Written Testimony of
Tom Burt

Corporate Vice President
Customer Security & Trust
Microsoft Corporation

to the House Judiciary Committee
to discuss emerging technologies and the security of US elections
September 27th, 2019

Chairman Nadler, Ranking Member Collins, Members of the Committee, thank you for the opportunity to testify today on the important topic of how emerging technology can contribute to the security of our elections.

My name is Tom Burt and I am the Corporate Vice President of Customer Security and Trust (CST) at Microsoft, a cross-disciplinary team made up of engineers, lawyers, policy advocates, business professionals, data analysts, and cybercrime investigators who are collectively responsible for ensuring customer trust in Microsoft's products and online services[1]. We focus on advocating for and contributing to the stability and security of democratic institutions globally. Specifically, last year we created the Defending Democracy Program. This team works with a variety of governmental and non-governmental stakeholders in democratic countries globally to achieve the following goals:

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

[1] 60 Minutes, April 21, 2019: https://www.cbsnews.com/video/a-marriage-made-in-hell-superbugs-easter-island/

THREATS AGAINST DEMOCRATIC INSTITUTIONS

Microsoft's work to preserve and protect our electoral processes and institutions builds upon the company's experience in assessing and tracking cybersecurity threats. The Microsoft Threat Intelligence Center (MSTIC) has focused on tracking nation-state actors for more than a decade. We provide notification to customers, including government customers, when an online service account has been targeted or compromised by a nation-state actor that is tracked by the MSTIC team.

In the past year, Microsoft notified nearly 10,000 customers[2] that they've been targeted or compromised by nation-state attacks. About 84% of these attacks targeted our enterprise customers, and about 16% targeted consumer personal email accounts. While many of these attacks are unrelated to the democratic process, this data demonstrates the significant extent to which nation-states continue to rely on cyberattacks as a tool to gain intelligence, influence geopolitics or achieve other objectives.

The majority of nation-state activity in this period originated from actors in three countries – Iran, North Korea and Russia. We have seen extensive activity from the actors we call Holmium, Phosphorus, and Mercury operating from Iran, Thallium operating from North Korea, and two actors operating from Russia we call Yttrium and Strontium. This data has been compiled by MSTIC which works every day to track these global threats. We build this intelligence into our security products to protect customers and use it in support of our efforts to disrupt threat actor activities through direct legal action or in collaboration with law enforcement. But let's be clear – cyberattacks continue to be a significant weapon wielded in cyberspace. In some instances, those attacks appear to be related to ongoing efforts to attack the democratic process.

Last August Microsoft instituted enhanced cybersecurity services for campaign users of Office 365 and free email services[3]. The program is called AccountGuard, and since its launch in 2018 we have uncovered attacks specifically targeting organizations that are fundamental to democracy. We have steadily expanded AccountGuard to political campaigns, parties, think tanks, and democracy-focused

[2] "New cyberthreats require new ways to protect democracy", July 17, 2019: https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/

[3] "We are taking new steps against broadening threats to democracy", Aug 20, 2018: https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy/

nongovernmental organizations (NGOs), in 26 countries across four continents. While this service is relatively new, we've already made 838 notifications of nation-state attacks targeting organizations participating in AccountGuard. This data shows that democracy-focused organizations in the United States should be particularly concerned as 95% of these attacks have targeted U.S.-based organizations. By nature, these organizations are critical to society but have fewer resources to protect against cyberattacks than large enterprises.

Many of the democracy-focused attacks we've seen recently target NGOs and think tanks and reflect a pattern that we also observed in the early stages of some previous elections. In this pattern, a spike in attacks on NGOs and think tanks that work closely with candidates and political parties, or work on issues central to their campaigns, serve as a precursor to direct attacks on campaigns and election systems themselves. Similar attacks occurred in the U.S. presidential election in 2016 and in the last French presidential election. In 2018 we announced attacks targeting, among others, leading U.S. senatorial candidates and think tanks associated with key issues at the time[4]. Earlier this year we saw attacks targeting democracy-focused NGOs in Europe close to European elections[5]. As we head into the 2020 elections, given both the broad reliance on cyberattacks by nation-states and the use of cyberattacks to specifically target democratic processes, we anticipate that we will see attacks targeting U.S. election systems, political campaigns or NGOs that work closely with campaigns.

Our adversaries have a stated goal of seeking to diminish the confidence of our citizens in the processes that are at the very core of our democracy. We should anticipate that we will see more attacks on our election processes in 2020 in furtherance of this goal.

MULTI-STAKEHOLDER RESPONSE

Combatting these attacks will require a joint effort from private sector actors such as Microsoft, as well as state, local and federal governments, civil society, academia, and voters themselves.

[4] "Microsoft Says It Stopped Cyberattacks on Three 2018 Congressional Candidates", Time, July 19,2018: https://time.com/5343585/microsoft-candidate-cyberattacks/

[5] "New steps to protect Europe from continued cyber threats", Feb. 20, 2019 https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/

Cyber-attacks, especially ransomware attacks, are increasingly targeting state and local authorities, including for example, Atlanta (GA), Baltimore (MD), Cleveland (OH), Greenville (NC), Imperial County (CA), Stuart (FL), Augusta (ME), Lynn (MA), Cartersville (GA). Most recently there was an attack on over twenty government entities in Texas. Overall, we can reasonably expect that the situation will only get worse. Importantly, these and other attacks are increasingly leveraging sophisticated tools that are developed by governments, creating a dangerous ecosystem of cyber-weapons and requiring adoption of international norms for responsible behavior online. Through our Digital Diplomacy team in CST, Microsoft works to advance support for the adoption and observance of such norms.

Microsoft supports the multi-stakeholder approach taken by the Paris Call for Trust and Security in Cyber Space[6]. It reaffirms a number of norms and principles established in other forums, including at the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN-GGE), and at the G7 and G20, respectively. Importantly, the Paris Call includes a comparatively new principle to protect electoral processes from foreign interference - *Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.*

However, what truly distinguishes the Paris Call is that it recognizes that a multi-stakeholder approach is essential to achieve success. The Call has so far been signed by 67 nations, 139 civil society organizations and 358 industry members all agreeing to nine core principles to govern conduct in cyberspace. Microsoft was one of the private sector signatories and we will continue to advocate that all governments agree to observe the nine principles of the Call.

SECURING EXISTING ELECTION SYSTEMS

As the Senate Intelligence report on Russian interference in the 2016 U.S. elections[7] recently confirmed, at least 21 states had their election systems targeted by Russian actors, likely more. While the report states there was no

[6]Paris Call for Trust & Security in Cyber Space: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[7] Report of the Selection Committee on Intelligence United States Senate: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

evidence found to indicate vote tallies or voter registration systems were deleted or modified, the adversary succeeded at what was likely their primary goal – undermining U.S. voter's trust and confidence in our electoral system.

The undermining of such a vital democratic institution should cause us all alarm. At Microsoft, our Defending Democracy team began to review election infrastructure in the U.S. to identify areas where we could make a unique contribution to the security of our elections and restore voter confidence.

One surprising thing we identified was the active use of Windows 7 on several certified voting systems. For context, Windows 7 was launched by the company in 2009, and therefore represents decade-old security engineering. At that time we committed to supporting Windows 7 for ten years, and so in January of 2020 Windows 7 will reach its end of life and no longer be a supported operating system.

As we head into the 2020 elections though, knowing that many certified election systems are running Windows 7 without access to security patches does not sit well with us. With that in mind, last week we decided to offer free Windows 7 Extended Security Updates (ESUs) to federally certified election systems in the US through the end of 2020.[8] We have worked with the major election vendors to ensure they have access to these ESUs and are able to deploy them to customers as needed. We also are working with vendors who do not have a Windows 10 offering currently in the market to provide technical guidance and support as they make that transition.

STANDARDS AND CERTIFICATION

Providing free security updates does not completely solve the problem, however. A critical challenge to advancing the technical security of our vote is the complex and outdated federal election machine certification process. The current standards by which election machines are being certified today are even older than Windows 7!

The certification process has significant limitations that can stifle the introduction of advanced technology into this market, but also hinders basic security hygiene.

[8]"Extending free Windows 7 security updates to voting systems", Sep 20, 2019: https://blogs.microsoft.com/on-the-issues/2019/09/20/extending-free-windows-7-security-updates-to-voting-systems/

In the current system, if a certified device were to accept a minor security patch, it would be subjected to the same complete re-certification process that would be necessary for a major software update. This creates a perverse disincentive for election officials and vendors to deploy security patches to their machines, leaving our elections vulnerable via a self-inflicted wound.

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[9]. The EAC certifies voting systems against the Voluntary Voting System Guidelines (VVSG). In 2005, the EAC updated the 2002 Voting System Standards (VSS) 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) for the first time added security requirements to the certification criteria. Of the 57 currently certified voting systems, 52 are certified against the VVSG 1.0 and 5 against the 2002 standard that did not include security requirements. The EAC has 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. In the world of cybersecurity, this is ancient times.

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

[9] 52 U.S.C. § 20971.

maintaining certification by using a system with a known vulnerability. With today's threats, from agile and well-resourced adversaries attacking our election systems, this impediment to the rapid deployment of security updates is simply untenable and must be promptly rectified.

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[10] – for comment. Notably, the Principles and Guidelines allows for software updates, though the details of how security updates will be applied to systems without triggering a comprehensive certification process is still unclear.

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 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 strongly encourages the rapid adoption of VVSG 2.0 guidelines with provisions that support a much more agile and rapid process for the adoption and deployment of secure election technology.

INNOVATIVE ELECTION TECHNOLOGY - ELECTIONGUARD

Outdated standards not only impact the security of our existing systems, they serve as a hurdle for the introduction of new and innovative technology. We know this firsthand, as just this week we released a free, open-source software development kit (SDK) called ElectionGuard that will enable **end-to-end (E2E) verifiable (E2E)** elections.[11] **Simply put, ElectionGuard technology will enable the most secure and trustworthy elections in the history of the United States**.

In an end-to-end-verifiable election, any alteration or incorrect counting of votes can be detected by candidates, political parties, news outlets or interest groups; and this capability extends not only to external threats but even to potential

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

[11] "ElectionGuard available today to enable secure, verifiable voting", Sept. 24, 2019: https://blogs.microsoft.com/on-the-issues/2019/09/24/electionguard-available-today-to-enable-secure-verifiable-voting/

internal threats by faulty or malicious equipment or by overworked or even dishonest election officials. Even more importantly, individual voters will be able to verify that their votes were recorded and counted properly.

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 builds on Microsoft Research Senior Principal Cryptographer Josh Benaloh's foundational work on E2E- verifiability[12] accomplished through the use of homomorphic encryption. The ElectionGuard open-source SDK is available on GitHub[13] for anyone to review, though we have been working closely with all the major US election vendors, encouraging them to incorporate the code directly into their systems.

ElectionGuard 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 were properly counted when the election closes[14].

Ballot privacy is critical in elections. Elections have the unusual, perhaps even unique, requirement of not allowing participants to reveal their data – even if

[12] Written Testimony of Josh Benaloh to Subcommittee on Investigations & Oversight and the and the Subcommittee on Research & Technology: https://science.house.gov/imo/media/doc/Benaloh%20Testimony.pdf

[13] GitHub is the largest developer community in the world, and the home of 80% of all active open source projects. And it's more than just open source - more than 2 million organizations that use GitHub for their software projects, including the vast majority of technology startups and 50% of the Fortune 100

[14]We acknowledge this solution depends on the voter having access to a smart phone or to broadband connectivity. Microsoft notes that broadband connectivity is also an urgent national problem that we are committed to helping solve. We've contributed to this effort through our Microsoft Airband Initiative, a five-year commitment to bring broadband access to 3 million unserved Americans living in rural communities by July 2022. Microsoft is partnering with a number of local providers across the US to offer new broadband services where there is no option or affordable alternative.

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. With ElectionGuard voters can verify the accurate recording of their votes but cannot use their tracking codes to reveal their votes, and their privacy is thus protected.

Microsoft published an open specification in conjunction with ElectionGuard that enables 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.

In addition to enabling E2E-verifiability, the ElectionGuard SDK enables 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 could be abused by malicious actors.

DEMONSTRATION MACHINE AND ACCESSIBLE VOTING

To showcase the ElectionGuard technology, we have constructed reference implementation devices that demonstrate how it could be incorporated into low cost, secure and accessible voting machines. This demo system is not intended for sale – rather it exists to showcase the ElectionGuard code while highlighting other features that may be considered for new voting systems. At Microsoft our products are built to empower everyone, everywhere. [15] That principle applies to voting as well where accessibility is a paramount consideration for all voting officials. We therefore designed ElectionGuard to support a range of accessibility features including the Xbox adaptive controller for certain physical disabilities and

[15] Microsoft Accessibility: https://www.microsoft.com/en-us/accessibility

interfaces for other accessibility systems. We have several of these demo systems in our Redmond and DC offices and invite Members of the Committee to a demonstration of how emerging technology can be used to improve the security and accessibility of our elections.

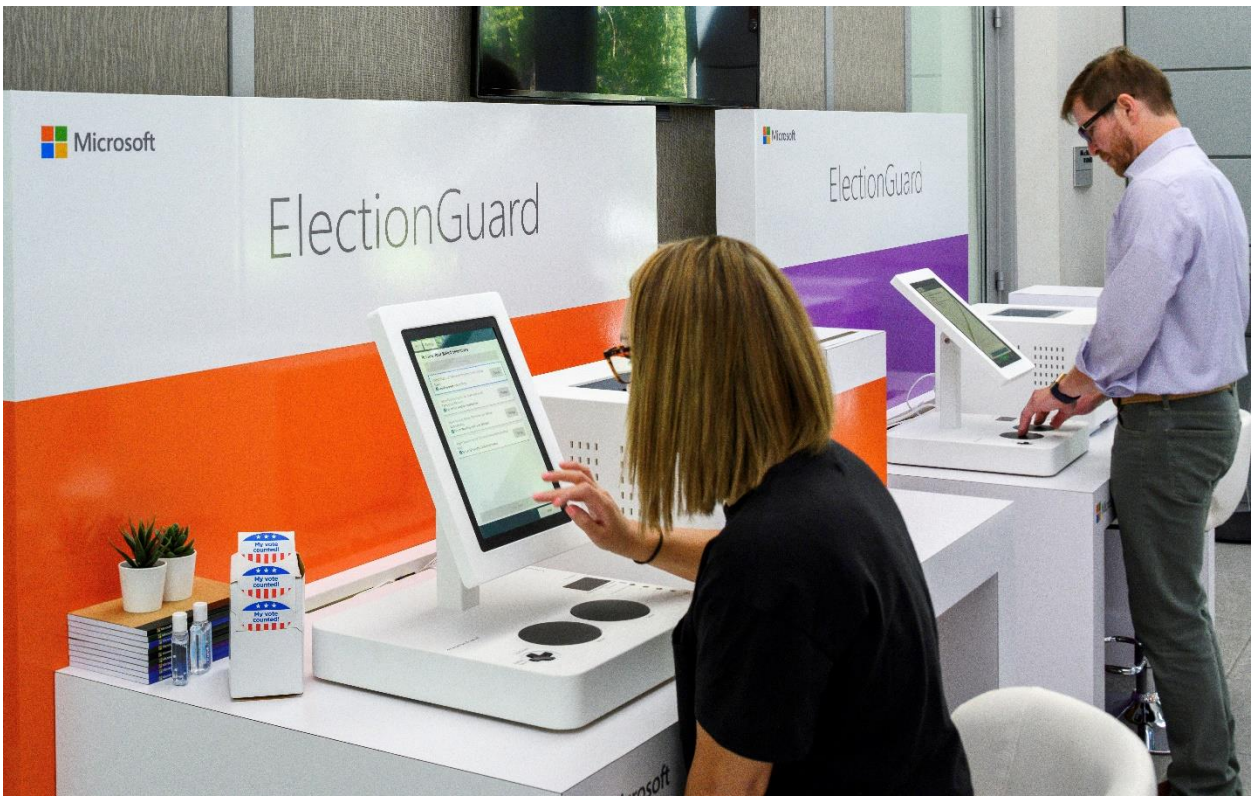

Figure 1 Microsoft employees testing an ElectionGuard demonstration system at the Aspen Security Forum

PAPER BALLOTS

As noted above, ElectionGuard is designed to support a wide range of voting systems and will continue to be enhanced to support others. In our reference implementation we demonstrate a system with a highly efficient, convenient and accessible ballot marking device which supports printed ballots that can be deposited and retained by voting officials as either the primary artifact or as a back-up. The recent debate about the security of voting devices has resulted in some calling for a return to manually marked paper ballots exclusively. While paper can be a helpful tool, it is not a goal in and of itself. The goals of ElectionGuard technology are to ensure security, trustworthiness, accessibility and efficiency – goals that can be achieved whether paper is used as primary artifact or backup, but which cannot be fully realized without ElectionGuard.

PROTECTING POLITICAL ACTORS

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) over the past 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 was also a key attack mounted by Russia and must not be overlooked.[16]

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 Microsoft may offer a package of free enhanced online account security protections at no additional charge on a nonpartisan basis to its election-sensitive customers. The FEC issued an Advisory Opinion concluding that the provision of AccountGuard is permissible and is not a prohibited in-kind contribution under campaign finance law.[17]

Until this advisory opinion, the FEC had not robustly addressed the provision of cybersecurity services to political campaigns and national committees. In response, this advisory opinion sparked a series of similar requests for approval[18] from cybersecurity firms to provide cybersecurity services to members of Congress, political campaigns, and national committees.

Political campaigns are fast-moving environments that face significant security threats from nation-state actors and criminal scammers – much like large enterprises. However, unlike enterprises, political campaigns often must ramp up and down quickly, vary in their ability to hire dedicated IT staff, and have

---

[16]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/.

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

[18] 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

unpredictable budgets. In some cases, they rely on scrappy "accidental administrators" who help with IT on the side; in other cases, they have experienced IT consultants but need to focus their budgets on getting out their candidates' message.

For these reasons, Microsoft recently announced the availability of Microsoft 365 for Campaigns.[19] The Microsoft 365 for Campaigns sign-up process allows for streamlined enrollment into Microsoft's AccountGuard service and is available at a price of just $5 per user per month – the same price as offered to nonprofits and nongovernmental organizations. Microsoft 365 for Campaigns, brings the high-end security capabilities of the Microsoft 365 Business offering – with specialized "wizards" to make it easy to deploy – to political campaigns at this reduced rate on a nonpartisan basis.

EMERGING THREATS

A few weeks ago CISA Director Chris Krebs drew attention to the threat of ransomware attacks against our local governments and the impact that could have on our elections if executed against voter registration systems close to, or on, election day.[20] We agree this is a risk that deserves attention from all election security stakeholders. Voter registration databases (some of the same systems targeted in 2016), are vulnerable because they are some of the only election sensitive systems that are regularly connected to the internet. We have advised Director Krebs that we stand ready to participate with CISA and others in the tech community to seek solutions, including providing all election officials with simple step-by-step recommendations on important security hygiene such as two-factor authentication for all relevant accounts, how to secure registration and other data systems, establish secure back-ups, and engage in exercises to ensure rapid restoration of data in the event of an attack.

An additional emerging threat is the increased potential for bad actors to use artificial intelligence to create malicious synthetic media, better known as "Deepfakes". Advances in synthetic media have created clear benefits; for example, synthetic voice can be a powerful accessibility technology, and synthetic

[19]"Protecting political campaigns from hacking", May 6, 2019: https://blogs.microsoft.com/on-the-issues/2019/05/06/protecting-political-campaigns-from-hacking/

[20]"CISA Director's Outlook on Ransomware", Aug 23, 2019: https://www.politico.com/newsletters/morning-cybersecurity/2019/08/23/cisa-directors-outlook-on-ransomware-5g-more-727286

video can be used in film production, criminal forensics, and artistic expression. However, as access to synthetic media technology increases, so too does the risk of exploitation. Deepfakes can be used to damage reputations, fabricate evidence, and undermine trust in our democratic institutions. To help guard against this challenge, Microsoft has established clear principles that govern its use and deployment of synthetic media and other artificial intelligence, including fairness, inclusiveness, reliability & safety, transparency, privacy & security, and accountability. Furthermore, Microsoft has engaged with partners in academia, civil society, and industry through forums like the Partnership on AI, where we can work together to advance best practices for the ethical use of AI and we and others are working on technical solutions to abuse of synthetic media systems.

CONGRESSIONAL ACTION

We applaud the Senate for its recent bi-partisan agreement to release additional funding to the states. This is an essential step in the right direction to equip local officials and to protect our election systems. But there is still more to be done. In our discussions with voting officials around the country we have learned that consistent and reliable funding over time will best enable election officials to plan ahead, purchase new equipment rather than letting outdated systems remain active, and invest in the kind of cybersecurity training and staffing that we expect of all critical infrastructure providers. Our adversaries are relentless and well resourced. To ensure we can maintain defenses, our state and local voting officials need a durable source of federal financial support so that the most secure technology can be deployed rapidly to ensure our vote is protected. The stewardship of our democracy demands nothing less.

In addition to funding, we need certification standards that are responsive to current technology and threats. Standards should incentivize security patching and updates, not create red tape that stands in the way of cyber best practices. While there are constructive conversations ongoing at the EAC, the pace of adoption and execution is slow, and the path to minimal security updates is still unclear. We hope Congress will encourage their colleagues at the EAC to pursue a speedy path to new standards, and in that process select a format that does not allow outdated standards to burden adoption of the most secure technology in the future.

Finally, Congress should encourage a multi-stakeholder and global commitment to pursue practical projects that are essential to protecting our online world. We must particularly strengthen our collective capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.

CONCLUSION

We live in a world with agile enemies who are persistent in their efforts to interfere in our democratic process. Voters are looking to us – private industry and federal and local governments – to be leaders. Our citizens deserve to be able to cast their vote with confidence that it will be counted without manipulation. We at Microsoft are committed to doing our part to ensure that every vote is counted and that every voter has confidence in our free, fair and democratic elections.