December 12, 2022

The Honorable Merrick Garland
Special Counsel Jack Smith
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530-0001

The Honorable Christopher Wray
Assistant Director Robert Wells
Federal Bureau of Investigation
935 Pennsylvania Avenue
Washington, D.C. 20530-0001

The Honorable Jen Easterly
Director
Cybersecurity & Infrastructure Security Agency (CISA)
Department of Homeland Security
Washington, DC 20023

Dear Attorney General Garland, Special Counsel Smith, Director Wray, Assistant Director Wells, and Director Easterly,

Elections form the foundation for the legitimacy of government in the United States. Protecting the security of our elections constitutes a top national security priority, and we appreciate the work the Department of Justice and the Department of Homeland Security have done to address threats to election security.

We[1] are writing to you to call attention to significant multi-state events impacting ongoing election security which were first revealed in discovery in a civil lawsuit by a non-governmental plaintiff.[2] Because these events were revealed

[1] Free Speech For People is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions, secure, transparent, trustworthy and accessible voting systems for all voters. We are not parties or counsel in the civil litigation referenced in this letter. The coalition of signatories includes renowned computer security experts and election experts.
[2] Emma Brown, Jon Swaine, "Inside the secretive efforts by Trump allies to access voting machines," *The Washington Post*, October 28, 2022. Available at: https://www.washingtonpost.com/investigations/2022/10/28/coffee-county-georgia-voting-trump/

in a private lawsuit rather than through a law enforcement investigation, the significance and consequences may not have registered with the relevant federal agencies. Specifically, we are writing regarding the multi-state plan, directed and funded by attorneys for Donald Trump—including Sidney Powell, Lin Wood, and Jesse Binnall—to access voting systems and obtain and distribute copies of voting system software unlawfully,[3] which could potentially constitute federal crimes and be relevant to investigations into efforts to overturn the 2020 presidential election.

The same software is used in voting systems across the U.S. Its misappropriation and distribution pose serious risks to the credibility and trustworthiness of election results. The matter urgently requires your agencies' attention. This alarming development was not addressed in the Public Service Announcement (PSA), published by CISA on October 4, 2022.[4] On October 28, 2022, news reports confirmed that the Department of Homeland Security, the Federal Bureau of Investigation, the U.S. Capitol Police, and the National Counterterrorism Center released a joint intelligence assessment warning that violent domestic extremists pose a heightened threat to the security of the 2022 mid-term elections.[5] Federal security agencies are rightly concerned about potential attacks on elections. But because the unauthorized access and copying of election system software was uncovered by private action, it appears that the consequences of those activities —orchestrated by individuals associated with domestic extremists—have not been factored into these risk assessments. We write to highlight this important information for your agencies to integrate it into threat assessments, criminal investigations, and risk mitigations.

1. Executive Summary

According to evidence obtained in a civil lawsuit, attorneys and allied advisors for Donald Trump directed and funded a plot that included copying voting system software from multiple jurisdictions in multiple states. The operatives successfully obtained software from both Dominion Voting Systems and Election Systems &

[3] Jon Swain, Aaron C. Davis, Amy Gardner, Emma Brown, "Files copied from voting systems were shared with Trump supporters, election deniers," *The Washington Post*, August 22, 2022. Available at: https://www.washingtonpost.com/investigations/2022/08/22/election-system-copied-files-trump/
[4] Available at: https://www.ic3.gov/Media/PDF/Y2022/PSA221004.pdf
[5] Geneva Sands, Sean Lyngass, "Feds warn that domestic violent extremists pose heightened threat to midterm elections," *CNN,* October 28, 2022. Available at: https://www.cnn.com/2022/10/28/politics/midterm-domestic-extremist-threat/index.html

Software (ES&S).[6] Together, ES&S and Dominion equipment and software count more than 70% of the votes in the U.S.[7]

Now that the Dominion and ES&S software has been accessed and distributed by individuals without authorization, the election system software is considered to be "in the wild," available to an unknown number of people and organizations that could use the software to undermine, disrupt, or tamper with elections in a number of ways.[8]

Access to the software enables bad actors to install the software on their own hardware to create their own exact replicas of voting systems, probe them, and develop exploits. They can decompile the software to get the source code, study it for vulnerabilities, and develop malware tailored to the system. Such malware can be loaded onto systems by a poll worker, maintenance worker, or even a voter: little physical access is needed.[9] Nor is Internet access needed. Bad actors could use the software to develop ways to cause the system to malfunction to prevent voters from voting or to manipulate the vote count.

Moreover, access to this software may also be used in service of disinformation campaigns to cast doubt on legitimate election results. Perhaps the most easily executed attack would be to simply use the software as the basis of fabricated evidence of election manipulation to delegitimize the results and destabilize our government.[10]

---

[6] Emma Brown, Jon Swaine, Aaron C. Davis, Amy Gardner, "Trump-allied lawyers pursued voting machine data in multiple states, records reveal," *The Washington Post*, August 15, 2022. Available at: https://www.washingtonpost.com/investigations/2022/08/15/sidney-powell-coffee-county-sullivan-strickler/

[7] https://verifiedvoting.org/verifier/#mode/navigate/map/makeEquip/mapType/normal/year/2022

[8] The threats to election security posed by the unauthorized distribution of voting system software are described in detail in the July 14, 2022 statement from the OSET Institute "Increasing Concerns About Amplified Threats To Voting Systems," available at: https://trustthevote.org/wp-content/uploads/2022/07/14July22_StatementOnPublicDisclosures.pdf.

[9] University of Michigan Professor J. Alex Halderman, one the nation's foremost experts on election system security, examined the Dominion Voting System ballot marking device for the Curling lawsuit and documented multiple security vulnerabilities that could be exploited. Though his detailed report remains sealed by the Court, Prof. Halderman submitted a public declaration recounting a high level summary of his findings, which includes this statement, "*Attackers could exploit these flaws to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems."* No. 17-cv-02989-AT (N.D. Ga. filed Aug. 8, 2017). Document 1304-3

[10] We have already seen this play out. Matt DePerno, a former candidate to be Michigan's Attorney General and prominent figure in denying the results of the 2020 election, used access to voting system software to support allegations of election fraud. *See*: "Michigan Candidate Matt DePerno Boasts of Effort Showing How to Stuff Ballots," *Deadline Detroit*, September 3, 2022. Available at:

Insider attacks by temporary election workers are an increasing threat to election security. A statement issued by the Bipartisan Policy Center warned: "There is mounting concern that temporary election workers recruited and trained by organizations with nefarious intent may undermine security and trust in the election process."[11] Since organizations with likely nefarious intent also now possess copies of voting system software, this creates a profound threat scenario.

Though some of the impacted states are reportedly pursuing individual criminal investigations,[12] the coordinated, multi-state plan by Powell indicates there could be potential federal criminal liability that compels intervention by the Department of Justice.

Furthermore, we ask that the Department of Justice's National Security Division and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) urgently assess the increased threats to election security posed by the unauthorized distribution of voting system software to individuals who have already spread misinformation and may attempt to disrupt elections, and factor these threats into activities to protect elections.

Because the multistate plan was not discovered by local or state law enforcement (which presumably would have shared such findings with the Department of Justice through normal channels) but by the private civil litigation *Curling v. Raffensperger*, we are writing (1) to urge the Department of Justice and the Department's Special Counsel to investigate this coordinated plot to copy election system software from multiple states; and (2) to urge the Department of Justice's Counterterrorism Division and the Department of Homeland Security's CISA to assess the ongoing threats introduced by the distribution of voting system software, and calibrate efforts to protect elections to include those risks.

---

https://www.deadlinedetroit.com/articles/31208/michigan_candidate_matt_deperno_boasts_of_effort_showing_how_to_stuff_ballots

[11] Grace Gordon, Rachel Orey, "Closing Gaps in Poll Worker Policy," The Bipartisan Policy Center, October 3, 2022. Available at: https://bipartisanpolicy.org/explainer/poll-worker-policy/

[12] Nathan Layne, "Republican clerk could be charged in Michigan voting-system breach," *Reuters,* October 4, 2022. Available at: https://www.reuters.com/legal/exclusive-michigan-police-ask-prosecutors-consider-charging-republican-clerk-2022-10-04/

2. Background

In 2017, a public interest organization and individual voters filed a lawsuit in federal court in Georgia challenging the use of the state's voting equipment, *Curling v. Raffensperger*.[13] The case, now in its second phase, is being heard by the Honorable Amy Totenberg in the Northern District of Georgia. (*Curling v. Raffensperger* does not allege any election has been incorrectly decided.) In the course of discovery, plaintiffs obtained evidence that certain individuals had accessed voting equipment in Coffee County, Georgia, and copied all election data and the software that records, counts, and reports votes.[14] This software is used in all of Georgia's 159 counties, making this a breach of the entire state's software and system. (Similar versions of the software are used in other jurisdictions, including Riverside, California, and Washington County, Pennsylvania.) Plaintiffs sought additional discovery to ascertain what had happened in Coffee County.[15]

Through evidence obtained in discovery, the plaintiffs have established that the data management firm SullivanStrickler was engaged by Sidney Powell to go to the Coffee County, Georgia, elections office and image all Dominion voting system equipment and devices.[16] Cathy Latham, an influential Georgia Republican Party official, and an "alternate elector," represented by Sidney Powell and Lin Wood in then-pending litigation to overturn the 2020 election, was a key local Coffee County organizer of the software collection effort. The plaintiffs in Curling also obtained surveillance camera video that shows several individuals, including Doug Logan of the Cyber Ninjas, visiting the Coffee County election office over the course of several days for extensive equipment access.[17] Plaintiffs also obtained copies of SullivanStrickler's voting system equipment forensic images and system

[13] No. 17-cv-02989-AT (N.D. Ga. filed Aug. 8, 2017). Affidavits and depositions referred to herein are available at this docket.
[14] Jose Pagliery, "Texts Reveal GOP Mission to Breach Voting Machine in Georgia," *The Daily Beast,* June 5, 2022. Available at: https://www.thedailybeast.com/how-a-coffee-county-gop-chair-coordinated-a-voting-machine-breach
[15] Jose Pagliery, "Subpoenas Probe GOP Mission to Breach Georgia Voting System," *The Daily Beast,* June 15, 2022. Available at: https://www.thedailybeast.com/subpoenas-probe-gop-mission-to-breach-georgia-voting-system
[16] Mark Niesse, "Georgia election data copied under direction of Trump attorney," *The Atlanta Journal Constitution,* August 16, 2022. Available at: https://www.ajc.com/politics/georgia-election-data-copied-under-direction-of-trump-attorney/XCPM33PXC5ABJN6UXG645EXLM4/
[17] Kate Brumback, "Video fills in details on alleged Ga. election system breach," *The Associated Press,* September 6, 2022. Available at: https://apnews.com/article/2022-midterm-elections-technology-donald-trump-voting-92c0ace71d7bee6151dd33938688371e

logs.[18] These show that the forensic images (containing the system software) have been uploaded over the Internet to an online ShareFile site and downloaded multiple times by other parties, including Conan Hayes. Hayes is implicated in the copying of voting system software in Mesa County, Colorado, and in the copying and unauthorized distribution of Antrim County, Michigan, software.[19]

Because credentials were shared and because the downloaded software may have been copied and shared, it is not possible to know how many people in the United States or abroad currently possess the Dominion Voting System software taken from Coffee County and used in hundreds[20] of other U.S. jurisdictions.

The *Curling* plaintiffs have amassed emails, contracts and other documentation that show SullivanStrickler was hired and paid by Sidney Powell to copy and distribute the software. The contracts show that Powell hired SullivanStrickler to access and copy voting system software in Georgia, Michigan, and Nevada, making this a multi-state enterprise.[21]

3. <u>The Georgia state election officials' response has been inadequate, and doesn't reflect the severity of the breach, slowing state and federal law enforcement responses.</u>

Evidence that the security of the voting system in Georgia may have been compromised first surfaced in December of 2020, when the Coffee County Election Director, Misty Hampton, posted a video to YouTube critical of the voting system.[22] In the video, which went viral, the password for the election management server is visible on a post-it note on Hampton's computer. According to testimony from the Secretary of State's office, the office opened an investigation

---

[18] *See* ECF No. 1518-1, available at https://storage.courtlistener.com/recap/gov.uscourts.gand.240678/gov.uscourts.gand.240678.1518.1.pdf; ECF No. 1518-2, available at https://storage.courtlistener.com/recap/gov.uscourts.gand.240678/gov.uscourts.gand.240678.1518.2.pdf.

[19] *See supra* note 3.

[20] https://verifiedvoting.org/verifier/#mode/search/year/2022/equipment/Ballot%20Marking%20Device/make/Dominion%20Voting%20Systems/model/ImageCast%20X%20BMD

[21] Emma Brown, Jon Swaine, Aaron C. Davis, Amy Gardner, "Trump-allied lawyers pursued voting machine data in multiple states, records reveal," *The Washington Post*, August 15, 2022. Available at: https://www.washingtonpost.com/investigations/2022/08/15/sidney-powell-coffee-county-sullivan-strickler/

[22] Doug Richards, "Coffee County attention started with YouTube video," *11Alive*, September 29, 2022.Available at: https://www.11alive.com/article/news/politics/elections/coffee-county-youtube-election-dominion-vote/85-14b18082-6f80-4657-8e37-b27e0d892735

into the video and the posting of the password.[23] While the Secretary's investigators ultimately recommended penalties for failure to secure the doors to the election server room,[24] they apparently made no effort to review available video surveillance records to determine whether the server or server room security had been breached.[25] In fact, on January 26, 2021, the investigator charged with the investigation of the posted password and video happened upon one of the Cyber Ninja's colleagues, Jeffrey Lenberg, in Ms. Hampton's office with voting equipment made available to Lenberg for unauthorized access and testing.[26] There is no evidence that appropriate inquiry or further investigation ensued.

Misty Hampton resigned to avoid termination in February 2021.[27]

In May 2021, her successor, James Barnes, wrote the Secretary of State's office because he was alarmed to find a business card from Doug Logan of Cyber Ninjas under the election director's computer.[28] Staff in the Secretary's office forwarded the message to the Secretary's chief investigator, asking her to investigate. According to an email produced in discovery, the Secretary's office planned to initiate an investigation to determine whether Cyber Ninjas had accessed the equipment.[29] The investigator acknowledged the email but, according to Barnes, no state investigation ensued.[30]

Weeks later, Barnes needed to access the election management server, but found that the password he had been given did not work. He reported this to the Secretary's office. Technicians made a limited troubleshooting effort but were unable to access the server.[31] They replaced the server and central scanner workstation on June 8, 2021.[32] This incident, which suggested that someone had improperly changed the password, did not trigger any investigation into

---

[23] Germany Aff.¶ 7 Document 1444-1 filed August 8, 2022.
[24] See State Election Board Transcripts for 2021, available at: https://sos.ga.gov/sites/default/files/2022-02/2021_seb.pdf
[25] Georgia Secretary of State Investigation Summary, September 28, 2021, available at: https://www.dropbox.com/s/7jj34weu5pwy0a6/SEB%20investigation%2020-250.pdf?dl=0
[26] "Georgia video, testimony at odds," *Northwest Arkansas Democrat Gazette*, September 21, 2022. Available at: https://www.nwaonline.com/news/2022/sep/21/georgia-video-testimony-at-odds/
[27] "Coffee Co. elections supervisor named in investigation resigns," *WALB News,* March 31, 2021. Available at: https://www.walb.com/2021/03/31/coffee-co-elections-supervisor-named-investigation-resigns/
[28] Barnes Dep. Page 55. Document 1440-1 filed July 29, 2022.
[29] Available at: SOS investigation Doug Logan. .pdf - Dropbox
[30] Barnes Dep. Pages 160-168 Document 1440-1 filed July 29, 2022.
[31] Barnes Dep. Pages 106-110 Document 1440-1 filed July 29, 2022.
[32] Document 1377 and 1377-4.

unsanctioned voting system and software access in Coffee County. After taking possession of the potentially compromised server, the Secretary's office did not make meaningful efforts to access the contents of the server, nor did it examine the system forensically to determine whether there had been unauthorized access as Mr. Barnes had feared when he alerted the Secretary's office in May 2021.

In late February 2022, the plaintiffs shared with the Secretary's staff an audio recording of a call from an individual associated with the Trump campaign who was one of the organizers of the breach in Coffee County.[33] But in the following months, there was still no indication that the Secretary was investigating the allegations. On April 7, 2022, the Secretary of State's office represented to the court that it opened an investigation immediately after it received a recording of the phone call on March 2, 2022.[34] But records show the investigation was not actually opened until April 25, 2022—18 days *after* telling the court that the investigation had been opened.[35]

Public statements from the Secretary's office suggest that for many months it failed to investigate the evidence of improper access to voting systems. In April 2022, Secretary Raffensperger claimed his office was investigating but found no evidence a breach had occurred.[36] That same month, at an event at the Carter Center, the Interim Georgia Deputy Secretary of State Gabriel Sterling summarily dismissed concerns of a breach in Coffee County, stating emphatically that the breach "did not happen."[37]

While an investigation may have been "opened" on paper in late April 2022 by the Secretary and the State Election Board, their investigators made no efforts to interview Coffee County officials or potential witnesses, or request documents, obtain missing emails, or video surveillance records from Coffee County.[38] Nor was there a meaningful effort to forensically examine the seized server, now known to contain evidence of the January 7, 2021, breach.

---

[33] See *supra* note 2.
[34] April 7, 2022 hearing transcript, available at: http://freespeechforpeople.org/wp-content/uploads/2022/11/court-transcript-4.7.22.pdf
[35] Germany Aff.¶ 26, Document 1444-1 filed August 8, 2022.
[36] *See supra* note 21.
[37] Restoring Confidence in American Elections | Panel 3 (April 29, 2022) - YouTube at 35:30
[38] Barnes Dep. Pages 160-161 Document 1440-1 filed July 29, 2022

Only in August 2022, months after the breach was publicly reported, did the Secretary—at the direction of the State Election Board Chair[39] —bring in the Georgia Bureau of Investigation, which opened an investigation.[40]

Thus, despite numerous concerning incidents, there is no indication Georgia state authorities did anything to investigate the statewide system breach until more than a year had passed. Sorting out the facts around the Coffee County incident and the Secretary's slow response has been further complicated by conflicting statements provided by the Secretary to the press and courts.[41] The Secretary's delay in alerting Georgia law enforcement to this issue delayed Georgia authorities' sharing information with the U.S. Department of Justice, Georgia Fusion Centers, and CISA—including the fact that this was a coordinated, multi-state plan orchestrated and funded by Donald Trump's campaign attorneys.

4. <u>Failure of the Georgia Secretary of State to respond to the security threats appropriately may also undermine a federal response to protect elections.</u>

In public statements, the Georgia Secretary of State and his representatives have downplayed ongoing and escalating security threats stemming from the breach, claiming that the breach was sufficiently addressed by the removal of Misty Hampton and the replacement of the election server in 2021.[42] The Secretary's office has even dismissed concerns that the copying and distribution of the software poses ongoing risks as "fear-mongering."[43]

The inadequacy of the state's response to this breach is clear in sworn testimony by Georgia's own Chief Information Officer (CIO), Merritt Beaver.[44] In a deposition taken before the incident in Coffee County was confirmed, the CIO was asked hypothetically, "Can you explain what are the reasons that election

[39] Retired federal judge, The Honorable William S. Duffey, Jr., serves as the Chair of Georgia's State Election Board.
[40] See *supra* note 3.
[41] "Questions raised in timeline of state response to Coffee County breach," *11Alive*, September 26, 2022. Available at: https://www.11alive.com/article/news/politics/coffee-county-breach-timeline-georgia-secretary-of-state-brad-raffensperger-response/85-f3d75b6f-6ba8-445b-88d6-7fda894358be
[42] Gabriel Sterling on CNN's "Out Front with Erin Burnett," CNN Transcripts, September 7, 2022. Available at: https://transcripts.cnn.com/show/ebo/date/2022-09-07/segment/01
[43] https://twitter.com/GabrielSterling/status/1576298738892836864
[44] Mark Neisse, "Georgia election security chief splits time with second state job," *Atlanta Journal Constitution*, August 5, 2022. Available at: https://www.ajc.com/politics/georgia-election-security-chief-splits-time-with-second-state-job/SNR3WHSJIFB6RDAI3L6M7A43RE/

software is not released to the public?" He responded, "It's pretty obvious. You don't expose your—basically your system to the public because they—basically you're giving them a road map to how to basically get in and access the system."[45] But the Secretary's office has denied the unauthorized copying of the software poses any "long-term security threats,"[46] and has not adopted additional safeguards to protect future elections.

We raise these facts not to embarrass the Secretary's office, but because they provide important context for federal agencies to respond efficiently and effectively. The failure of Georgia's state election officials to investigate the events in Coffee County promptly, and the refusal of the Secretary to mitigate the danger to the entire statewide system demonstrate two things: 1) the Secretary's office remains poorly informed about the events in Coffee County, and therefore the Department of Justice and the Department of Homeland Security should seek information from other sources, including from the plaintiffs and their attorneys in *Curling*; and 2) federal guidance is urgently needed to address the security risks posed by the unlawful access to and distribution of voting systems by entities that have demonstrated intentions to disrupt and destabilize U.S. elections *going forward*.

5. <u>The Georgia system compromise is far more expansive and poses greater election security threats than the better understood serious breaches in other states.</u>

Before the revelations of the breach of Georgia's statewide system, county-level voting system breaches had been documented in multiple states including Michigan, Colorado, and Pennsylvania.[47] These serious security compromises are less threatening than the Georgia statewide breach, for multiple reasons:

[45] Beaver Dep. Document 1368-3 Page 157-158.
[46] Mark Niesse, "Video shows fake elector aided copying of Georgia election data," *The Atlanta Journal Constitution,* September 6, 2022. Available at: https://www.ajc.com/politics/video-shows-fake-trump-elector-aided-copying-of-georgia-election-data/NQM2F4KKMNGKRBHEAUSH6ALTGU/
[47] Alexandra Ulmer and Nathan Layne, "Trump allies breach U.S. voting systems in search of 2020 fraud 'evidence,'" *Reuters,* April 28, 2022. Available at: https://www.reuters.com/investigates/special-report/usa-election-breaches/

1) Unlike other states, Georgia uses the same software in each county: *every* Georgia county's software was taken. The other states use multiple vendors and software versions, so a breach in any one county is not a statewide breach.

2) Unlike Michigan, Colorado, and Pennsylvania, the programming and configuration of the machines is coordinated at the state level, creating a "single point of failure" for an attacker who may want to attack multiple counties or polling locations.

3) Georgia is the only state using touchscreen Ballot-Marking Devices ("BMDs") as the primary voting system for in-person voting. The paper trail produced by BMDs is inherently untrustworthy: it is a record of what the BMD did, not what the voters did. In contrast, the other states primarily use hand-marked paper ballots, which makes it possible for audits and recounts to detect and correct wrong outcomes. Georgia's voting system does not support such auditing or error detection.[48]

4) Georgia's breach, unlike the others mentioned, encompassed the Election Management Server, scanners, touchscreen BMDs, electronic pollbooks, and all system components. Other states' breaches generally obtained access to fewer voting-system components.

Another difference between the incidents in other states and in Coffee County, Georgia, is that everywhere else, the chief state election officials promptly engaged law enforcement, exercised their authority to contain the fallout, and made public the risk, enforcement measures, and mitigation efforts. State authorities investigated and enforced their laws and the cases were regarded as isolated. At the time, there was no public evidence that the breaches were connected—but now there is.

[48] Andrew Appel, Rich DeMillo, Philip Stark, "Ballot Marking Devices (BMDs) Cannot Ensure the Will of the Voters," December 27, 2019. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755

6. Conclusion

One of the most significant revelations uncovered by the plaintiffs in *Curling v. Raffensperger* is that the Coffee County breach was just one element of a coordinated plan to access and copy voting system software from multiple states, multiple jurisdictions, and different voting system vendors,[49] by lawyers acting on behalf of the Trump campaign, possibly constituting federal crimes. Because this plot was orchestrated by individuals currently under investigation for their attempts to overturn the 2020 presidential election, it is possible that the coordinated effort to obtain voting system software was also part of an ongoing conspiracy to overturn elections. This calls for a vigorous and swift investigation by the Department of Justice, the Special Counsel, and the Federal Bureau of Investigation. Because the Georgia Secretary of State and State Election Board failed to investigate in a serious or timely manner, and to ensure that you get the most complete and accurate information regarding the Georgia breach, we urge you to seek information from the plaintiffs in *Curling*.

In addition, the Department of Homeland Security and Department of Justice's Division of Counterterrorism should immediately assess how the release of the software may affect the security of future elections and recommend security mitigations. Potential avenues of attack could include fabricating false evidence for disinformation campaigns, disrupting elections to prevent voting or cast doubt on the integrity of the process, or even altering the results. Your agencies' awareness, monitoring, and readiness for action is needed, since exploits may occur with little warning.

We thank you very much for your consideration and stand ready to assist in any way we can.

Sincerely,

Susan Greenhalgh
Senior Advisor for Election Security
Free Speech For People
Susan@FreeSpeechForPeople.org

Ron Fein
Legal Director
Free Speech For People
RFein@FreeSpeechForPeople.org

[49] See *supra* note 2.

Elizabeth Bradley Ph.D.
Professor
University of Colorado Boulder*

Duncan Buell Ph.D.
Chair Emeritus — NCR Chair in Computer Science and Engineering
Dept. of Computer Science and Engineering
University of South Carolina*

Lowell Finley
former Deputy Secretary of State
California

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

Harri Hursti
Founding Partner Nordic Innovation Labs
Election Integrity Foundation*

David Jefferson Ph.D.
Lawrence Livermore National Laboratory* (retired)
Election Integrity Foundation*

Douglas W. Jones Ph.D.
Emeritus Associate Professor of Computer Science, University of Iowa*

Daniel P. Lopresti Ph.D.
Professor, Department of Computer Science and Engineering*
Chair, Computing Research Association's Computing Community Consortium (CCC)*
Past-President, International Association for Pattern Recognition (IAPR)*
Lehigh University

Peter G. Neumann Ph.D.
Chief Scientist,
SRI International Computer Science Lab*

Mark Ritchie
Former MN Secretary of State
Member of the EAC Board of Advisors*
Former president of the National Association of Secretaries of State*

Philip B. Stark Ph.D.
Distinguished Professor
Department of Statistics
University of California, Berkeley*

John E. Savage Ph.D.
An Wang Professor Emeritus of
Computer Science
Brown University*

Penny M. Venetis
Director, International Human Rights
Clinic*
Distinguished Clinical Professor of
Law*
Judge Dickinson R. Debevoise
Scholar*
Center for Law and Justice
Newark, NJ

*Affiliations are listed for identification purposes only and do not imply institutional endorsement.