BRENNAN CENTER FOR JUSTICE

August 11, 2022

To the Executive Committees of US State Associations of Election Officials:

Insider threats are not a new phenomenon, nor are they unique to election security,[1] but the current participation of election deniers in the election process, and active recruitment of more, has sparked an increase in breaches of the physical security of election equipment.[2] At the same time, those who manufacture distrust in elections use false claims that security has been breached or chain of custody broken as part of their efforts.[3]

Of course, election officials may face criminal prosecution for assisting or cooperating with those who seek to improperly access election equipment.[4] Just as importantly, they have an affirmative obligation to implement steps to prevent and detect unauthorized access to these systems, which have been designated by the Department of Homeland Security as critical infrastructure under federal law,[5] as well as to take remedial action in the event of such a breach.

For example, as the Department of Justice has noted, election officials are required to "safeguard and preserve federal election records,"[6] including records related to any "act requisite to voting" retained on election systems used in federal elections conducted in the previous twenty-two months.[7] The Department has also stated that, "the obligation to retain and preserve [these]

[1] Cybersecurity and Infrastructure Security Agency, *Insider Threat Mitigation Guide*, 2020, https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf.
[2] There have been at least 17 reported incidents where unauthorized actors sought access to voting equipment or election systems since November 2020, and at least five of those incidents led to actual breaches. Nathan Layne and Peter Eisler, "Exclusive: Michigan Widens Probe into Voting System Breaches by Trump Allies," Reuters, June 7, 2022, https://www.reuters.com/world/us/exclusive-michigan-widens-probe-into-voting-system-breaches-by-trump-allies-2022-06-06/; and Alexandra Ulmer and Nathan Layne, "Trump Allies Breach U.S. Voting Systems in Search of 2020 Fraud 'Evidence,'" Reuters, April 28, 2022, https://www.reuters.com/investigates/special-report/usa-election-breaches/.
[3] Philip Bump, "Here Is the Latest Baseless Voter Fraud Allegation, Brought to You by Trump and Tucker Carlson," *Washington Post*, July 15, 2021, https://www.washingtonpost.com/politics/2021/07/15/here-is-latest-baseless-voter-fraud-allegation-brought-you-by-trump-tucker-carlson (overviewing how Tucker Carlson spread false information that a warehouse holding absentee ballots in Fulton County was broken into and that ballots were counted twice).
[4] See Bente Birkeland and Megan Verlee, "Colorado Clerk Is Indicted for Election Tampering and Misconduct," NPR, March 9, 2022, https://www.npr.org/2022/03/09/1085452644/colorado-clerk-indicted-on-13-counts-of-election-tampering-and-misconduct. Those who pressure election officials to turn over access to voting equipment may also face prosecution. See Heidi Przybyla, "Michigan AG Calls for Special Prosecutor in Case Now Involving Her Trump-Backed Opponent," *Politico*, August 7, 2022, https://www.politico.com/news/2022/08/07/michigan-attorney-general-special-prosecutor-trump-00050244.
[5] Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.
[6] 52 U.S.C. § 20701.
[7] See, e.g., U.S. Department of Justice, Letter from Principal Deputy Assistant Attorney General Pamela Karlan to Arizona State Senator Karen Fann dated May 5, 2021, https://www.justice.gov/crt/case-document/file/1424586/download (detailing concerns that "the ballots, election systems and election materials" for Maricopa County "are not being adequately safeguarded," and noting that "state and local election officials …

Brennan Center for Justice at New York University School of Law
120 Broadway, Suite 1750 New York, NY 10271

election records remains intact regardless of who has physical possession of those records."[8] It is "a federal crime for '[a]ny officer of election' or 'custodian' of election records to willfully fail to comply with the retention and preservation requirements."[9]

Moreover, because breaches of equipment could allow malicious actors to corrupt election systems in ways that may be undetectable, failure to respond appropriately when there is a suspected breach risks violating voters' rights under federal and state law,[10] including the right to have their votes counted accurately.[11] Failure to appropriately respond may also risk violating state law where the use of voting systems certified by the Election Assistance Commission (EAC) is required.[12] To protect voters in the face of this growing threat, state and local election officials should follow these key recommendations:

- **Follow best practices and principles for detecting and confirming whether physical breaches have occurred in the first place**.

These practices include the use of keycard systems and video surveillance to track and log access to sensitive equipment, along with regular monitoring of these records to detect potential breaches.[13]

- **Prepare and plan to respond to breaches promptly and decisively.**

A prompt and decisive response to such breaches is only possible if you have a plan in place for what to do when an intrusion is detected. As the Cybersecurity and Infrastructure Security

---

[must] maintain, for twenty-two months after the conduct of an election for federal office, 'all records and papers' relating to any 'act requisite to voting in such election')(citations omitted).

[8] Department of Justice, *Federal Law Constraints on Post-Election "Audits"*, 2021, 3, https://www.justice.gov/opa/press-release/file/1417796/download.

[9] Department of Justice, *Federal Law Constraints on Post-Election "Audits"*, 2021, 3, https://www.justice.gov/opa/press-release/file/1417796/download (52 U.S.C. § 20701).

[10] 52 U.S.C. § 10307; e.g., Nev. Const. art. 2, § 1A.

[11] 52 U.S.C. § 10310; where a private right of action exists to enforce these and related rights and laws, those continuing to use potentially corrupted equipment may also face litigation from aggrieved voters.

[12] See Election Assistance Commission, *Voting System Testing and Certification Program Manual Version 3.0*, 39, https://www.eac.gov/sites/default/files/TestingCertification/Testing_and_Certification_Program_Manual_Version_3_0.pdf ("Any modification to the system not authorized by the EAC voids the certificate."); see also Election Assistance Commission, *Notice of Clarification 19-01: Software De Minimis Changes*, 2019, 1, https://www.eac.gov/sites/default/files/voting_equipment/NOC19.01_SoftwareDeMinimisChanges_11-15-2019.pdf ("Under no circumstances shall a change be considered de minimis if it has reasonable and identifiable potential to impact the system's performance and compliance with the applicable voting Standard."); Kim Zetter, "Election Commission Orders Top Voting Machine Vendor to Correct Misleading Claims," *Politico*, August 13, 2020, https://www.politico.com/news/2020/08/13/election-voting-machine-misleading-claims-394891; Jerome Lovato, "Certification: State vs Federal: An Insider's Perspective," Election Assistance Commission Presentation, Slide 14, http://bowencenterforpublicaffairs.org/wp-content/uploads/2018/06/Certification-State-vs-Federal-an-Insiders-Perspective-6-19-18.pdf (a map of states that require federal certification).

[13] Cybersecurity and Infrastructure Security Agency, *Election Infrastructure Insider Threat Mitigation Guide*, 4, https://www.cisa.gov/sites/default/files/publications/election_insider_threat_mitigation_guide_508_0.pdf; see Maggie Astor, "Colorado County Clerk Indicted in Voting Security Breach Investigation," *New York Times*, March 9, 2022, https://www.nytimes.com/2022/03/09/us/politics/tina-peters-colorado-election.html (discussing how prosecutors used evidence such as "someone us[ing] [a] badge to enter secure areas of the election offices" and records of "the security cameras in the election office [being] turned off" to indict Tina Peters for tampering with voting equipment).

Agency (CISA) has noted, "If it is determined that the chain of custody of critical systems have been compromised, the safest practice is to decommission and replace those systems."[14] A rapid response will help to ensure that potentially corrupted equipment is replaced in time for the next election, including time to allow for pre-election testing on the new equipment.

- **Communicate remedial steps to the public.**

Public confidence in future elections can be severely damaged by plausible allegations that unauthorized or biased actors have been given physical access to voting equipment.[15] When a breach has been detected, or there is an allegation of such a breach, state and local officials should explain publicly what steps they have taken to investigate the allegations, how they have confirmed the truth or falsity of the allegations, and how they have responded to mitigate the possible risks.

I. How Insider Threats Risk Both the Integrity of Election Equipment and Americans' Trust in Elections

Since the 2020 election, there have been at least 17 reported incidents where conspiracy theorists have gained or attempted to gain access to voting equipment.[16] These incidents were often in coordination with, or at the behest of, some of the most prominent purveyors of election disinformation.[17]

We have attached a table with this letter that details what is publicly known about some of the most notable incidents. It demonstrates that most jurisdictions with known breaches have promptly replaced election equipment after physical access to the equipment was provided to unvetted parties.[18] When officials were unable to verify chain of custody, replacement of the equipment was the best way to ensure that voters would be using machines free from possible corruption.

Of course, actual corruption of election systems is not the only risk to election integrity in the event of unauthorized access to election systems. When election officials, election workers, or

---

[14] Rosalind S. Helderman, "Arizona Secretary of State Says Maricopa County Should Replace Election Equipment Because GOP-Backed Recount Compromised Its Security," *Washington Post*, May 20, 2021, https://www.washingtonpost.com/politics/arizona-audit-voting-equipment/2021/05/20/a8370368-b9a4-11eb-a5fe-bb49dc89a248_story.html.

[15] Cybersecurity and Infrastructure Security Agency, *Election Infrastructure Insider Threat Mitigation Guide*, 8, https://www.cisa.gov/sites/default/files/publications/election_insider_threat_mitigation_guide_508_0.pdf.

[16] Nathan Layne and Peter Eisler, "Exclusive: Michigan Widens Probe into Voting System Breaches by Trump Allies," Reuters, June 7, 2022, https://www.reuters.com/world/us/exclusive-michigan-widens-probe-into-voting-system-breaches-by-trump-allies-2022-06-06/.

[17] Lawrence Norden, "Illegal Attempts to Access Voting Machines Didn't Stop with Jan. 6 Insurrection," Brennan Center for Justice, June 28, 2022, https://www.brennancenter.org/our-work/analysis-opinion/illegal-attempts-access-voting-machines-didnt-stop-jan-6-insurrection.

[18] See, e.g., Lacey Latch and Mary Jo Pitzl, "Maricopa County Will Spend Millions to Replace Voting Machines Turned Over to the Arizona Senate for Audit," *Arizona Republic*, July 14, 2021, https://www.azcentral.com/story/news/politics/arizona/2021/07/14/arizona-audit-maricopa-county-spend-2-8-m-replace-voting-machines/7965882002; and Faith Miller, "Mesa County Commissioners Vote to Replace Dominion Voting Equipment," *Colorado Newsline*, August 24, 2021, https://coloradonewsline.com/briefs/mesa-county-commissioners-vote-to-replace-dominion-voting-equipment.

even observers seek to sow distrust, they can use physical proximity to election equipment or ballots to make it appear as if unauthorized or unknown persons have accessed these sensitive materials. For instance, in 2021, a group sowing baseless conspiracies about the integrity of Fulton County, Georgia's election in November 2020 found a door left accidentally unlocked at a county building. This was used to spin a false narrative implying that the ballot rooms had been broken into.[19] The resulting conspiracy theory that ballots could have been tampered with was cited by people who left death threats for election workers.[20]

CISA has previously warned that malicious actors may use publicly available voter registration data to spread false claims of a compromised election infrastructure, such as a hacked voter registration database.[21] In the current environment, insiders may use their status to spread false claims of compromised voting systems, as part of their efforts to sow distrust in those systems.[22]

II. How to Respond to Allegations of a Physical Breach

A. Conduct a prompt investigation and move to replace equipment if needed, providing financial assistance where possible.

Breaches of physical security of election equipment can result in corrupted election systems that can no longer be used to conduct elections safely.[23] According to CISA, "[T]he safest practice is to decommission and replace those systems."[24] If software were altered in any manner, this

[19] Bill McCarthy, "Tucker Carlson Spins Web of Misleading Claims as He Alleges 'Meaningful Voter Fraud' in Georgia," *PolitiFact*, July 20, 2021, https://www.politifact.com/factchecks/2021/jul/20/tucker-carlson/tucker-carlson-spins-web-misleading-claims-he-alle/; Stephen Fowler, "Fulton County Investigating Alarm at Election Warehouse as Conspiracy Theories Grow," Georgia Public Broadcasting, June 1, 2021, https://www.gpb.org/news/2021/06/01/fulton-county-investigating-alarm-at-election-warehouse-conspiracy-theories-grow; and Madeleine May and Alexis Johnson, "How an Election Conspiracy Theory Led Back to Georgia Cops," *Vice News*, March 11, 2022, https://www.vice.com/en/article/qjbnyd/georgia-fulton-county-election-conspiracy.

[20] Madeleine May and Alexis Johnson, "How an Election Conspiracy Theory Led Back to Georgia Cops," *Vice News*, March 11, 2022, https://www.vice.com/en/article/qjbnyd/georgia-fulton-county-election-conspiracy.

[21] Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, *False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections*, 2020, https://www.cisa.gov/sites/default/files/publications/PSA_voter_registration_data_508pobs.pdf.

[22] See, e.g., Michael Lyle, "GOP SOS Hopeful Imports Election Fraud Theorists to Promote Nye County Measure," *Nevada Current*, March 16, 2022, https://www.nevadacurrent.com/2022/03/16/gop-sos-hopeful-imports-election-fraud-theorists-to-promote-nye-county-measure/; and Rosalind S. Helderman, Amy Gardner, and Emma Brown, "How Trump Allies Are Pushing to Hand-Count Ballots around the U.S.," *Washington Post*, April 4, 2022, https://www.washingtonpost.com/politics/2022/04/04/trump-hand-counted-ballots-dominion-machines.

[23] For instance, Maricopa County had to replace voting equipment after said equipment had possibly been tampered with during an election audit. See Lacey Latch and Mary Jo Pitzl, "Maricopa County Will Spend Millions to Replace Voting Machines Turned Over to the Arizona Senate for Audit," *Arizona Republic*, July 14, 2021, https://www.azcentral.com/story/news/politics/arizona/2021/07/14/arizona-audit-maricopa-county-spend-2-8-m-replace-voting-machines/7965882002. See also Letter from Secretary of State Katie Hobbs to Senators Karen Fann and Warren Petersen, March 3, 2021, https://azsos.gov/sites/default/files/Fann_Letter_3_3_2021.pdf (warning the Arizona State Senate that it should "[d]evelop and implement procedures to ensure the physical security of the ballots and physical, data, and cyber security of election equipment" before assuming custody of said equipment, because it could otherwise be mishandled and compromised).

[24] Rosalind S. Helderman, "Arizona Secretary of State Says Maricopa County Should Replace Election Equipment Because GOP-Backed Recount Compromised Its Security," *Washington Post*, May 20, 2021,

would void EAC certification of the equipment.[25] Voters may even seek to litigate to enforce provisions of federal or state law that forbid the use of corrupted or uncertified equipment. As a result, state and local officials should conduct prompt investigations into suspected physical breaches of equipment in order to determine the extent and scope quickly, so that compromised equipment can be replaced before it must be used in election preparation, pre-election testing, and the election itself. This should include checking all election system logs to see if there were failed or successful log-in attempts, as well as any other activity. Where replacement of equipment is impossible, election officials should consult closely with CISA to determine whether alternate steps will provide adequate protection.

As seen in the table attached to this letter, multiple states that have faced this scenario have chosen to prioritize security, by obtaining replacement equipment for potentially corrupted assets—or at the very least decommissioning or seizing potentially corrupt equipment—well before any criminal or civil sanctions are imposed on any individuals.[26]

State and local officials should not only determine the facts promptly; they should assist counties and municipalities that may be facing surprise costs. Such officials should access emergency funds and any unallocated federal funds provided through the EAC when possible to help counties replace corrupted equipment in time to protect the next election.

B. Communicate remediation steps to the public.

Public confidence in future elections can be severely damaged by plausible allegations that unauthorized or untrusted actors have been given physical access to voting equipment. State and local officials should explain publicly what steps they have taken to investigate the allegations, and how they have confirmed the truth or falsity of the allegations.[27] Officials should also explain how they have determined the scope of any breach, and how that impacts the scope of

---

https://www.washingtonpost.com/politics/arizona-audit-voting-equipment/2021/05/20/a8370368-b9a4-11eb-a5fe-bb49dc89a248_story.html.

[25] See Election Assistance Commission, *Voting System Testing and Certification Program Manual Version 3.0*, 41, https://www.eac.gov/sites/default/files/TestingCertification/Testing_and_Certification_Program_Manual_Version_3_0.pdf ("Any modification to the system not authorized by the EAC voids the certificate.").

[26] See, e.g., Lacey Latch and Mary Jo Pitzl, "Maricopa County Will Spend Millions to Replace Voting Machines Turned Over to the Arizona Senate for Audit," *Arizona Republic*, July 14, 2021, https://www.azcentral.com/story/news/politics/arizona/2021/07/14/arizona-audit-maricopa-county-spend-2-8-m-replace-voting-machines/7965882002; Faith Miller, "Mesa County Commissioners Vote to Replace Dominion Voting Equipment," *Colorado Newsline*, August 24, 2021, https://coloradonewsline.com/briefs/mesa-county-commissioners-vote-to-replace-dominion-voting-equipment; Nathan Layne and Peter Eisler, "Exclusive: Michigan Widens Probe into Voting System Breaches by Trump Allies," Reuters, June 7, 2022, https://www.reuters.com/world/us/exclusive-michigan-widens-probe-into-voting-system-breaches-by-trump-allies-2022-06-06/ (discussing how law enforcement seized election equipment in various localities); and CBS News Pittsburgh, "Pennsylvania Decertifies Fulton County's Voting System after Post-Election Audit," July 21, 2021, https://www.cbsnews.com/pittsburgh/news/pennsylvania-decertifies-fulton-county-voting-system-audit.

[27] See, e.g., Letter from Acting Secretary of the Commonwealth Veronica W. Degraffenreid to James M. Stein, July 20, 2021, https://www.dos.pa.gov/about-us/Documents/statements/2021-07-20-Letter-to-Fulton-County-Officials.pdf (explaining in a public letter how Pennsylvania's Secretary of the Commonwealth arrived at the conclusion to decertify election equipment in Fulton County, PA); and Justin Gray, "Georgia Election Officials Show Frame-by-Frame What Happened in Fulton Surveillance Video," WSB-TV, December 4, 2020, https://www.wsbtv.com/news/politics/georgia-election-officials-show-frame-by-frame-what-really-happened-fulton-surveillance-video/T5M3PYIBYFHFFOD3CIB2ULDVDE.

replacing equipment. For instance, officials can indicate that they have reviewed camera surveillance footage and determined that an alleged breach did not occur, as Fulton County officials did in response to allegations that ballots were left unsecure.[28] Or, they can indicate that they confirmed through such footage that an unauthorized visitor was never left alone with equipment, or never touched it.

III. Prevent and Detect Future Breaches

In order to successfully carry out the steps outlined above, best practices for preventing and detecting breaches must be in place.[29] If keycard access logs and surveillance camera footage is not available to review, then it may be impossible to determine the truth or falsity of an alleged breach, not to mention the scope of the breach. States and counties should take the following actions (and, where appropriate, provide the funds necessary to support such mandates):

A. Restrict access to election systems.

Election officials should ensure that an individual only has access to critical systems—both physical and digital—if access is necessary for that individual to perform their official responsibilities, and only to the extent that those responsibilities require it (this is known as the "principle of least privilege").[30] In addition, election officials should require all individuals that access critical systems to first complete a background check. A recent regulation in Colorado,[31] for example, restricts voting system access to individuals who have passed a background check and are an employee of the county clerk, voting system provider, or secretary of state's office.

Where possible, official procedures should require two people and/or bipartisan teams to be present when accessing election systems, ballots, and election records. Election staff should also be on site with private vendors at all times.

B. Establish transparent procedures and monitor for inappropriate activity.

Transparency protocols helped officials in Colorado identify the source of leaked voting system information.[32] All election officials should adopt and actively review transparency protocols to ensure that every person who accesses election systems is authorized to do so. Funding should be provided for election officials to install keycard access to facilities that hold voting systems, so that a log of every entry can be created. All election offices should be equipped with and require

---

[28] Justin Gray, "Georgia Election Officials Show Frame-by-Frame What Happened in Fulton Surveillance Video," WSB-TV, December 4, 2020, https://www.wsbtv.com/news/politics/georgia-election-officials-show-frame-by-frame-what-really-happened-fulton-surveillance-video/T5M3PYIBYFHFFOD3CIB2ULDVDE.
[29] Cybersecurity and Infrastructure Security Agency, *Election Infrastructure Insider Threat Mitigation Guide*, 5, https://www.cisa.gov/sites/default/files/publications/election_insider_threat_mitigation_guide_508_0.pdf.
[30] "Election Security Spotlight – Principle of Least Privilege," Center for Internet Security, accessed August 10, 2022, https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-principle-of-least-privilege.
[31] State of Colorado Department of State, *Notice of Temporary Adoption: Election Rules 8 CCR 1505-1*, 2021, https://www.sos.state.co.us/pubs/rule_making/files/2021/20210617ElectionsNoticeTempAdoption.pdf.
[32] Emma Brown, "An Elections Supervisor Embraced Conspiracy Theories. Officials Say She Has Become an Insider Threat," *Washington Post*, September 26, 2021, https://www.washingtonpost.com/investigations/an-elections-supervisor-embraced-conspiracy-theories-officials-say-she-has-become-an-insider-threat/2021/09/26/ee60812e-1a17-11ec-a99a-5fea2b2da34b_story.html.

24-hour surveillance of voting systems and ballots, which can be reviewed and compared with access logs in the event of unauthorized activity—real or alleged. Note that in the Fulton County incident described above, without security camera footage, it would have been impossible to ultimately disprove the misleading claims that ballot security had been compromised.

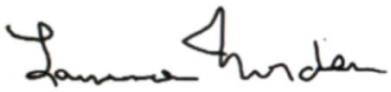
C. Don't forget the vendors.

Private vendors are involved at every stage of an election, from registering voters to counting ballots to reporting results. States can act now to establish standards on cybersecurity, personnel security, and supply chain integrity for their election vendors.[33] Local election offices can also build in safeguards through contracts when purchasing equipment and services, as detailed in a 2019 Brennan Center Report.[34]

* * *

Former CISA leader Chris Krebs has described the current threat to election infrastructure from insiders as "new and, frankly more discouraging."[35] However, the steps detailed in this letter can mitigate this threat. When unauthorized access is alleged, state and local officials should promptly investigate the allegation and determine the scope of any potential breach, replacing equipment that is no longer trustworthy, and securing resources where possible to cover the sudden costs that affected counties may be forced to bear. This will avoid violations of state law that may require the use of certified equipment, as well as state and federal laws protecting the right to vote and have one's vote counted.

Respectfully,



Lawrence Norden
Senior Director, Elections and Government
Brennan Center for Justice at NYU School of Law

---

[33] Lawrence Norden, Gowri Ramachandran, and Christopher Deluzio, *A Framework for Election Vendor Oversight*, Brennan Center for Justice, November 12, 2019, https://www.brennancenter.org/our-work/policy-solutions/framework-election-vendor-oversight.

[34] Christopher Deluzio, *A Procurement Guide for Better Election Cybersecurity*, Brennan Center for Justice, March 22, 2019, https://www.brennancenter.org/our-work/policy-solutions/procurement-guide-better-election-cybersecurity.

[35] Nick Corasaniti and Alexandra Berzon, "The Strange Tale of Tina Peters," *New York Times*, June 26, 2022, https://www.nytimes.com/2022/06/26/us/politics/tina-peters-election-conspiracy-theories.html.

List of Notable Incidents and State Response		
Location	**Description**	**State Response**
Mesa County, CO	County Clerk allowed an unauthorized person to make an image of voting equipment hard drives, which were later shared online and at a Mike Lindell-sponsored conference of election deniers, along with passwords used to access the county's election software.	Secretary of State decommissioned the voting equipment following investigation into breach.
Coffee County, GA	Elections Supervisor opened her offices to election-denier activists. The Supervisor said that they did not enter a room that housed the county's voting machines, but did not know whether they entered the room housing the election management system server, the central computer used to tally election results.	Secretary of State launched an investigation and removed the county's election server shortly after notification of incident.
Adams Township, MI	Township Clerk refused to allow a vendor to perform routine maintenance on a voting machine because the clerk falsely believed the maintenance would erase old data that could prove the machines were rigged. A central component went missing shortly thereafter, but has since been recovered.	Secretary of State removed election responsibilities from township clerk and transferred to county clerk.
Barry, Missaukee & Roscommon Counties, MI	At least nine clerks were pressured by state and local officials to turn voting equipment over to unauthorized third parties, with some agreeing to do so. A vendor review of the voting equipment that had been turned over found evidence of physical tampering, but no evidence of software or firmware manipulation.	Attorney General and State Police launched an investigation into the incidents following a request from the Secretary of State. The state recovered and decommissioned all voting equipment.
Fulton County, PA	Fulton County gave a third party access to its election databases and other certified equipment to conduct a review of the 2020 results.	Secretary of the Commonwealth decommissioned the County's voting equipment.