Written Testimony of
Ginny Badanes
Director of Strategic Projects
The Defending Democracy Program
Microsoft Corporation

to the Subcommittee on Cybersecurity, Infrastructure Protection & Innovation
of the House Committee on Homeland Security
The Road to 2020: Defending Against Election Interference
November 19, 2019

Chairman Richmond, Ranking Member Katko, Members of the Subcommittee, thank you for the opportunity to testify today on the important topic of campaign security.

My name is Ginny Badanes and I am the director of strategic projects for Microsoft's Defending Democracy program. We focus on advocating for and contributing to the stability and security of democratic institutions globally. In a non-partisan manner, our team works with a variety of governmental and non-governmental stakeholders in democratic countries 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 campaign organizations 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.

Though the Defending Democracy team undertakes several initiatives in pursuit of these goals, my testimony today will focus on our efforts to increase the cybersecurity and resilience of campaign organizations.

Threats to Campaign Organizations

To address how campaign organizations can protect themselves, it is helpful to first understand the threats that they are up against. Campaign organizations face uniquely challenging circumstances when it comes to securing themselves. Outside of a handful of Presidential campaigns, many campaign organizations often have limited technology budgets and usually even more limited cybersecurity expertise. Yet, they can face outsized threats, an asymmetry that can have detrimental effects on our democratic processes. Campaign organizations are like technology startups with enterprise cybersecurity needs.

Microsoft's work to protect campaign organizations and democratic institutions broadly 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 election-sensitive customers, when an online service account has been targeted or compromised by a nation-state actor that we are tracking. We continuously track these global threats, building this intelligence into our security products to protect customers and using 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.

In the past year, Microsoft notified nearly 10,000 customers, including campaign organizations,[1] that they have 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. 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.

Based upon the threats we are tracking, most of the nation-state activity in recent months originated from actors in three countries – Iran[2], North Korea and Russia[3]. We have also seen activity by actors operating from China, but not at the same volume as the actors in these three nations. These actors have targeted a variety of industries including a number of stakeholders that are important to political dialogue and democratic processes, including think tanks, universities, diplomatic entities, journalists, current and former government officials, and campaign staff.

Microsoft & Campaign Security

Recognizing the unique needs of campaign organizations, Microsoft offers services to help them increase their cybersecurity and resilience.

- Online account security protection
- Security guidance, ongoing education and training
- Microsoft 365 for Campaigns

Online Account Security Protection

In August of 2018, Microsoft instituted enhanced cybersecurity services for campaign users of Office 365 and free consumer email services. With more than 60 million users of its paid Office365 (O365) cloud-based productivity software and free Outlook.com and Hotmail.com

[1] New Cybersecurity Threats require new ways to protect democracy. https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/

[2] Recent Cyberattacks Require Us All To Be Vigilant. https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/

[3] New Cyberattacks Targeting Sporting and Anti-Doping Organizations. https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

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 Federal Election Commission (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 Advisory Opinion concluded that the provision of such services is not a prohibited in-kind contribution under campaign finance law.[4]

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[5] from cybersecurity firms to provide cybersecurity services to members of Congress, political campaigns, and national committees at reduced costs or at no cost at all.

The Microsoft service is called **AccountGuard**[6], and it serves two primary functions.

1) **Cross-Account Notifications:** We recognize that threat actors do not only attack the enterprise accounts of their targets, they go after the target's personal accounts as well. We provide AccountGuard customers with the ability to enroll the personal Microsoft email accounts (Hotmail.com, Outlook.com) of staff and other affiliates of their organization. This optional enrollment provides our threat monitoring team with valuable information about what might otherwise appear to be a typical consumer account. More importantly, it allows us to notify the individual and organization quickly if we identify a threat-actor targeting that personal account.

2) **Nation-State Attack Enhanced Monitoring:** If an AccountGuard customer is targeted by a nation-state actor that we track, the team provides customers with additional services and notification. In addition to informing them about the attack, we include information about what to do next, especially if the attack resulted in a breach. This additional communication ensures that notifications reach the right person within an organization.

Since the launch of AccountGuard we have uncovered attacks specifically targeting organizations that are fundamental to democracy. We have steadily expanded AccountGuard to political campaigns, political parties, think tanks, and democracy-focused nongovernmental organizations (NGOs), in 26 countries across four continents. While this service is relatively new, we've already made over 900 notifications of nation-state attacks targeting organizations

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

[5] 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

[6] Microsoft AccountGuard, https://www.microsoftaccountguard.com/en-us/

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 that 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, typically serves as a precursor to direct attacks on campaign organizations 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 detected attacks targeting, among others, U.S. Senate offices, and think tanks associated with key issues at the time.[7] Earlier this year we saw attacks targeting democracy-focused NGOs in Europe close to European elections.[8] 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 potential attacks targeting U.S. election systems, campaign organizations or NGOs that work closely with campaign organizations.

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.

Security Guidance, Ongoing Education & Training

Informed by our observations about campaign challenges, Microsoft provides in-person cybersecurity trainings tailored to the specific needs of the campaign community regardless of whether there is any formal relationship with Microsoft.[9] These trainings cover the basics of cybersecurity hygiene and highlight many of the best practices recommended by our partners at Harvard Belfer Center in their Cybersecurity Campaign Playbook[10]. To date, we've trained over 1000 political professionals in 13 countries with our security workshop trainings.

In addition to the in-person trainings, we conduct webinars focused on specific cybersecurity topics of interest to campaign organizations. Just this week, for example, Microsoft security

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

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

[9] We acknowledge these security solutions and ongoing trainings depend on the campaign organizations and individuals 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

[10] Cybersecurity Campaign Playbook, https://www.hks.harvard.edu/publications/cybersecurity-campaign-playbook

experts are hosting two webinars representative of our training efforts in this area. One helps non-technical election sensitive customers learn how to protect their user accounts. We will cover topics such as common attack vectors, multi-factor authentication, credential hygiene, and identity best practices. The other webinar helps information technology (IT) professionals in the election-sensitive space learn technical best practices and tools available to them to secure their organization's environment.

Finally, all our AccountGuard customers receive monthly guidance from us. This guidance highlights stories of relevance, provides best practices, and promotes better cybersecurity hygiene across their organization.

M**icrosoft 365 for Campaigns**

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

While the AccountGuard service is a step in the right direction to help protect campaign organizations facing these challenges, we recognized that we could do more to provide this community with access to secure, reliable, accessible, and affordable software. For those reasons, Microsoft recently announced the availability of **Microsoft 365 for Campaigns**.[11]

First, to address the constrained budgets of campaign organizations, we have used our non-profit pricing model for this offering so campaign organizations can get access to software at a significantly reduced rate.

Second, to address the problem of ease of use for non-technical users, we have streamlined the configuration and setup of high-impact security settings. With only a click or two, customers can now turn on recommended security features to create a secure baseline from which to operate their campaign organization.

Just a few examples of the settings that can now be automated –

- *Enabling multi-factor authentication:* A second layer of security for sign-ins
- *Turning on Office 365 Advanced Threat Protection:* A service that protects emails, links, and files from phishing and malware attacks
- *Providing device protection*: Secures access to sensitive data on mobile devices using a service called Microsoft Intune[12]

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

[12] Microsoft InTune, https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/microsoft-intune

This offering derives from our Microsoft 365 Business product, which is tailored to small and medium businesses. That means campaign customers can now access the high-end security capabilities typically leveraged by enterprise customers, enjoy easier deployment of those features, and do so at an affordable rate.

Other Ways Campaign Organizations Can Protect Themselves

While we encourage innovation in this area, campaign organizations can best protect themselves by employing basic hygiene.[13] A few examples of how that can be achieved:

- *Password management:* In 2016, Microsoft saw over 10 million username/password pair attacks every day. This gives us a unique vantage point to understand the role of passwords in account takeovers.[14] Despite general awareness of the importance of using unique passwords to secure data, users admitted to reusing the same password 62% of the time for multiple accounts as recently as a year ago.[15] As a result, we train campaign organizations to use strong unique passwords and more importantly, to use password managers to generate them.
- *Two-factor authentication:* We encourage campaign organizations to use a two-step authentication source like a phone app or a physical key for all accounts.
- *Using a cloud service provider:* We encourage campaign organizations to leverage cloud services for email, documents, and infrastructure and avoid public or anonymous sharing.
- *Using a secure communications platform*: For sensitive data, Microsoft encourages campaign organizations to use encrypted communications channels and avoid using public Wireless Fidelity (Wi-Fi) channels for accessing sensitive information.

Emerging Threats

Earlier this fall, Director of the Cybersecurity and Infrastructure Security Agency (CISA), 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.[16] We agree this is a risk that deserves attention from all election security stakeholders. Voter registration databases (some of the same systems targeted in

[13] Your Pa$$word Doesn't Matter. https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Your-Pa-word-doesn-t-matter/ba-p/731984.

[14] Microsoft Password Guidance by the Microsoft Identity Protection Team. https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf.

[15] See eg. Passwords Reuse Abound Recent Survey Shows. https://www.darkreading.com/informationweek-home/password-reuse-abounds-new-survey-shows/d/d-id/1331689.

[16] "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

2016), are vulnerable because they are some of the only election sensitive systems that are regularly connected to the internet. We are currently exploring how we can work with government and others in the tech community to continue to raise awareness of this threat while also providing additional solutions to protect against ransomware. Basic security recommendations in this context include using modern technology, setting up two-factor authentication for all relevant accounts, creating secure back-ups, and engaging 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 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 to work together to advance best practices for the ethical use of AI. One such effort includes a recent "Deepfakes Detection Challenge" we helped launch together with Facebook and the Partnership on AI, a technology industry consortium focused on best practices for AI systems, which invites researchers to build new technologies that can help detect deepfakes and manipulated media.

What Congress Can Do

When conducting trainings for political parties and campaign organizations in democracies around the world, we always encourage leadership of those organizations to attend the sessions alongside their teams. While leaders may not have a technical background, they play an incredibly important role when it comes to their organization's cyber health: setting the culture.

Similarly, Congress plays a critical role in securing our campaign organizations and elections. By holding this hearing on the cybersecurity health of campaign organizations and the election space more broadly, the Committee is contributing to the culture of security that is necessary to ensure a more secure environment.

Beyond culture setting, Congress also can contribute to a multi-stakeholder approach to addressing the threats themselves. We believe that combatting 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 campaign organizations themselves.

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. Microsoft advances 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[17]. 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 endorsed by over 1000 signatories, the largest coalition of signatories ever in support of a cybersecurity document: 74 governments, 357 civil society and public sector organizations, and 607 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.

While we are here today to discuss campaign organizations, we’d be remiss not to address other ways Congress can support securing our elections. 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 owners and operators. 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.

Conclusion

Campaign organizations face the threat of capable, well-funded, and agile adversaries. Organizations of any size would struggle to be prepared for these challenges, but the size and

[17] 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

nature of campaign organizations makes them especially vulnerable. There is a lot that campaign organizations can do to protect themselves. They can create a culture of cyber-awareness, encourage everyone associated with the campaign organization to turn on two-factor authentication on all their accounts (personal as well as organizational), and be aware of phishing campaigns. These are the most important actions campaign organizations can take to protect themselves. But they need additional help. They will benefit from industry partners providing access to tools that support these efforts. They will benefit from NGOs like Defending Digital Campaigns and Cyberdome who can help filter and provide tools at affordable rates. And finally, they would benefit from Congressional and Executive Branch leadership in multi-stakeholder engagement, especially around establishing international norms to discourage nation-state attacks against our democratic institutions.