a responsibility to apply best practices and try to harden our electoral infrastructure, it is simply not reasonable to think that we can make our infrastructure impervious to attack.

Instead, the report noted the importance of auditing technologies that can detect compromises of our election systems – even if attacks cannot always be prevented. The report specifically recommends pursuing both **risk-limiting audits** and **end-to-end verifiability** as auditing technologies that can improve election integrity by enabling detection of any alteration of votes or tallies.

Risk Limiting Audits

Risk Limiting Audits (RLAs) are like traditional audits in that auditors – ideally together with members of the public – randomly select ballots and check to see that they are consistent with published tallies and other public data. Unlike traditional audits, however, RLAs use sophisticated statistical methods to dynamically determine the point at which an audit can conclude to achieve a pre-set level of confidence in the correctness of election results. RLAs can be far more effective and efficient than traditional administrative audits, especially when performed by comparing individual ballots against digital records of ballot contents.

RLAs have been piloted in several states and local jurisdictions, and some states have passed laws to require their use.

End-to-End Verifiable Elections

[3]Securing the Vote, https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

End-to-end verifiability offers a public means of auditing elections. Election administrators don't need to be trusted to follow correct procedures, and election equipment doesn't need to be trusted to function properly.

An election is *end-to-end verifiable (E2E)* if two properties are met.

1. Voters can verify the accurate recording of their votes, and
2. Anyone can verify the accurate tallying of the recorded votes.

In other words, in an E2E-verifiable election, any alteration or incorrect counting of votes in an election can be detected by candidates, political parties, news outlets, interest groups, and even voters themselves; and this capability extends not only to external threats but even to potential internal threats by faulty or malicious equipment and by careless or dishonest election officials.

The technologies that enable E2E-verifiability are not new – they date back more than 30 years. However, they have evolved over that time and have become more practical, efficient, and voter friendly. After years of academic research and small pilots, the technology is now sufficiently mature and stable for widespread public use.

ElectionGuard

Microsoft is working to advance the development and adoption of E2E-verifiability and RLAs. Later this summer, along with partners, Microsoft will make available an open-source software developer kit (SDK) called **ElectionGuard** which will be available on GitHub for anyone to access freely. This software will enable voting system vendors, existing as well as new, to build end-to-end verifiability into their systems.

The technology is intended to augment – rather than replace – existing voting systems. It can be used in conjunction with a variety of voting scenarios including electronic ballot marking devices and hand-marked paper ballots read by precinct-based optical scanners. The voting processes will be almost identical to the processes that voters use and are familiar with today - with one exception. Voters will receive and be able to leave their polling locations with printed tracking codes and instructions for how they can, if they choose, confirm their votes when the election closes.

Ballot privacy is critical in elections. Elections have the unusual, perhaps even unique, requirement of not allowing participants to reveal their data – even if they choose to do so. A voter who can reveal a vote to someone else can sell that vote or be coerced into voting according to the wishes of another. Even though voters can verify the accurate recording of their votes, they cannot use their tracking codes to reveal their votes, and their privacy is thus protected.

ElectionGuard will enable election officials to publish encryptions of all votes cast in an election. Voters will have the ability to use their unique tracking codes to look up their encrypted votes and confirm that they are unaltered and correctly counted, but these tracking codes neither reveal votes nor allow them to be shown to others.

Microsoft will publish an open specification in conjunction with ElectionGuard that will enable anyone to write an election verifier that can review an election record and confirm that the encrypted votes are all properly constructed and correctly tallied. This will enable news outlets, universities, civil society organizations, candidates, political parties, and even individual voters to build their own programs to verify the results of an election. This confirmation is based entirely on the publicly available election record that is produced by an E2E-verifiable system and requires no special access nor trust in the system that produced the public record. Anyone can then run verifiers built by organizations or individuals they trust to publicly confirm that the results of an election are accurate.

In addition to enabling E2E-verifiability, the ElectionGuard SDK can enable an enhanced form of risk-limiting audits (RLAs) that offers better privacy than the systems in current use. At present, the process for implementing the highest quality RLAs includes the publication of digital cast vote records (CVRs) corresponding to the physical ballots cast in an election. However, the publication of these CVRs can subject voters to coercion and allow them to sell their votes. By using the ElectionGuard SDK, election officials will be able to publish CVRs in an encrypted form that doesn't impede auditing and allows for public verification of the election tallies – all without releasing sensitive raw election data that can be abused by malicious actors.

Together with the ElectionGuard SDK and specification details, Microsoft is working to produce reference implementations that demonstrate how the software can be effectively incorporated in a variety of settings. The first will be a universally-accessible ballot marking device designed to be easily usable by any voter – including those with a wide range of accessibility needs. An optical scanner that can support E2E-verifiability and enhanced RLAs with hand-marked paper ballots is also being designed. By providing tracking codes as a means of enabling verification of accurate recording of votes, the ElectionGuard SDK enables more accessible and usable voting methods with higher assurance than those in use today.

ElectionGuard and the associated reference implementations are the result of partnerships with many organizations, including Columbia University, Free&Fair, the Center for Civic Design, and VotingWorks.

System Certifications

For the sake of election security as well as ensuring a positive experience for voters, it is imperative to create an environment where innovation is possible. The current certification environment has significant limitations that can stifle the introduction of advanced technology into this market.

In 2002, the Help America Voting Act (HAVA) created the **Election Assistance Commission (EAC)** to set voting system standards, provide for the testing and certification of those voting systems, establish guidelines against which those systems are certified, and accredit independent non-federal laboratories that certify voting systems[4]. The EAC currently lists 57 certified voting systems deployed by seven registered voting system manufacturers.

The EAC certifies voting systems against the Voluntary Voting System Guidelines (VVSG). The EAC produced the first version of these guidelines, the 2002 Voting System Standards (VSS) prior to the enactment of HAVA. At that time, the VSS did not focus on security; but rather, "specif[ied] minimum functional requirements, performance characteristics, documentation requirements, and test evaluation criteria." There are currently 5 voting systems certified against these 2002 standards.

[4] 52 U.S.C. § 20971.

In 2005, the EAC updated the guidelines in collaboration with the Technical Guidelines Development Committee (TGDC) and the National Institute for Standards and Technology (NIST). These updated 2005 Voluntary Voting System Guidelines (VVSG 1.0) added security requirements to the certification criteria. The purpose of VVSG 1.0 was "to provide a set of specifications and requirements against which voting systems can be tested to determine if they provide all of the basic functionality, accessibility, and security capabilities required to ensure the integrity of voting systems." Of the 57 currently certified voting systems, 52 are certified against the VVSG 1.0. The EAC further modified the VVSG 1.0 and created the VVSG 1.1 to "enhance the testability and clarity of several of the requirements contained in version 1.0." No voting systems have ever been certified to VVSG 1.1; most systems in use were thus certified to a 2005 standard.

The certification process requires applicants to attest that the software submitted for certification testing shall be the exact software that will be used in production units consistent with section 1.6 of the VVSG 1.0. As the VVSG explains, "[t]o ensure that correct voting system software has been distributed without modification, the Guidelines include requirements for certified voting system software to be deposited in a national software repository. This provides an independent means for election officials to verify the software they purchase." This conformance requirement does not contemplate software updates, including security updates; and therefore, certified voting system software cannot be updated without losing its certification. This creates a dilemma for election officials when a vulnerability is discovered in a platform used by a voting system. The choice is between applying a security patch and losing certification or maintaining certification by using a system with a known vulnerability.

The EAC is now in the process of developing VVSG version 2 and has published the Technical Guidelines Development Committee recommendations – the VVSG 2.0 Principles and Guidelines document[5] – for comment. Notably, the Principles and Guidelines allows for software updates.

Microsoft has submitted comments on the VVSG 2.0 Principles and Guidelines. Those comments describe its strong support for the guidelines as an important step towards improving election technology security in the United States. Recognizing that diversity in organization, systems, networks, and assets of the

[5] VVSG 2.0 Guidelines, https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf

elections infrastructure expands the attack surface and increases the risk of a cyber-attack altering elections results, Microsoft's comments specifically emphasize its support for the VVSG 2.0 guidelines on auditability. Microsoft hopes there is a speedy process that will result in more current technology in use in our elections.

Public/Private Partnerships

It takes engagement across sectors to secure our elections, which is in part why Microsoft opted to comment on VVSG 2.0. This kind of engagement and collaboration is key. Recently, there have been several examples of public/private engagements in election security that showcase progress.

Local Government Partnerships

Recognizing the need for improved collaboration among governors' offices, election officials, and state cabinet agencies within local jurisdictions across states, the National Governor's Association (NGA) recently established a policy academy to develop strategies to improve cybersecurity operations and communications around elections. Six states, including Minnesota, Idaho, Hawaii, Virginia, Arizona, and Nevada, will participate in this academy and receive cybersecurity technical assistance from the NGA. The NGA policy academy will run from June to December of this year. It is a partnership with the University of Southern California (USC) and supported by the National Association of State Election Directors (NASED) and the National Association of Secretaries of State (NASS), with financial support from the Democracy Fund.[6]

Microsoft understands the value of such local partnerships and the impact of private sector participation. For example, when Minnesota was seeking additional cybersecurity support heading into the 2018 elections, the Secretary of State reached out to Microsoft to form a partnership and quickly deploy solutions[7]. As announced in the press release:

[6] "States Get Assistance on Election Cybersecurity", https://www.nga.org/news/press-releases/states-get-assistance-on-election-cybersecurity/

[7] Minnesota press Release "Secretary Simon Announces New Steps To Enhance Election Cybersecurity," https://www.sos.state.mn.us/about-the-office/news-room/secretary-simon-announces-new-steps-to-enhance-election-cybersecurity/

"Outside forces are targeting for attack our instruments of democracy," said Secretary Simon. "In Minnesota, the stakes are particularly high because we are the #1 state in voter turnout – with a total turnout of 74.7% of eligible voters casting ballots in 2016. With the 2018 election rapidly approaching, I am grateful to Microsoft for working with my office to enhance and harden our election cybersecurity ahead of the 2018 General Election. This is one of many steps my office has taken to ensure that Minnesota is more prepared than ever before to confront outside threats to our elections."

Federal Government Partnerships

In January 2017, the U.S. Department of Homeland Security (DHS) designated Election Infrastructure as a critical infrastructure subsector of the Government Facilities critical infrastructure sector. Election Infrastructure typically includes both physical and digital components. Computers, servers, databases, and other information technology systems and assets are used to fulfill elections roles, including storing voter registration systems, managing the entire voting process, recording and tabulating votes, reporting election night results, providing the public with general elections information, and compiling and storing electronic poll books. Recognizing that many election infrastructure assets and systems are owned and operated by the private sector, this designation galvanized relationships between critical infrastructure owners and operators, state and local governments, and federal departments and agencies.

DHS led in this area by assisting private election industry owners and operators with forming an Election Infrastructure Subsector Coordinating Council (SCC)[8], where participants share and collaborate on issues of election security. Microsoft is pleased to participate in the Election Infrastructure SCC. DHS similarly established the Election Infrastructure Subsector Government Coordinating Council (GCC)[9], which brings together federal, state, and local government bodies, including the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED). DHS often brings both councils together to collaborate on cybersecurity strategies and plans.

[8]DHS Sector Coordinating Councils, https://www.dhs.gov/sites/default/files/publications/govt-facilities%20-EIS-scc-charter-2018-508.pdf

[9] https://www.dhs.gov/sites/default/files/publications/govt-facilities-election-infrastructure-subsector-gcc-charter-2017-508.pdf

In November 2018, DHS hosted a mid-term election day situation room. DHS recognized that a coordinated response from federal, state, local, and private sector groups is the best way to mitigate risks of malicious cyber-activity associated with elections. Microsoft was a participant and coordinated with Microsoft's own election day dedicated situation rooms in Washington, DC and Microsoft headquarters in Redmond, WA. Allowing elections infrastructure stakeholders to share information in real-time on election day facilitates a coordinated response should a cyber-incident occur.

Attempts to interfere with the electoral process extends to the political campaign environment as well, which has been very much in focus at the Federal Election Commission (FEC) this year. Though much attention has been given to the Russian "Internet Research Agency's" attempts to sow discord through online propaganda targeted at American voters, the hacking of the online accounts of political operatives and party committees must not be overlooked.[10]

With more than 60 million users of its paid Office365 (O365) cloud-based productivity software and free Outlook.com and Hotmail.com web-based e-mail services, Microsoft found itself in a unique position to protect election-sensitive users of its products against such hacking. To that end, Microsoft requested and received an advisory opinion from the FEC confirming that the company may offer a package of enhanced online account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers, including but not limited to federal candidates and national party committees. The FEC concluded that the provision of AccountGuard[11] is permissible and is not a prohibited in-kind contribution under campaign finance law.[12]

Until this advisory opinion, the FEC had not robustly addressed the provision of cybersecurity services to political campaigns and national committees. In

[10]Ofc. of the Director of Nat' I Intelligence, Background to "Assessing Russian Activities and Intentions in Recent U.S. Elections" (Jan. 6,2017) at 2-3, https://www.dni.gov/files/documents/ICA_2017_01.pdf; The John Podesta Emails Released by WikiLeaks, CBSNEWS.COM (Nov. 3,2016), https://www.cbsnews.com/news/the-john-podesta-emails-released-by-wikileaks/.

[11] "Protecting Democracy with Microsoft AccountGuard", (August 20, 2018), https://blogs.microsoft.com/on-the-issues/2018/08/20/protecting-democracy-with-microsoft-accountguard/

[12] FEC Advisory Opinion 2018-11, https://www.fec.gov/files/legal/aos/2018-11/2018-11.pdf

response, this advisory opinion sparked a series of similar requests for approval[13] from cybersecurity firms to provide cybersecurity services to members of Congress, political campaigns, and national committees.

These examples demonstrate that the private sector has a shared responsibility to protect the election ecosystem and we need the continued support and partnership of government counterparts at the local and federal level to do more.

Conclusion

As the 2020 election grows closer, it's clear that there is much work left to do. There are numerous challenges – technical, regulatory, financial, educational, and otherwise – to overcome. Congressional collaboration with the states to expedite and fund these efforts would help respond to these growing challenges.

I am encouraged to see organizations and individuals across many different sectors actively working together to identify solutions and drive improvement. The National Academies report offers numerous concrete steps which can dramatically improve the state of our election infrastructure. Microsoft's ElectionGuard and other offerings from its Defending Democracy Program can help address some of the technological challenges, but this represents only a fraction of the need. Congressional incentives to modernize our infrastructure and implement good auditing technologies together with work to update standards could help greatly at moving us towards a more secure election ecosystem.

I would again like to thank this committee for the opportunity to address this vital topic and look forward to your questions. Thank you.

[13] FEC Advisory Opinion 2018-15 (approving Senator Wyden's request to use campaign funds for cybersecurity expenses), https://www.fec.gov/data/legal/advisory-opinions/2018-15/; FEC Advisory Opinion 2018-12 (approving the provision of free cybersecurity resources to candidates and political party committees, by nonprofit corporation and its private sector sponsors and partners), https://www.fec.gov/files/legal/aos/2018-12/2018-12.pdf