CENTER FOR
DEMOCRACY
& TECHNOLOGY

Testimony of

Dr. Joseph Lorenzo Hall
Chief Technologist
The Center for Democracy & Technology[1]

Hearing on "Election Security"
The Committee on House Administration, U.S. House of Representatives

May 8, 2019

Chairwoman Lofgren, Ranking Member Davis, and members of the Committee:

Thank you for the opportunity to speak to you today and to submit these written remarks on one of the most critical subjects facing our democracy today, election security.

My name is Joseph Lorenzo Hall,[2] I'm the Chief Technologist at the Center for Democracy & Technology (CDT). For almost twenty-five years, CDT has been a leader in protecting digital civil liberties and defending democratic principles online. With multidisciplinary programs focused on free expression, privacy and data, an open internet, security and surveillance, and internet architecture, CDT provides a complete and collaborative approach to identifying practical solutions and policy recommendations for today's most difficult technology questions.

I oversee CDT's Election Security and Privacy project, which focuses on educating the elections community about cybersecurity concepts and practices through a set of online interactive courses, "Election Cybersecurity 101" field guides, and by holding regular briefings and trainings for election officials, legislative staff, and journalists. I hold a PhD and Masters degrees from the University of California, Berkeley in information science and astrophysics; my PhD dissertation work involved studying electronic voting systems as a critical case study in the transparency of black box technologies used by governments as they increasingly adopt digital technologies.

[1] The Center for Democracy & Technology (CDT) is a nonpartisan nonprofit public interest advocacy organization that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communication technologies. With expertise in law, technology, and policy, CDT promotes policies that protect and respect users' fundamental rights to privacy and freedom of expression, and enhance their ability to use communications technologies in empowering ways. CDT has testified in front of Congress numerous times in its over 25-year history and is a highly trusted voice in technology policy. I would like to thank CDT staff and especially Senior Technologist Maurice Turner for assistance with preparing this testimony. Please direct additional inquiries to me via email (joe@cdt.org) or phone (+1-202-407-8825).

[2] My curriculum vitae is here: https://josephhall.org/HallJosephResume.pdf.

1. Securing Elections is a Systems Problem

The events leading up to the 2016 election were a wake-up call for the entire elections community.[3] Nation-state adversaries that attacked electoral and campaign systems were proof that powerful adversaries sought to sabotage the very machinery of our democracy,[4] and that election officials must harden their defenses and prepare for inevitable future attacks.

After 2016, election administrators had to adapt to address cybersecurity threats from well-resourced nation-state attackers trained to scan and compromise election information systems. Security concerns around election technologies up to this point had focused on voting machines themselves – the machines used in polling places to cast votes. However, the lesson of the 2016 election attacks was that technology is now an integral part of the elections, campaign, and voting processes, such that any subsystem that connects to the elections systems is a target for malicious attacks. While certainly the security of vote-casting systems deserves ongoing attention, we must increasingly reinforce the security of the entire system that goes into running modern elections, across different functions like voter registration, vote-casting, vote tabulation, and election-night reporting. This involves different types of information systems such as voting machines, voter registration systems, electronic pollbooks, county and state information networks, and the back-office business networks used by election administrators, their staff, and volunteers.

In short, the election community learned from 2016 that election security is a *systems* problem and that the threats and risks involved are best dealt with by using systems-level solutions, such as designs and mitigations that can neutralize entire classes of attacks (e.g., multi-factor authentication).

For election administrators, their staff, and volunteers, this is a time of cultural change, where the security of the election system now equals the importance of other legal, logistical, and performance goals. Elections workers are now in the spotlight of international cybersecurity attention, and they’ve had to learn new tactics and strategies to reduce risks to and increase resiliency of election systems and processes.

2. Progress Since 2016 Has Been Encouraging

Compared to 2016, cyberattacks against elections interests in 2018 were relatively quiet, directed more towards campaign entities rather than election administrators. Three Congressional campaigns[5]

[3] United States Director of National Intelligence, “Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections,” (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

[4] National Academies of Sciences, Engineering, and Medicine. 2018. *Securing the Vote: Protecting American Democracy.* Washington, DC: The National Academies Press. https://doi.org/10.17226/25120; Lawrence Norden and Wilfred U. Codrington III, “America’s Voting Machines at Risk – An Update,” Brennan Center for Justice (Mar. 8, 2018), https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update.

[5] Olivia Beavers, “Primary season cyberattacks illuminate campaign vulnerabilities,” *The Hill* (Oct. 7, 2018), https://thehill.com/policy/cybersecurity/410229-primary-season-cyberattacks-illuminate-campaign-vulnerabilities.

were targeted with tactics from malicious keylogging software,[6] phishing attacks,[7] brute-force login attempts,[8] and denial-of-service (DoS) attacks.[9] In addition, a 2018 Senate campaign was unsuccessfully targeted by Russian attackers using the same methods that had been successful in 2016.[10] Finally, leading up to and after the 2018 election, there were incidents involving successful attacks on the email system of the National Republican Congressional Committee (NRCC) and a number of malicious websites mimicking the websites of political organizations.[11]

Despite these attacks on campaign-related entities, election administrators did not appear to be heavily targeted in 2018. The level of awareness about cybersecurity was high throughout the election community, and there were dozens of opportunities for stakeholders (election officials, journalists, and legislative staff) to attend briefings, trainings, and continuing cybersecurity education designed specifically for election officials.[12] Many of these efforts prioritized basic cybersecurity concepts that had been problematic in the 2016 elections. These included issues such as good password hygiene,[13] two-factor login (or two-step login),[14] and mitigation of distributed DoS attacks.[15] While in some cases this outreach has included hundreds of election officials at a time, given that there are more than 8,000 election jurisdictions around the country, these educational efforts will need to be sustained and adapted in time to new technologies and techniques.

Unfortunately, in addition to malicious attacks, errors and flaws in election operations remain a significant issue. In the 2018 general election there were serious breakdowns across all polling places in a small number of jurisdictions, most notably in New York City where jammed optical-scanning

[6] Keylogging software is malicious software that is designed to record and send everything a victim types into a keyboard.

[7] Phishing attacks involve spoofed email that convinces the victim to click on a link or email attachment to install malicious software or to disclose private information to an attacker.

[8] Brute-force login attempts involve an attacker quickly and repeatedly guessing many different combinations of usernames and passwords in order to gain unauthorized access to an information system.

[9] A denial-of-service (DoS) attack is any kind of attack that results in an service no longer functioning as it normally would, usually achieved by directing enormous amounts of network traffic to the victim computer causing it to have no capacity to respond to legitimate traffic. In a distributed denial-of-service (DDoS) attack, the increased traffic volume comes from a large distribution of sources, making the attack more difficult to stop.

[10] Associated Press, "Democratic Sen. Claire McCaskill confirms Russian hacking attempt," *Los Angeles Times* (Jul. 27, 2018), https://www.latimes.com/politics/la-na-pol-russia-hacking-mccaskill-20180727-story.html.

[11] "2019 Internet Security Threat Report, Volume 24," *Symantec* (February 2019), https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

[12] Efforts included those of the Belfer Center at Harvard Kennedy School, the Center for Internet Security (CIS), the National Council of State Legislatures (NCSL), the Center for Democracy & Technology (CDT), the Center for Technology & Civic Life (CTCL), the International Association of Government Officials (iGO) as well as US Government agencies such as the Department of Homeland Security (DHS) and the U.S. Election Assistance Commission (EAC).

[13] "Election Cybersecurity 101 Field Guide – Passwords," Center for Democracy & Technology (Aug. 29, 2018), https://cdt.org/insight/election-cybersecurity-101-field-guide-passwords/.

[14] "Election Cybersecurity 101 Field Guide – Two Factor Authentication," Center for Democracy & Technology (Aug. 3, 2018), https://cdt.org/insight/election-cybersecurity-101-field-guide-two-factor-authentication/.

[15] "Election Cybersecurity 101 Field Guide – DDoS Attack Mitigation," Center for Democracy & Technology (Nov. 2, 2018), https://cdt.org/insight/election-cybersecurity-101-field-guide-ddos-attack-mitigation/.

machines caused long lines[16] and in Johnson County, Indiana where failed connections to electronic pollbook databases stopped voting throughout the county for four hours (with no extension of polling hours).[17] Basic ballot design errors remain a serious problem, with a poor ballot design in one U.S. Senate race potentially disenfranchising tens of thousands of voters.[18] These kinds of errors are especially concerning as a clever adversary could attempt to make their attacks appear to be a result of error (and not from intentionally malicious activity). In order to best be able to detect and correct anomalous activity due to malicious attacks, it is important to minimize systemic or potentially outcome-changing flaws with election technology and processes.

3. Election Security Priorities Heading into 2020

CDT believes the following five areas must be policy priorities heading into 2020:

3.1. Prioritize the Replacement of Dangerously Outdated Voting Technologies;
3.2. Limit the Use of Paperless Voting Systems;
3.3. Promote Research, Development, and Implementation of Risk-Limiting Audits;
3.4. Commit to Long-Term Funding of U.S. Election Infrastructure; and,
3.5. Return the EAC Budget to Nominal Levels.

3.1. Prioritize the Replacement of Dangerously Outdated Voting Technologies

While states and local jurisdictions continue to make progress updating their outdated voting technologies with newer systems that keep an auditable voter verifiable paper record,[19] it is important to prioritize the continuing replacement of paperless direct-recording electronic (DRE) systems. DRE systems are not "software-independent" systems,[20] are unauditable, and as such unsuitable for government elections. There are good signs that many of the jurisdictions we worried the most about

[16] Ian MacDougall, "What Went Wrong at New York City Polling Places? It Was Something in the Air. Literally." *ProPublica Electionland* (Nov. 6, 2018), https://www.propublica.org/article/new-york-city-polling-places-midterms-2018-humidity.

[17] Voting System Technical Oversight Program, "A Preliminary Investigation of ES&S Electronic Poll Book Issues in Johnson County, Indiana for the 2018 General Election," Indiana Secretary of State (Dec. 31, 2018), https://www.in.gov/sos/elections/files/Report%20-%20Johnson%20County%20ePB%20Investigation%20Dec%2031%202018.pdf (Indiana VSTOP report).

[18] Dana Chisnell and Whitney Quesenbery, "How a badly designed ballot might have swayed the election in Florida," *Washington Post* (Nov. 12, 2018), https://www.washingtonpost.com/outlook/2018/11/12/how-badly-designed-ballot-might-have-swayed-election-florida/.

[19] Marc Levy, "Pennsylvania Senate moves to slow replacing voting machines," *Washington Post* (Apr. 30, 2019), https://www.washingtonpost.com/national/pennsylvania-senate-moves-to-delay-replacing-voting-machines/2019/04/30/b93c7f92-6b88-11e9-bbe7-1c798fb80536_story.html; Mark Niesse, "New Georgia voting machines win final vote in state House," (Mar. 14, 2019), https://www.ajc.com/news/state--regional-govt--politics/new-georgia-voting-machines-win-final-vote-state-house/twQCxrn1Cy9bFbLcUEwTlN/.

[20] "A voting system is software-independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome." Ronald L. Rivest and Madars Virza, "Software independence revisited," *Real-World Electronic Voting: Design, Analysis and Deployment*, CRC Press (2016), https://people.csail.mit.edu/rivest/pubs/RV16.pdf.

in 2016 and 2018 – notably, Pennsylvania and Georgia[21] – have committed to move to voting systems with an auditable paper record. However, until there is a federal mandate or a particularly attractive incentive tied to paper-based systems, there will continue to be jurisdictions that use completely electronic (paperless) systems with no auditable record, both because 1) some jurisdictions have already purchased paperless systems in the recent past and have no available resources to purchase new systems, and/or 2) these kinds of systems are unfortunately still available for sale.

3.2. Limit the Use of Paperless Voting Systems

As the state and local jurisdictions continue to modernize their election systems, it is important to also limit the potential risk of malicious attacks or changes to official ballot data through the use of remote vote-casting or ballot-marking systems that do not require a paper record be transmitted to an election official. These forms of paperless remote voting – often used for military and overseas voting, for voters with disabilities, and for voters in hard-to-reach rural areas – can include email, fax, and even internet voting, and must be kept to the minimum number of voters possible, in order to minimize the risks they may pose.[22] These systems 1) unacceptably increase the risk that votes may be changed on the client-side (due to malware on a voter's device), in transit (due to hostile network attackers), or on the server (compromised web or application server) and 2) unacceptably increase the risk that the information systems facilitating remote voting may themselves be subject to attack and potential compromise.[23]

3.3. Promote Research, Development, and Implementation of Risk-Limiting Audits

The secret ballot was a remarkable public policy invention at the turn of the 20th century, reducing the ability to buy votes and exercise undue influence, while paradoxically depressing voter turnout – voters could no longer get paid for their vote.[24] Put differently, the secret ballot was a technical and process development in election administration that resulted in a more trustworthy vote count.

The equivalent to the secret ballot for the 21st century is the risk-limiting post-election audit. Risk-limiting audits provide statistical assurance of the correctness of an electoral outcome by

[21] *Id.*, Levy and Niesse, fn. 19.

[22] From a network security perspective, remote ballot-marking systems should only store voted ballot data on the client-side of the communication, not the server-side (the marking interface or software should work without a network connection once activated or downloaded), to prevent transmission of voters' choices over the network; people should be required to send via postal mail or courier if at all possible, rather than transmit an electronic vote and potentially waive their ballot privacy if jurisdictions require ballot duplication for these kinds of remotely cast ballots.

[23] Election systems that must be available over the internet and web – e.g., voter registration systems, election night reporting systems – should be isolated in their own separate network segment (called a network demilitarized zone or network DMZ). This has proved effective at stopping common types of attacks, *see:* Nathaniel Herz, "Hackers broke partway into Alaska's election system in 2016. Officials say no damage was done." *Anchorage Daily News* (May 7, 2018), https://www.adn.com/politics/2018/05/07/hackers-broke-partway-into-alaskas-election-system-in-2016-officials-say-no-damage-was-done/.

[24] Jac C. Heckelman, "The effect of the secret ballot on voter turnout rates," *Public Choice* **82**:1-2, 107-124 (1995); Jac C. Heckelman, "Revisiting the relationship between secret ballots and turnout: A new test of two legal-institutional theories," *American Politics Quarterly* **28**:2, 194-215 (2000), http://users.wfu.edu/heckeljc/papers/published/APQ.pdf.

examining a randomly selected subset of ballots.[25] Alternatively, an official can conduct a full manual recount, which by definition is the correct result. A number of states now permit or require risk-limiting post-election audits,[26] and Congress should work to promote increasing experience, development and use of risk-limiting audits through incentives to States and localities in piloting these methods and sharing their experiences. With such a nascent field as risk-limiting post-election auditing, it is also important to encourage additional research and development of new methods and technologies.[27] In addition, incentives could be put to good use to encourage researchers to explore increasingly usable and modular end-to-end cryptographic or "open audit" voting technologies.[28]

3.4. Commit to Long-Term Funding of U.S. Election Infrastructure

There is a long-standing need for a long-term source of funding for elections infrastructure, which has only become more acute now due to increasing cybersecurity risks. Election systems and the systems that support them are critical infrastructure that require sustained and ongoing resources, support, and investment in order to harden their defenses. Funding for election security will help undergird infrastructure at the state and regional level as well as shore up our frontline defenses by ensuring dedicated funds for election security are available to local election officials.

Where funds were absorbed by activities at the state level, some local election officials did not directly benefit from the relatively modest $380 million in 2018 HAVA security funds.[29] With no indication of forthcoming money at the federal level, state-level election administrators may have decided that this money was best spent on state-level infrastructure. A regular cycle of directed election administration funds would allow for both state-level and local-level investment to help local election officials upgrade to more modern and secure information systems and practices.

3.5. Return the EAC Budget to Nominal Levels

The U.S. Election Assistance Commission (EAC) is in desperate need of a significant budget increase in order to meet the tremendous security needs of election officials. The EAC is a critical part of our national election infrastructure, providing a proven mechanism for distribution of modernization

[25] Mark Lindeman and Philip B, Stark, "A Gentle Introduction to Risk-limiting Audits," *IEEE Security & Privacy* **10**:5, 42-49 (2012), https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

[26] Including Colorado, Michigan, Rhode Island, and Virginia, *see:* Malachi Barrett, "'Risk-Limiting' Audits Could Provide Election Assurances," *Government Technology* (Dec. 5, 2019), https://www.govtech.com/security/Risk-Limiting-Audits-Could-Provide-Election-Assurances.html.

[27] For example, methods of *precinct-count* single-ballot ballot-comparison risk-limiting audits (ballot-comparison audits are currently only practical on central-count systems), which would allow the most statistical power by counting the smallest number of ballots per contest.

[28] Ben Adida, "Helios: Web-based Open-Audit Voting," *USENIX Security Symposium 2008* (2008), https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf.

[29] Ashley Lopez, "Local Officials Call Federal Election Funds 'A 10-Cent Solution To A $25 Problem'," *NPR News* (Aug. 4, 2018), https://www.npr.org/2018/08/04/634707340/local-officials-call-federal-election-funds-a-10-cent-solution-to-a-25-problem ; Blake Paterson and Ally J. Levine, "Fund Meant to Protect Elections May Be Too Little, Too Late," *ProPublica Electionland* (Aug. 21, 2018), https://www.propublica.org/article/fund-meant-to-protect-elections-may-be-too-little-too-late.

funding, oversight of the voting system testing and certification process, advice and training in election administration, and serving as the steward of the national voting system standards, the Voluntary Voting System Guidelines (VVSG). Approving an updated VVSG is a priority for the EAC[30] and supporting its implementation will be a major undertaking. The last time the EAC had a quorum of four sitting commissioners was in FY 2010 during which their budget was $16.5 million,[31] roughly double its current FY 2019 budget of $9.2 million.[32]

4. Compounded Risks from the Wider Ecosystem

In addition to what was well-known about election cybersecurity attacks in 2016 against voter registration databases and networks that hosted voter registration databases, the recent Mueller Report further implicates two additional types of targets: 1) a voting system services provider, and 2) at least one Florida county, which both had their networks compromised by officers of the Russian GRU (military intelligence).[33] Malicious software of some undisclosed type was installed by the attackers on their networks, allowing attackers to potentially change traffic in transit on the network or break into additional machines connected to the network.

These details are instructive in two ways: first, despite the election community's renewed focus on cybersecurity, other entities contracted to run pieces of elections – e.g., software developers, services vendors, logistics providers, hardware manufacturers, printers – may be compromised by an attacker seeking to influence the election or election operations, allowing a "stepping stone" attack where attackers compromise clients or vendors downstream of their ultimate target. Second, while election defenders rightly focus on hardening election officials' networks, those networks may be connected to other government networks – municipal, county, state – that may themselves be compromised.

The wider ecosystem of election officials' vendors and partners should adhere to generally-accepted cybersecurity practices, which might require a mixture of incentives and regulation. A key piece of a mature cybersecurity practice is a functional vulnerability handling process and associated vulnerability reporting mechanisms, ensuring that vulnerabilities can be properly fixed and establishing a public vulnerability reporting program. Election Systems & Software, Inc., a major election systems manufacturer, recently disclosed that it was working with Congressional staff on legislation to specify

[30] U.S. Election Assistance Commission, "Press Release: Eac Commissioners Unanimously Vote To Publish Vvsg 2.0 Principles And Guidelines For Public Comment," (Feb. 15, 2019) https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/.

[31] U.S. Election Assistance Commission, "Fiscal Year 2010 Congressional Budget Request," (May 7, 2009) https://www.eac.gov/assets/1/6/155.PDF.

[32] U.S. Election Assistance Commission, "Fiscal Year 2019 Congressional Budget Justification," (Feb. 12, 2018) https://www.eac.gov/assets/1/6/FY_2019_CBJ_Feb_12_2018_FINAL.pdf.

[33] Robert S. Mueller, III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election," United States Department of Justice (2018), https://www.justice.gov/storage/report.pdf; Matt Vasilogambros, "Mueller Findings Raise Election Hacking Fears in States," Pew Stateline (May 2, 2019), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2019/05/02/mueller-findings-raise-election-hacking-fears-in-states.

an industry-wide coordinated vulnerability disclosure program.[34] This is welcome and encouraging news, as standard vulnerability handling and reporting programs can help coordinate effective response to serious vulnerability discoveries.[35] These programs should also facilitate quicker response times after published third-party independent security analyses. These types of mechanisms are especially important with cutting-edge election systems that handle actual voted ballot data – such as blockchain-mediated remote vote-casting systems.[36]

We've also seen serious problems with electronic pollbooks – often in the form of tablet or laptop computers that serve to replace paper pollbooks used to check-in voters at the polling place. Electronic pollbooks can serve as chokepoints or single-points-of-failure in polling place processes – e.g., in 2018 where voting had to be stopped for four hours in one case[37] and in another case where lines were five hours long.[38] Electronic pollbooks have not in the past been considered formal parts of certified voting systems, but this clearly must change and Congress should consider whether to simply add them to the overarching definition of "voting system" or whether a separate, more modular type of election support-system certification could suffice to better vet these systems before wide use.

Attackers will not wait until Election Day to break-in and compromise or disrupt election systems. Government systems at all levels are particularly vulnerable to attack due to the likelihood they are composed of older hardware running outdated software. Attackers scan and infiltrate government information systems, often with months elapsing before their presence is detected. Adversaries intent on disrupting March 2020 primary elections are likely sending spear-phishing emails to election officials and infiltrating election systems this very moment.

5. High Hopes For Innovative Alternatives

As we consider the future of voting, the reality is that high barriers to entry stand in the way of new entrants into the voting technology market due to the requirements for federal and state certification and testing, the wide variety of requirements for elections around the country, and the halting availability and scant nature of election funding. CDT holds high hopes for emerging market-alternative solutions such as the LA County Voting Systems for All People (VSAP) system and new models for providing more modular technologies that build off of lessons learned in much more resourced sectors to provide high levels of confidentiality, integrity, and availability. In addition, we are very encouraged

[34] Greg Otto, "Election tech vendors say they're securing their systems. Does anyone believe them?" *Cyberscoop* (Apr. 24, 2019), https://www.cyberscoop.com/election-security-es-s-dhs-pen-testing-idaho-national-labs-procircular/.

[35] *See:* ISO, ISO/IEC Standard 29147:2014, "Information technology – Security techniques – Vulnerability disclosure," (2014), https://www.iso.org/standard/45170.html; ISO, ISO/IEC Standard 30111:2013, "Information technology – Security techniques – Vulnerability handling processes," (2013), https://www.iso.org/standard/53231.html.

[36] Maya Kosoff, "'A Horrifically Bad Idea': Smartphone Voting Is Coming, Just In Time For The Midterms," *Vanity Fair* (Aug. 7, 2018), https://www.vanityfair.com/news/2018/08/smartphone-voting-is-coming-just-in-time-for-midterms-voatz.

[37] *Id.*, Indiana VSTOP report, fn. 17.

[38] Jessica Huseman, Isaac Arnsdorf, and Jeremy B. Merrill, "Georgia Voters Face Hourslong Waits as State Scrambles to Accommodate Turnout," *ProPublica Electionland* (Nov. 6, 2018), https://www.propublica.org/article/georgia-voters-face-hours-long-waits-as-state-scrambles-to-accommodate-turnout.

by the response of the private sector, which we hope Congress would seek to further enable, from industry leaders and start-ups.

For six years, CDT has been part of an effort lead by the Los Angeles County Registrar, Recorder, and County-Clerk, Dean Logan, called the VSAP project.[39] The VSAP system was designed from scratch to put the voter at the center of the voter experience, and to produce a highly secure, completely open, publicly owned elections system.[40] By focusing on creating a voting system that in the future any jurisdiction can own, operate, and modify, this opens the market for system integrators who may not want to invest in creating an entire voting system, but who can service, support, and deliver highly secure, usable, and affordable elections once the basic building blocks are in place.

Moving to well-managed secure cloud software products – software-as-a-service – can increase system resilience and decrease administrative burdens by concentrating expertise across many users. Similarly, commercial-off-the-shelf (COTS) cybersecurity products and services can greatly enhance the capacity of election officials and campaigns at a fraction of the cost of customized solutions. Other examples include the nonprofit election systems vendor, Voting Works[41] – a project of CDT – which focuses on producing secure and affordable voting technologies composed of COTS hardware and software. Just this week, Microsoft and Galois announced Election Guard,[42] an end-to-end auditing layer that can be easily incorporated into existing voting systems.

The private sector has also risen to the challenge, providing enterprise-class products at cost or often for free, including distributed DoS protection from Cloudflare,[43] Akamai,[44] and Jigsaw[45] and secure password management software from 1Password.[46] CDT applauds this sense of corporate civic duty to protect democracy and would like to see an increasingly broad and deep set of reduced-cost commercial cybersecurity products and services available to election officials.

6. Conclusion

I would like to once again thank the Committee, Chairperson Lofgren, and Ranking Member Davis for the opportunity to speak to you, and please do not hesitate to follow up with any outstanding questions you may have.

Thank you.

[39] *See:* http://vsap.lavote.net/.
[40] Kevin Monahan and Cynthia McFadden, "Has Los Angeles County just reinvented voting?" *NBC News* (May 2, 2019), https://www.nbcnews.com/politics/2020-election/has-los-angeles-county-just-reinvented-voting-n1000761.
[41] *See:* https://voting.works/.
[42] *See:* https://news.microsoft.com/on-the-issues/topic/defending-democracy-program/.
[43] *See:* https://www.cloudflare.com/athenian/.
[44] *See:* https://content.akamai.com/us-en-PG11022-elections-protection-etp.html.
[45] *See:* https://protectyourelection.withgoogle.com/intl/en/.
[46] *See:* https://1password.com/for-democracy/.