May 7, 2020

Director Chris Krebs
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, DC 20528

Dear Director Krebs,

In this letter we, the undersigned computer and election security experts, offer strong concerns about the content of the document entitled "Electronic Ballot Delivery and Marking" published under your "COVID-19 and Elections" web page at

https://www.cisa.gov/publication/covid-19-election-resources.

As States grapple with the difficult task of holding elections during the novel coronavirus pandemic, we appreciate CISA's ability to provide guidance and recommendations on this subject. As the agency dedicated to helping secure our cyber infrastructure, CISA is uniquely suited to provide considered and valuable advice to election officials regarding electronic ballot delivery and marking. Regrettably, this particular document fails to address the most significant cyber security and privacy threats associated with electronic ballot delivery and especially electronic ballot marking, and neglects to provide recommendations and best practices to mitigate those risks. We recognize that as states expand and rely on vote by mail, it is essential to offer a remote accessible ballot marking option for disabled voters and therefore it is incumbent on CISA to acknowledge the risks that exist with these processes and offer practices to mitigate that risk.

We believe this document should be reconsidered, and the "Security Recommendations" section substantially revised.

We urge CISA to clarify that by far the most secure option for remote voting is for jurisdictions to mail pre-printed paper ballots to voters as is traditionally done for mail-in ballots. This allows the ballots to be hand-marked and to be mailed back in a condition suitable for immediate scanning without re-making the ballot. Jurisdictions should make every effort to ramp up their capability to bulk mail paper ballots to all voters, or to as many as allowed by law.

CISA should recommend that jurisdictions unable to mail pre-printed ballots to all voters should offer the capability of downloading a blank ballot through the Internet. Voters would then print the blank ballot on their own printers, mark their choices with a pen, and mail it back. Most voters should be advised not to mark the ballot electronically before printing, even if that capability is available in the software they are using. Only voters with a disability that makes it difficult to mark a ballot with a pen should advised to mark their choices by computer before printing it.

We have three primary concerns that we believe CISA should address:

1. Online ballot marking greatly amplifies the security threats of online ballot delivery and introduces significant risks to ballot secrecy. It should be discouraged except for voters with relevant disabilities.

2. Ballots delivered online are vulnerable to cybersecurity attacks. Unlimited/large scale online ballot delivery may enable the casting of fraudulent ballots if appropriate safeguards are not in place.
3. The back-end processing of electronically transmitted blank ballots involves a much greater workload and potential health risk for election workers compared to the processing of pre-printed absentee ballots. Large-scale adoption of electronically delivered ballots will both burden election offices and increase the risk of person-to-person contact among election workers during the novel coronavirus pandemic if proper sanitation and social distancing precautions are not taken.

We expand on these concerns below and provide suggested recommendations to mitigate these risks.

1. **Online ballot marking introduces serious security and privacy vulnerabilities.** Adding an additional "feature" to allow the voter to mark the ballot through the device's mouse or touchscreen and then print the *voted* ballot adds a host of additional security and privacy concerns. We urge CISA to advise election officials to make *printing the blank ballot* be the default action of any ballot download application, and to encourage all voters who do not have a disability to fill out the printed blank ballot by hand before mailing.

   Integrity threats of electronic ballot marking: If the voter's device is infected with malware, or the marking or printing app is simply buggy, it may record false votes on the printed ballot. Just as with a precinct-based ballot marking device (BMD) this leaves the voter with the error-prone task of carefully verifying that the printed ballot correctly reflects his or her intentions. CISA should recommend that voters with disabilities be strongly urged to perform this verification step.

   Threats to ballot secrecy on ballot marking systems. If the voter enters her vote choices into her computer or mobile device, the secrecy of the votes is at risk. Copies of the votes will still remain in the clear in the device's RAM and virtual memory unless the application has been carefully designed to zero that data before the app is closed. We urge CISA to advise election officials not to certify client applications unless they are verified to perform this zeroing. Images of the voted ballot will also remain as invisible temporary files in the device's file system and in the file system and memory of the printer or print server, at least until they are overwritten. A voting application has no direct way to overwrite these temp files, so the votes are available to any skilled person for a substantial time after voting is complete.

   Ballot marking on networked devices: Data sent to a networked printer is generally transmitted in the clear, so any other computer on the same network can monitor the network traffic and make a copy of the voted ballot being printed, compromising vote secrecy.

   A voter who uses a business-, institutional- or employer-owned device or network or printer may have no right of privacy. All three may be freely monitored without the voter's knowledge or consent. We ask that CISA advise jurisdictions to recommend that voters who must input their votes electronically should use their own personal devices, networks, and printers if possible, unless the voter is concerned about privacy in her home environment.

Ballot marking on Internet connected devices: If the device used for marking the ballot is connected to the Internet, vote secrecy can be violated in ways that are hard to prevent or detect. Malware can transmit the voted ballot along with the voter's ID to any third party. Some systems, such as the Maryland ballot distribution system (also adopted in New Mexico) and some commercially available systems are actually designed to routinely transmit voters' choices via the Internet back to a server as the ballot is marked in order to format the final voted ballot as a file for printing back on the voter's environment. The vote choices are stored as the voter marks her ballot in a file that is linked directly to the voter's identity when the server validates the voter's registration and ballot style. This type of system constitutes a wholesale vote privacy violation *by the state.* This concern was examined by NIST, which explicitly stated:

> *"To protect ballot secrecy, the printable ballot should be constructed using software that runs solely on voters' computers. At no point should the ballot marking application transmit voter selections to the Web-server."*[1]

We urge that CISA concur with NIST and explicitly warn against this practice and advise States against the use of systems with this architecture.

California, a state which has come to receive most of its ballots by mail, has already adopted legislation for remote accessible ballot marking that forbids systems that transmit vote selections over the Internet. It is important to note that it is possible to provide the same accessibility features for voters with disabilities with systems that adhere to this security and privacy best practice.

Any app that inputs vote choices should be designed to allow input of votes only when Internet connectivity has been turned off. More generally we urge CISA to make a clear recommendation that no voter should ever enter vote choices into any computer or device while it is connected to the Internet.

2. **Online blank ballot delivery is vulnerable to cyber attack**. Online transmission of *blank* ballots does not have the same risk profile as the online transmission of *voted* ballots but the cybersecurity threats to online blank ballots must be mitigated to the extent possible.

   Threats to the integrity of blank ballots delivered online. Transmitting a blank ballot to a voter for printing and hand-marking raises a number of standard cybersecurity concerns because the ballot server must be online continuously, exposing it to online attackers that could corrupt the ballot files sent to the voters. Offering unlimited or large-scale online ballot delivery will make electronically delivered ballots an attractive hacking target. Contests and/or candidates could be deleted, rearranged, or altered by a motivated hacker to corrupt an election contest. Some voters might notice that they did not receive the correct contests or candidates on their ballots, but there remains a serious risk that voters will not notice it. Even if a voter does notice an error, it may be difficult to alert election officials in a timely way so that the error can be corrected for all affected voters.

---

[1] NIST IR 7711, Regenscheid and Beier, "Security Considerations for Electronic Transmission of UOCAVA Election Materials," NIST IR 7711 https://www.nist.gov/itl/draft-nistir-7711-security-best-practices-electronic-transmission-uocava-election-materials

Online blank ballot delivery may provide opportunities to cast fraudulent ballots. By impersonating legitimate voters, online blank ballot delivery may be exploited by criminals or hackers anywhere in the world. Attackers could also intercept emails sent to voters that requested blank ballots and vote their absentee ballots. Verification of voters' signatures on submitted ballots (which has shortcomings) may be the only barrier to fraud, and not every state requires verification of the voters' signatures. Though some states require digital PII (partial social security number, date of birth, driver's license number, etc.) as credentials to request an absentee ballot, that information is typically easily available for tens of millions of voters as a result of many mass breaches of online databases in the past. This data would allow an attacker to impersonate voters and successfully request and cast fraudulent absentee ballots if there is no signature check on the mailed-in ballot envelope.

The U.S. Senate Intelligence Committee Report on Foreign Interference has warned that Russian agents have been collecting much of the information routinely used to validate a voter's absentee ballot request including voters' email addresses.[2] Bad actors can use voters' credentials to:

- Register eligible citizens that are not registered to vote, and then download and vote their absentee ballots.
- Request absentee ballots on behalf of registered voters and ask the ballot be delivered to an email address owned by the attacker.
- Print multiple copies of a ballot in order to cast fraudulent ballots. (This attack could be defeated by requiring signature verification for the submitted ballot but this practice is not universal. For example, Maryland has adopted online ballot delivery, but validates voters only at the ballot request stage. There is no voter authentication step when the ballot is received and counted.)

Many of these attacks could be partly or wholly, automated, making the attacks easier to scale and much more dangerous.

3. **The increased workload associated with electronically delivered ballots will burden election workers and require consideration of potential health risks.** Many ballot scanners cannot read ballots printed from voters' home printers because the paper weight is wrong, so the voter's selections must be laboriously hand-copied onto traditional paper ballot stock that can be read by a scanner. This is a time and resource-consuming process that may create a health risk for election workers who are typically directed to sit in pairs in order to prevent manipulation or fraud. Without transparent oversight and strict security protocols, this process introduces opportunities for error or tampering.

    - Even if ballots are remade by scanning a barcode printed on electronically marked ballots for disabled voters it is essential that the remade ballot be checked against the original, ideally by two election workers. When remaking ballots, jurisdictions should be advised to retain the original ballots and use them (rather than the remade ballots) for audits and recounts.

[2] Excerpts from an alleged leaked NSA document indicate that the hackers might have been exploring vulnerabilities associated with online delivery of absentee ballots. The top of the leaked document says: "*Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors…Research Absentee Ballot email addresses."*

For these reasons we urge CISA to recommend that states control the delivery of electronic ballots and limit electronic ballot delivery to: (a) voters who cannot be mailed a pre-printed blank ballot, (b) voters eligible by law to receive blank ballots electronically, and (c) voters with relevant disabilities.

Summary: For all of these reasons we urge CISA to explain vulnerabilities of electronic ballot marking in its guidance documents and consider these recommendations:

- Place limits on electronic ballot delivery, provided only to those who are cannot be mailed a pre-printed blank ballot, who are required to have electronic delivery available by law, or who have relevant disabilities.
- Advise States to consider electronically delivered ballots to be at risk of unauthorized duplication, warranting authentication of the voter's identity and eligibility.
- Urge election officials to make *printing the blank ballot* be the default action of any ballot download application, and to encourage all voters who are able to do so to fill out the printed blank ballot with a pen before mailing.
- Advise States to adopt remote accessible ballot marking systems that confine vote selection data to the voter's infrastructure, in compliance with recommendations by the National Institute of Standards and Technology (NIST) and Center for Civic Design.
- Advise officials that voters who must input their votes electronically should prefer to use their own personal devices, networks, and printers, if possible, rather than an employer's or institution's infrastructure, unless they are concerned about privacy at home.
- Advise election officials not to certify ballot marking applications unless they are verified to zero out vote choices from all memory.
- Encourage election officials to instruct voters who do mark their ballots with a computer or device application to carefully verify that their vote choices where recorded correctly.
- Encourage election administrators, if they choose to use the barcode or QR code feature on a ballot marking application, to instruct election workers remaking the ballots to carefully check each ballot and ensure the remade ballot matches the human-readable selections on the original ballot.
- Advise jurisdictions to retain the original ballots and use the human readable part (rather than the remade ballots, barcodes, or QR codes) for audits and recounts.
- Explicitly warn States against the use of online ballot marking systems that transmit vote selections over the Internet in agreement with NIST's recommendations, and advise them to only adopt systems that permit a voter to mark a ballot accessibly from software that keeps vote data local to her computer and printer.
- Recommend clearly that no voter should ever enter vote choices into any device while it is connected to the Internet.

We strongly urge CISA to consider these recommendations and hope they are useful. We welcome your questions and any opportunities to support your work in this area. Please don't hesitate to contact us if there is any way we may be helpful.

Sincerely,

Free Speech For People
Amherst. Massachusetts

Center for Scientific Evidence in Public Issues
American Association for the Advancement of Science
Washington, DC

Susan Greenhalgh
Senior Advisor on Election Security
Free Speech For People

Dr. Michael D. Fernandez
Founding Director
Center for Scientific Evidence in Public Issues
American Association for the Advancement of Science

Dr. Andrew W. Appel
Eugene Higgins Professor of Computer Science Princeton University

Harvie Branscomb
ElectionQuality.com

Dr. Duncan Buell
NCR Chair and Professor, Computer Science and Engineering
College of Engineering and Computing
University of South Carolina

Dr. L. Jean Camp
Director of Center for Security and Privacy in Informatics, Computing, and Engineering
Professor of Informatics
Adjunct Professor of Computer Science
Adjunct Professor of Telecommunications
Indiana University

Dr. Richard A. DeMillo
Charlotte B. and Roger C. Warren Professor of Computer Science
College of Computing
Georgia Institute of Technology

Dr. J. Alex Halderman
Professor, Computer Science and Engineering
Director, Center for Computer Security and Society
University of Michigan

Dr. David Jefferson
Lawrence Livermore Laboratories

Dr. Douglas W. Jones
Associate Professor
University of Iowa Department of Computer Science
Former chair, Iowa Board of Examiners for Voting Machines and Electronic Voting Systems

Dr. Joseph Kiniry
Principal Scientist
Galois

Dr. Jeanna Neefe Matthew
Associate Professor of Computer Science
Clarkson University

Dr. Peter G. Neumann
Chief Scientist

Mark Ritchie
Former MN Secretary of State

SRI International Computer Science Lab

Member of the EAC Board of Advisors
Former president of the National Association of Secretaries of State

Kevin Skoglund
Chief Technologist
Citizens for Better Elections

Dr. Philip B. Stark
Professor, Associate Dean of Mathematical and Physical Sciences
Department of Statistics
University of California at Berkeley

Dr. Poorvi L. Vora
Professor of Computer Science
The George Washington University

Luther Weeks
Executive Director
CTVotersCount.org

Dr. Daniel M. Zimmerman
Principal Researcher, Galois
Principled Computer Scientist, Free & Fair

*Affiliations of the undersigned are for identification purposes only they do not imply institutional endorsement.

cc. House Homeland Security Committee

Senate Committee on Homeland Security