CONFLICTS OF INTEREST AND ELECTION CYBERSECURITY: HOW BIPARTISAN CONGRESSIONAL OVERSIGHT CAN INFORM THE PUBLIC, ADDRESS ELECTION SYSTEM VULNERABILITIES, AND INCREASE VOTER CONFIDENCE IN ELECTION INTEGRITY

KIMBERLY BREEDON† & A. CHRISTOPHER BRYANT‡

---

† Assistant Professor, Barry University School of Law.

‡ Rufus King Professor of Constitutional Law, University of Cincinnati College of Law. The authors thank the participants in the February 28, 2020, American Constitution Society Constitutional Law Scholars Forum for helpful and encouraging comments. The authors also thank Zachery Hullinger for excellent research assistance, and the University of Cincinnati and the Harold C. Schott Foundation for financial support. Of course, remaining errors are ours alone.

ABSTRACT

Fewer than four months out from what will certainly be one of the most consequential and polarizing presidential elections in American history—and four years after unprecedented foreign efforts to influence a U.S. presidential election—much of our election infrastructure remains dangerously vulnerable to cyber manipulation or attack. This Article begins by recounting the core principles that comprise election cyber-security best practices. It then identifies some of the more egregious examples of existing systems falling short of those standards. Next, the Article turns to an examination of the role that congressional oversight already has played—and in coming months might continue to play—in shoring up our election infrastructure against vulnerabilities to attack. To do so, this Article first surveys the congressional inquiries into election security that have to date occurred and discusses the major themes that have emerged from those proceedings. It then explores why, going forward, congressional oversight may offer the best avenue for federal intervention in support of improving election cyber security. For reasons both practical and theoretical, the best that federal legislators may be able to do at this point is to shine the light of disclosure on problems remaining unresolved in the hopes of bringing public attention and political pressure to bear on those currently in positions to address these problems directly. But this proposed use of oversight to reveal wrongdoing itself raises fundamental questions about the proper purpose and reach of congressional investigatory authority. Those questions are examined herein in the light cast by the Supreme Court's rather ambivalent treatment of Congress's "informing function" over the last eighty years. This Article concludes by identifying principles for differentiating between appropriate congressional efforts to "inform" the public as to existing problems needing attention and improper and abusive congressional efforts to "expose" for the purpose of punishing;

these principles illustrate why the congressional oversight of election security that is discussed in this Article falls on the correct side of that divide.

I. INTRODUCTION

It is tempting to assume that, at this late date, one would have to be under a proverbial rock not to be aware that entities, foreign and domestic, are targeting the integrity of this year's—and coming years'—U.S. elections. If this assumption is true, judging from their conduct alone, it appears that too many of our nation's officials who are responsible for election administration have not been much in the sun of late.

One year ago, we published an article identifying significant gaps in electronic election security.[1] We hardly expected our piece to spur Herculean efforts, as law review articles rarely—and ours never—have such tangible impact. But still, it is disturbing how little progress has been made to close those gaps and how much work remains in the rapidly diminishing window of time that exists until our electoral system will again face its most dramatic test.

In this Article, we first reiterate, in Part II, the core principles that comprise election cyber-security best practices,[2] and, in Part III, we identify some of the more egregious examples of existing systems still falling short of those standards.[3] Then, we turn our attention to the role that congressional oversight already has played—and in coming months might continue to play—in shoring up our election infrastructure against vulnerabilities to attack. Part IV surveys the congressional inquiries into election security that have to date occurred,[4] and Part V discusses the major themes that have emerged from those proceedings.[5] Part VI explores why, going forward, congressional oversight may offer the best avenue for federal intervention in support of improving election cyber security, noting that for reasons both practical and theoretical, the best that federal legislators may be able to do at this point is to shine the light of disclosure on problems remaining unresolved in the hopes of bringing

1. Kimberly Breedon & A. Christopher Bryant, *Counting the Votes: Electronic Voting Irregularities, Election Integrity, and Public Corruption*, 49 U. MEM. L. REV. 979 (2019).
2. *See infra* Part II.
3. *See infra* Part III.
4. *See infra* Part IV.
5. *See infra* Part V.

public attention and political pressure to bear on those currently in positions to address these problems directly.[6]

In calling upon committees of Congress to exercise their oversight authority to reveal potentially embarrassing, and perhaps even legally culpable, failures on the part of those not serving in the federal bureaucracy, we arguably strain the role properly played by congressional committees in exercising the body's public-informing function. We acknowledge this dilemma and employ this occasion to explore the tension between Congress's appropriately celebrated informing function as well as its equally and appropriately condemned abuse of the power to expose individuals for the purpose of eliciting public scorn (or worse).[7] To frame this discussion, Part VII first recounts the ambivalent treatment that Congress's informing function has received in the Supreme Court's case law arising out of and circumscribing congressional investigatory authority.[8] That Part then concludes by providing guidelines to differentiate between salutary informing and condemnable exposing; finally, this Article applies that rubric to assess our own calls for congressional oversight as a remedy for election security vulnerabilities.[9]

II. RECOMMENDED BEST PRACTICES

Cyber security and election security experts have reached a unanimous consensus that attacks from malign actors—whether foreign or domestic—on our election systems are most effectively countered by the use of paper ballots and post-election risk-limiting audits.[10] Further,

6. *See infra* Part VI.
7. *See infra* Part VII.
8. *See infra* Part VII.
9. *See infra* Part VII.
10. In a recent congressional hearing before the House of Representatives Committee on House Administration, Juan E. Gilbert, Professor and Chair of the Computer & Information Science & Engineering Department at the University of Florida, observed that the 2018 report by the National Academies of Sciences, Engineering, and Medicine, "Securing the Vote: Protecting American Democracy," recommends the use of "human-readable" paper ballots, which "may be marked by hand or machine, such as a ballot marking device (BMD)." *2020 Election Security–Perspectives from Voting System Vendors and Experts Before the H. Comm. on H. Admin.*, 116th Cong. 4 (2020) [hereinafter *2020 Election Security*] (opening statement of Juan E. Gilbert). Other experts emphasize the need for hand-marked paper ballots unless and until BMDs have undergone more rigorous studies. *See, e.g.*, *id.* at 9 (opening statement of Matt Blaze) (explaining the need for caution in the face of "exploitable weaknesses and usability flaws . . . found in these systems" even with "relatively little scrutiny."); *see also* Christopher DeLuzio, *Pennsylvania Commission Issues Urgent Call to Replace*

in its long-awaited report on Russia's attacks on the 2016 U.S. election, the bipartisan Senate Select Committee on Intelligence emphasized the critical and urgent importance of replacing paperless voting systems as a vital means for protecting the nation's elections from malign attacks, and it expressed support for using paper ballots and optical scanners, recognizing that they are "the least vulnerable to cyber attack."[11] In addition, the Bipartisan Policy Center recently convened a task force to develop recommendations for implementing best practices to improve the voting experience of American citizens.[12] The resulting report includes twenty-one recommendations ranging from voter registration to post-election certification.[13] Among the Bipartisan Policy Center's recommendations was the following: "Recommendation 18: States

---

Vulnerable Voting Machines, BRENNAN CTR. FOR JUST. (Sept. 27, 2018), https://www.brennancenter.org/our-work/analysis-opinion/pennsylvania-commission-issues-urgent-call-replace-vulnerable-voting [http://web.archive.org/web/20200422175858/https://www.brennancenter.org/our-work/analysis-opinion/pennsylvania-commission-issues-urgent-call-replace-vulnerable-voting] (quoting Brennan Ctr. Counsel Elizabeth L. Howard's testimony before a Pennsylvania legislative committee and noting that the "'unanimous national security and scientific community consensus is that replacing all paperless voting machines with equipment that creates a paper record of every vote cast is the simple solution' to bolster the security of elections"); Robert McMillan & Dustin Volz, *Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds*, WALL ST. J. (Sept. 27, 2018), https://www.wsj.com/articles/widely-used-election-systems-are-vulnerable-to-attack-report-finds-1538020802 [http://web.archive.org/web/20200422180010/https://www.wsj.com/articles/widely-used-election-systems-are-vulnerable-to-attack-report-finds-1538020802] (observing that the National Academies of Sciences, Engineering, and Medicine recommended that "U.S. states move away from voting machines that don't include paper ballots"); J.B. Wogan, *Votes Miscounted? Your State May Not Be Able to Find Out,* GOVERNING (Dec. 2, 2016), http://www.governing.com/topics/politics/gov-states-vote-election-audits-recounts.html [http://web.archive.org/web/20200422175532/https://www.governing.com/topics/politics/gov-states-vote-election-audits-recounts.html] ("[A]s it's become clear that without a paper record there's no way to verify vote tallies, computer scientists and election activists have begun pushing for states to not only keep a paper record but to also institute routine post-election audits.").

11. 1 SENATE SELECT COMM. ON INTELLIGENCE, 116TH CONG., RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf [https://web.archive.org/web/20200616071308/https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf] [hereinafter RUSSIAN ACTIVE MEASURES].

12. BIPARTISAN POLICY CENTER, LOGICAL ELECTION POLICY: REPORT AND RECOMMENDATIONS OF BPC'S TASK FORCE ON ELECTIONS 5 (2020).

13. *See generally id.*

should conduct pre-certification tabulation audits where all types of ballots are subject to review."[14]

To contextualize these recommendations, this Part first describes the options for casting and counting votes,[15] as well as those for conducting post-election audits,[16] and then it discusses the reasons why paper ballots and risk-limiting audits are deemed by experts to be the gold standard for election security and integrity.[17]

A. Options for Casting and Counting Votes

When voters cast their ballots in U.S. elections, they do so using one of three general classes of voting machines: optical scan ballot readers, ballot marking devices (BMDs), or direct-recording electronic (DRE) voting machines.[18] An optical scan ballot reader relies on voter-marked paper ballots that are scanned by and entered into the machine, which captures and stores both the paper record and an electronic tally of the votes cast by the ballot.[19] A ballot marking device is a voting machine that allows voters to cast their votes on a computer touchscreen and that then prints a paper ballot with a QR code or other barcode representing the voters' selections, along with an English-language "translation"; the ballot can then be entered into a separate scanning device, which reads the QR code or the barcode and tallies and stores the votes.[20] BMDs were originally designed as an assistive technology to aid visually-impaired or mobility-impaired voters in casting their votes, but they have since been

---

14. *Id.* at 40. The task force also recommended that if "significant discrepancies" are uncovered by a post-election audit, then states should have in place and employ "a process to correct the result, such as a recount." *Id*. at 42.

15. *See infra* Part II.A.

16. *See infra* Part II.B.

17. *See infra* Part II.C.

18. Raj Karan Gambhir & Jack Karsten, *Why Paper Is Considered State-of-the-Art Voting Technology*, BROOKINGS (Aug. 14, 2019), https://www.brookings.edu/blog/techtank/2019/08/14/why-paperless-is-considered-state-of-the-art-voting-technology/ [http://web.archive.org/web/20200422182154/https://www.brookings.edu/blog/techtank/2019/08/14/why-paperless-is-considered-state-of-the-art-voting-technology/]; *2020 Election Security*, *supra* note 10, at 15 (opening statement of Matt Blaze). Some descriptions of BMD machines categorize them as a type of DRE machine. *See, e.g.*, Breedon & Bryant, *supra* note 1, at 988–89.

19. *2020 Election Security*, *supra* note 10, at 4–5 (opening statement of Matt Blaze); Gambhir & Karsten, *supra* note 18.

20. *2020 Election Security*, *supra* note 10, at 15 (opening statement of Matt Blaze); Gambhir & Karsten, *supra* note 18.

adopted for widespread use among all voters.[21] A direct-recording electronic voting machine requires votes to be entered by touchscreen or similar input devices, which then transmit the data representing digital ballots directly into the voting machine's memory.[22] Although some DREs include a Voter Verified Paper Audit Trail, which displays the voter's electronic selection of candidates on a paper roll visible to the voter behind a window on the machine,[23] the DREs used in several jurisdictions do not provide any paper record at all.[24]

B. Options for Conducting Post-election Audits

Post-election audits relying on a paper trail generally fall into one of two categories: traditional "percentage" audits and more recent "tabulation" audits.[25] According to the National Conference of State Legislatures, thirty-four states and the District of Columbia require percentage audits after elections have been conducted.[26] A percentage audit reviews the cast ballots in a randomly chosen fixed percentage of voting districts or voting machines and compares the ballots or other voter-verifiable paper record to the results produced by the voting system.[27] When jurisdictions use percentage audits, the number of ballots to be counted remains constant, regardless of how wide or narrow the margin is between the votes cast for the winning candidate and those cast for the losing candidate or candidates.[28] In some jurisdictions, this type

---

21. *2020 Election Security*, *supra* note 10, at 5, 8–9 (opening statement of Matt Blaze); *Id.* at 4 (opening statement of Juan E. Gilbert).

22. *Id.* at 15 (opening statement of Matt Blaze); Kim Zetter, *The Crisis of Election Security*, N.Y. TIMES MAG. (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html [http://web.archive.org/web/20200422183351/https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html]; Gambhir & Karsten, *supra* note 18.

23. Gambhir & Karsten, *supra* note 18; Zetter, *supra* note 22.

24. Zetter, *supra* note 22; Wogan, *supra* note 10 (noting that in the 2016 presidential election, "[fifteen] states [did] not require paper trails that could be compared against electronic voting tallies").

25. BIPARTISAN POLICY CTR., *supra* note 12, at 41.

26. *Post-Election Audits*, NAT'L CONF. OF ST. LEGISLATURES (Oct. 25, 2019), http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx [http://web.archive.org/web/20200422183944/https://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx].

27. *Id.*; BIPARTISAN POLICY CTR., *supra* note 12, at 41.

28. *Post-Election Audits*, *supra* note 26 ("Even in a landslide election, [auditors] will count the same number of ballots as they would in a nail-biter election.").

of audit is conducted wholly manually, while in others, some portion of the audit may be conducted electronically.[29]

By contrast, tabulation audits seek to ascertain whether the equipment used to tabulate the ballots "counted and reported the vote accurately on the entire population, not only a random selection of precincts."[30] Risk-limiting audits, a species of tabulation audits and the type of audit recommended by cyber security experts, require a manual spot-check of paper ballots' matches to the electronically stored results of those ballots, and they use a random sampling of paper ballots against which to measure a pre-specified "risk limit" (i.e., the percentage chance that the reported outcome is incorrect).[31] Journalist Eric Geller provides the following explanation of risk-limiting audits:

> In a risk-limiting audit, state officials select a sample of paper ballots—usually based on the margin of the outcome—and compare them using statistical methods to the electronically cataloged results of those ballots. They also select a "risk limit," which is the percentage chance that their audit will fail to catch incorrect results that could have been caused by tampering. For example, an audit with a risk limit of [five] percent will have a [ninety-five] percent change of successfully catching the incorrect vote tabulation. Risk-limiting audits can be used to determine whether a more comprehensive recount is needed.[32]

---

29. *Id.*

30. BIPARTISAN POLICY CTR., *supra* note 12, at 41.

31. *See, e.g.*, Eric Geller, *Colorado to Require Advanced Post-Election Audits*, POLITICO (July 17, 2017, 1:01 PM), https://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631 [http://web.archive.org/web/20200422184745/https://www.politico.com/story/2017/07/17/colorado-post-election-audits-cybersecurity-240631]; Marc Schneider, *Protect Public Trust by Auditing Elections: It's Easier Than You Might Think*, THE HILL (Nov. 3, 2018, 4:00 PM), https://thehill.com/opinion/campaign/414631-protect-public-trust-by-auditing-elections-its-easier-than-you-might-think [http://web.archive.org/web/20200422184331/https://thehill.com/opinion/campaign/414631-protect-public-trust-by-auditing-elections-its-easier-than-you-might-think]; BIPARTISAN POLICY CTR., *supra* note 12, at 41].

32. Geller, *supra* note 31.; *see also 2020 Election Security*, *supra* note 10, at 15 (opening statement of Matt Blaze) (explaining risk-limiting audits as follows: "In a risk limiting audit, a statistically rigorous method is used to select a randomized sample of ballots, which are manually checked by hand and compared with their electronic interpretation. (This must be done for *every* contest, not just those with close results that might otherwise call for a traditional 'recount'.) If discrepancies are discovered between the manual and electronic tallies, additional manual checks are conducted.").

Although the Bipartisan Task Force report expressly declined to endorse any particular method for conducting post-election audits,[33] cybersecurity experts have wholeheartedly embraced risk-limiting audits as the preferred method.[34]

Because cybersecurity and election experts uniformly agree that protecting election integrity requires the use of risk-limiting audits, and because risk-limiting audits require a reliable paper record reflecting voter selections, the current majority consensus recommends hand-marked paper ballots that can be retained and used in such audits. Accordingly, Matt Blaze, Professor of Computer Science and Law at Georgetown University, in testimony before the House Committee on House Administration, emphasized that "risk-limiting audits are only meaningful if there is a reliable, human-readable artifact of the voters' true selections, such as is provided by paper ballots that have been directly marked by the voter"[35] and recommended that paperless DRE machines be abandoned altogether.[36] BMD-based voting systems present a potentially more secure alternative, but experts disagree on whether those systems can adequately capture the vote as the voter expresses it.[37] Because BDMs are a newer technology, future studies and technological developments may yield greater expert consensus on their reliability for purposes of risk-limiting audits. For now, an apparent majority of

---

33. BIPARTISAN POLICY CTR., *supra* note 12, at 42.

34. A recent consensus report by the National Academies of Sciences, Engineering, and Medicine has set a recommended target date of 2028 by which "risk-limiting audits should be conducted for all federal and state election contests, and for local contests where feasible." MARK LINDEMAN, VERIFIED VOTING FOUND., CITY OF FAIRFAX, VA: PILOT RISK-LIMITING AUDIT 4 (2018) (citing NAT'L ACADS. OF SCI., ENG'G., & MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 101 (2018)), https://www.verifiedvoting.org/wp-content/uploads/2018/12/2018-RLA-Report-City-of-Fairfax-VA.pdf [http://web.archive.org/web/20200422185436/https://www.verifiedvoting.org/wp-content/uploads/2018/12/2018-RLA-Report-City-of-Fairfax-VA.pdf]); *see* Geller, *supra* note 31 ("Digital security specialists have long pushed for states to adopt risk-limiting audits, which they say are a fast and inexpensive way to give the public confidence that votes were not altered in any way.").

35. *2020 Election Security*, *supra* note 10, at 15 (opening statement of Matt Blaze).

36. *Id.* at 2. Professor Blaze also cites other security reasons for eliminating DREs, including, for example, their greater vulnerability to hacking and tampering. *See id*. at 9–10.

37. *Compare id.* (expressing deep concerns about the vulnerability of BMDs to hacking and tampering in ways that voters will be unlikely to catch), *with id.* at 15 (opening statement of Juan E. Gilbert) (arguing that improving instructions to voters to check their selections decreases errors or successful malign changes before voter selections are scanned).

experts—while accepting the use of BMDs as assistive devices—recommend hand-marked paper ballots for voters who do not require assistive devices to cast votes.[38]

C. Why Paper Ballots and Risk-limiting Audits Are Considered by Experts as Best Practices for Election Security and Election Integrity

These measures—voter-verifiable (preferably hand-marked) paper ballots and post-election risk-limiting audits—are deemed to be the gold standard for protecting election integrity for a number of reasons. First—and perhaps counterintuitively, given the pervasiveness of electronic record-keeping in today's world—eliminating reliance on technological tools for tallying and reporting votes makes election integrity easier to protect.[39] In other words, the introduction of computer technology into election systems invites the attention of potential hackers.[40] Accordingly, when the machines used to vote or to count votes are computerized, thereby rendering them more susceptible to error, tampering, or hacking, the methods adopted to confirm vote tallies and election results should not rely upon computer hardware or software that may have been subject

---

38. *See, e.g.*, Andrew Appel et al., *Ballot-Marking devices (BMDs) Cannot Assure the Will of the Voters* (Jan. 4, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755 [http://web.archive.org/web/20200422185943/https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755]; *2020 Election Security*, *supra* note 10, at 9 (opening statement of Matt Blaze) ("A maliciously compromised BMD could subtly mismark candidate selections on ballots in a way that might not be noticed by most voters and that could undetectably change election outcomes.").

39. *2020 Election Security*, *supra* note 10, at 3 (opening statement of Juan E. Gilbert) ("Currently, there's no known way to secure a digital ballot. At this time, any election that is paperless is not secure.").

40. Sue Halpern, *How Voting-Machine Lobbyists Undermine the Democratic Process, The New Yorker*, THE NEW YORKER (January 22, 2019), https://www.newyorker.com/tech/annals-of-technology/how-voting-machine-lobbyists-undermine-the-democratic-process [https://web.archive.org/web/20200616164939/https://www.newyorker.com/tech/annals-of-technology/how-voting-machine-lobbyists-undermine-the-democratic-process] ("Any time you introduce computer technology, you introduce the probability that, if there is value, somebody is going to try to hack it." (quoting Duncan Buell, University of South Carolina Professor of Computer Science)); *see also* McMillan & Volz, *supra* note 10 (describing the means by which hackers can gain remote access to a particular type of voting machine used in a number of voting jurisdictions across the country and can use that access to flip votes).

to "malicious subversion."[41] In this way, paper ballots serve a dual purpose: they accurately reflect a voter's choice of candidates, free from hacking or tampering, and they provide a reliable paper trail for conducting recounts or post-election audits.[42]

Second, the "malicious subversion" may remain undetected. As a coalition of election integrity organizations and security experts wrote in a letter to the United States Election Assistance Commission in 2018, "[T]he only way to ensure resilience in voting systems is by requiring voter-verified paper ballots and robust, manual post-election audits of the paper ballots."[43] Among the reasons for their conclusion is the capacity of malign actors to tamper with vote tallies without leaving any trace.[44] U.S. Election Assistance Commissioner Thomas Hicks, in written answers to questions posed by Representative Bennie G. Thompson, Chair of the House Committee on Homeland Security, after an election security hearing held by that Committee on February 13, 2019, explained that, although all voting systems must employ two compartmentalized sources for memory storage, the two separate sources for Direct Recording Electronic (DRE) voting machines are themselves both electronic and, therefore, "a sophisticated attack could alter both sources of memory to make them identical and cause alterations to the data to be undetected."[45] By employing post-election risk-limiting audits based

---

41. LINDEMAN, *supra* note 34, at 4 ("[C]omputerized voting and counting machines are vulnerable to error or malicious subversion, and [therefore] must be checked using methods that do not rely on the correctness of hardware or software.").

42. Breedon & Bryant, *supra* note 1, at 993 ("In short, paper ballots, whether manually counted or processed via optical-scan machines, provide a record of vote tallies independent from electronic capture and therefore are immune to electronic vote tampering, whether such tampering occurs at the polling place or from a remote location.").

43. Letter from Common Cause et al., to Tom Hicks, Chair, U.S. Election Assistance Commission et al. (Oct. 2, 2018), https://www.electiondefense.org/letter-to-eac-and-dhs [http://web.archive.org/web/20200422191806/https://www.electiondefense.org/letter-to-eac-and-dhs].

44. Greg Gordon, *Cyber Experts Cite Vulnerabilities in Washington, North Carolina Security*, MCCLATCHY WASH. BUREAU (Nov. 12, 2018, 9:26 PM), https://www.mcclatchydc.com/latest-news/article221423980.html [http://web.archive.org/web/20200422192024/https://www.mcclatchydc.com/latest-news/article221423980.html] (noting that, according to cyber experts, "[t]here may be no obvious clue to alert election officials when someone preys on the electronic systems."); *2020 Election Security*, *supra* note 10, at 7 (opening statement of Matt Blaze) ("In some cases, successful attacks may not be discovered until long after polls have closed, or may never be discovered at all.").

45. *Defending Our Democracy: Building Partnerships to Protect America's Elections Before the H. Comm. on Homeland Sec.*, 116th Cong. 98 (2019) [hereinafter *Defending Our Democracy*] (question from Chairman Bennie G. Thompson for Thomas Hicks),

upon the hand-marked paper ballots, election officials can counter various methods of electronic vote tampering that may remain invisible to voters and to election officials, including, for example, the clandestine (and potentially remote) planting of software that has been programmed to flip votes or to scramble tabulation systems undetected.[46]

Finally, these measures not only ensure that vote tallies are, in fact, accurate and that outcomes are reliable, but they also increase public confidence that vote tallies are accurate and that outcomes are reliable.[47] The United States Supreme Court recognized the importance of the former of these—the correct and complete counting of ballots—more than a century ago, stating: "We regard it as equally unquestionable that the right to have one's vote counted is as open to protection . . . as the right to [cast a vote]."[48] Several decades later, the Court reiterated the primacy of accurate vote counting in our constitutional order, observing that "[o]bviously included within the right to choose [representatives], secured by the Constitution, is the right of qualified voters within a state to cast their ballots *and have them counted*."[49] But the latter of these—public confidence in voting systems and electoral outcomes—is every bit as important as the former in protecting the healthy functioning of a democratic republic.[50] In other words, accurate vote tallies and reliable

---

https://www.govinfo.gov/content/pkg/CHRG-116hhrg35094/pdf/CHRG-116hhrg35094.pdf
[http://web.archive.org/web/20200422193036/https://www.govinfo.gov/content/pkg/CHRG-116hhrg35094/pdf/CHRG-116hhrg35094.pdf].

46. Frank Bajak, *U.S. Election Integrity Depends on Security-Challenged Firms*, ASSOCIATED PRESS (Oct. 29, 2018), https://www.apnews.com/f6876669cb6b4e4c9850844f8e015b4c
[http://web.archive.org/web/20200422193226/https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c].

47. BIPARTISAN POLICY CTR., *supra* note 12, at 41 ("It is clear to the Task Force that public confidence in election results requires auditing the election process."); LINDEMAN, *supra* note 34, at 4–5 ("A voting system that produces accurate results, but provides no way to know whether it did, is inadequate. It provides far too many ways for resourceful adversaries to undermine public confidence in election integrity.").

48. United States v. Mosley, 238 U.S. 383, 386 (1915).

49. United States v. Classic, 313 U.S. 299, 315 (1941) (emphasis added); *see also* Reynolds v. Sims, 377 U.S. 533, 555 (1964) ("It has been repeatedly recognized that all qualified voters have a constitutionally protected right to vote *and to have their votes counted*" (emphasis added)).

50. As the United States District Court for the Northern District of Georgia noted in *Curling v. Kemp*, "[u]ltimately, an electoral system must be accurate and trustworthy." Curling v. Kemp, 334 F. Supp. 3d 1303, 1324 (N.D. Ga. 2018). This sentiment has been similarly expressed by government officials involved in securing election integrity. *See, e.g.*, Anthony Izaguirre, *MIT: Hackers Could Alter Ballots in Widely Used Voting App*, ASSOCIATED PRESS (Feb. 13, 2020), https://apnews.com/708a578811bfdcffec1f2cfbae3cc

outcomes are a necessary but insufficient condition for effective democratic self-governance.[51] Unless the citizenry also believes that the vote tallies and outcomes are trustworthy, the actual accuracy and reliability of ballot counts and electoral results mean little.[52] An election outcome perceived as tainted casts doubt on the governing decisions made by the winning candidates and undermines the very essence of the democratic experiment itself.[53] In the immediate and near-term aftermath of such an election, the governed may, at least for a time, accept both the results of the election and the resulting policies implemented by office-holders; but repeated instances of perceived election irregularities—without mechanisms for countering them—eventually fosters within the citizenry suspicion of political processes and policies, disengagement from public discourse and political campaigns, and disenfranchisement from both the government and the laws it seeks to implement and uphold.[54] Because the use of paper ballots and manually conducted post-election audits insulates the voting and auditing processes from

---

063
[http://web.archive.org/web/20200422195838/https://apnews.com/708a578811bfdcffec1f2cfbae3cc063] ("'Obviously, integrity and security are prime, but voter confidence is equally important,' [General Counsel for West Virginia's Secretary of State Donald] Kersey said.").

51. *2020 Election Security*, *supra* note 10, at 6 (opening statement of Juan E. Gilbert) ("Representative democracy only works if all eligible citizens can participate in elections, have their ballots accurately cast, counted, and tabulated, *and be confident that their ballots have been accurately cast, counted, and tabulated*." (emphasis added)).

52. Breedon & Bryant, *supra* note 1, at 984 ("Elections succeed in their purpose of resolving differences and conferring legitimacy only to the extent that they enjoy public confidence."); *see also 2020 Election Security*, *supra* note 10, at 7 (opening statement of Matt Blaze) ("Errors in unofficial or final tallies can cast doubt on the legitimacy of entire elections.").

53. Zetter, *supra* note 22 ("The ballot box is the foundation of any democracy. It's not too grand to say that if there's a failure in the ballot box, then democracy fails.").

54. Representative J. Luis Correa stated the problem colorfully: "[R]eally in these elections, the issue is trust. If you wake up Wednesday morning and somebody fried your software system and there are questions [about] the validity of those election results, we are going to have major challenges to our democracy in this country." *DHS's Progress in Securing Election Systems and Other Critical Infrastructure Before the H. Comm. on Homeland Sec.*, 115th Cong. 76 (2018) [hereinafter *DHS's Progress*] (question from Rep. J. Luis Correa), https://www.govinfo.gov/content/pkg/CHRG-115hhrg33942/pdf/CHRG-115hhrg33942.pdf
[http://web.archive.org/web/20200422200645/https://www.govinfo.gov/content/pkg/CHRG-115hhrg33942/pdf/CHRG-115hhrg33942.pdf]; Breedon & Bryant, *supra* note 1, at 984; Zetter, *supra* note 22 ("If the people don't have confidence in the outcome of an election, then it becomes difficult for them to accept the policies and actions that pour forth from it.").

electronic tampering, these methods serve to increase public confidence in election outcomes.[55]

III. SURVEY OF MAJOR ISSUES RELATING TO ELECTION SECURITY

Despite the near-uniform best practices recommendations from cyber and election security experts, numerous election jurisdictions across the country continue to use voting systems that do not comply with those recommendations.[56] For example, in testimony before the Senate Select Committee on Intelligence in 2018, Amy Cohen, Executive Director of the National Association of State Election Directors, explained that a number of states have not adopted voting systems that use paper ballots or that produce a voter-verified paper audit trail; therefore, any recount would rely solely on the accuracy of the voting machines' electronically stored information.[57] The Brennan Center for Justice estimates that in the 2020 general elections, approximately sixteen million voters, representing twelve percent of voters, will cast their votes using paperless systems.[58]

The types of voting system problems present in these jurisdictions vary, and new difficulties are continually arising. Accordingly, a

---

55. *Post-Election Audits*, *supra* note 26. Post-election audits also increase voter confidence by deterring fraud and corruption and by acting as a systemic corrective by identifying programming or other bugs or errors in the system. *Id*. These observations mirror the experience of voting integrity advocates. *See, e.g.*, Matt Vasilogambros, *A Voter's Guide to Election Security*, PEW (Nov. 1, 2018), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/11/01/a-voters-guide-to-election-security [http://web.archive.org/web/20200422201156/https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2018/11/01/a-voters-guide-to-election-security] ("'Audits empower people to feel like their vote counted and feel engaged in the process,' said Aquene Freechild, co-director of nonprofit Public Citizen's Democracy Is For People Campaign. 'Voters in states and counties that lack audits cannot be sure their votes were fully counted.'").

56. Halpern, *supra* note 40. Although most jurisdictions relying on paperless systems are using older machines, the Houston Chronicle reported that two counties in Texas bought new paperless systems within the past two years. *2020 Election Security*, *supra* note 10, at 8 (2020) (statement of Elizabeth L. Howard, Counsel, Democracy Program, Brennan Ctr. for Justice).

57. *Open Hearing: Election Security Before the Senate Select Comm. on Intelligence*, 115th Cong. 59 (2018) [hereinafter *Open Hearing*] (statement of Amy Cohen, Executive Director, National Association of State Election Directors), https://www.intelligence.senate.gov/sites/default/files/hearings/CHRG-115shrg29480.pdf [https://web.archive.org/web/20200617055708/https://www.intelligence.senate.gov/sites/default/files/hearings/CHRG-115shrg29480.pdf.].

58. *2020 Election Security*, *supra* note 10 (statement of Elizabeth L. Howard, Counsel, Democracy Program).

complete catalog of vulnerabilities would be both impractical and almost immediately out of date. A brief snapshot of the major issues, however, should suffice to illuminate the broader challenges to election security across jurisdictions.[59]

A. Voting Machines with "End-of-Life" Software

In some instances, voting systems are insecure because they are so outdated that the latest security software does not offer patches or updates for them.[60] "Many older voting systems rely on outdated operating systems, like Windows XP and 2000, which are no longer supported . . . . Unsupported software is riskier from a security perspective, since it does not receive regular security updates and is vulnerable to new methods of attack."[61] Some of these operating systems for additional voting systems are expected to reach "end-of-life" in 2020, and they will no longer be supported with software patches.[62] Outdated software in voting systems is no mere inconvenience. Indeed, the Department of Homeland Security has identified the possibility of "malicious actors exploiting unpatched software" as one of various methods of attack on, or vectors of, intrusion into our election systems.[63]

B. Aging Voting Machines

In 2020, election jurisdictions across the country are relying on aging, and potentially unreliable, electronic voting machines that either are not designed to produce a paper backup or, as occurred in Georgia in 2018, are at risk of malfunctioning in the production of a paper record.[64]

---

59. *See infra* Parts III.A–G.

60. *Defending Our Democracy*, *supra* note 45 (opening statement of Alex Padilla).

61. Lawrence Norden & Christopher Famighetti, *Aging Voting Machines Threaten Election Integrity*, BRENNAN CTR. FOR JUST. (Apr. 4, 2016), https://www.brennancenter.org/our-work/analysis-opinion/aging-voting-machines-threaten-election-integrity [http://web.archive.org/web/20200422203302/https://www.brennancenter.org/our-work/analysis-opinion/aging-voting-machines-threaten-election-integrity].

62. Tami Abdollah, *New Election Systems Use Vulnerable Software*, ASSOCIATED PRESS (July 13, 2019), https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1 [http://web.archive.org/web/20200422203525/https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1].

63. *DHS's Progress*, *supra* note 54 (questions from Hon. John Katko for Christopher C. Krebs).

64. Jessica Huseman, *The Market for Voting Machines Is Broken. This Company Has Thrived in It.*, PROPUBLICA (Oct. 28, 2019, 2:20 PM), https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it

According to the Executive Director for the National Association of State Election Directors, Amy Cohen, "[m]any jurisdictions purchased their current voting equipment with Federal funds received under the Help American Vote Act of 2002, meaning that the equipment and software often predate parts of our lives that we now take for granted, such as smartphones."[65] Additional details from the front lines, as it were, are sobering. Secretary of State for the State of California Alex Padilla testified to the House Committee on Homeland Security that election officials routinely resort to online purchases of replacement parts for voting systems that are so old that their manufacturers no longer support them.[66]

For example, although Louisiana is in the process of transitioning to voting machines that produce a paper record, the purchase of new machines has been delayed because of a challenge to the procurement process.[67] Accordingly, Louisiana expects to use its older, fully electronic voting machines, known as direct recording electronic (DRE) voting machines, which produce no paper backup. Unlike Louisiana, which has plans to replace its aging machines, some other election jurisdictions with aging or vulnerable voting systems are not as far along, and some—mostly poor and rural localities—have no plans at all to transition away from paperless systems primarily because they lack the resources to do so.[68]

Lack of adequate funding is often cited as the primary barrier to replacing aging or vulnerable voting machines with voting systems that

---

[http://web.archive.org/web/20200422210421/https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it] (describing older computerized machines that did not produce paper backups in an election in which the electronic ballots of more than 150,000 voters "inexplicably" did not include votes cast for the lieutenant governor's race and noting that the absence of a paper record prevented officials from determining whether the errors were human or mechanical); *see also Open Hearing*, *supra* note 57 (statement of Amy Cohen, Exec. Dir., Nat'l Ass'n of State Election Dirs.) ("Aging voting equipment has been at the forefront for election officials for years. The Presidential Commission on Election Administration report, released in 2013, highlighted the impending crisis in voting technology.").

65. *Open Hearing*, *supra* note 57 (statement of Amy Cohen, Exec. Dir., Nat'l Ass'n of State Election Dirs.).

66. *Defending Our Democracy*, *supra* note 45 (opening statement of Alex Padilla).

67. Sam Karlin, *Amid Election Fears, La. Uses Aging Voting Machines*, DAILY COMET (Feb. 9, 2020, 3:59 PM), https://www.dailycomet.com/news/20200209/amid-election-fears-la-uses-aging-voting-machines [http://web.archive.org/web/20200422210816/https://www.dailycomet.com/news/20200209/amid-election-fears-la-uses-aging-voting-machines].

68. *2020 Election Security*, *supra* note 10, at 9 (statement of Elizabeth L. Howard, Counsel, Democracy Program, Brennan Ctr. for Justice).

use voter-verifiable paper records.[69] And jurisdictions that cannot afford to replace or repair their outdated voting machines are forced to rely on them "well past their intended use date."[70] These machines are particularly vulnerable to hacking or tampering by malign actors,[71] and they are more susceptible to system or mechanical failure than are new machines. In either event, the absence of a paper record could mean that votes would not be tallied or incorporated into the final tabulation at all.[72]

In her opening statement at an oversight hearing on the U.S. Election Assistance Commission, held by the Senate Committee on Rules and Administration in May 2019, Senator Amy Klobuchar highlighted concerns about the risk of foreign attacks on aging electronic voting systems,[73] and her concerns apply with equal force to system or

---

69. *Open Hearing*, *supra* note 57 (statement of Amy Cohen, Exec. Dir., Nat'l Ass'n of State Election Dirs.) ("Without additional funding, jurisdictions cannot afford to purchase new technology."); *see also* Wogan, *supra* note 10.

70. Ben Buchanan & Michael Sulmeyer, Paper, *Hacking Chads: The Motivations, Threats, and Effects of Electoral Insecurity*, BELFER CTR. FOR SCI. & INT'L AFF. 14 (Oct. 2016), https://www.belfercenter.org/sites/default/files/files/publication/hacking-chads.pdf [http://web.archive.org/web/20200422211512/https://www.belfercenter.org/sites/default/files/files/publication/hacking-chads.pdf]. More recently, Secretary of State for the State of California Alex Padilla confirmed that the voting systems in use in many jurisdictions are "at or beyond life expectancy." *Defending Our Democracy*, *supra* note 45 (prepared statement of Alex Padilla).

71. RUSSIAN ACTIVE MEASURES, *supra* note 11 ("Aging voting equipment, particularly voting machines that had no paper record of votes, [are] vulnerable to exploitation by a committed adversary.").

72. Karlin, *supra* note 67.

73. *Oversight of the U.S. Election Assistance Commission Before the S. Comm. on Rules and Admin.*, 116th Cong. 2 (2019) [hereinafter *Oversight of the EAC*] (opening statement of Sen. Amy Klobuchar), https://www.hsdl.org/?abstract&did=830775 (follow "[open pdf – 17MB]" hyperlink). Senator Ron Wyden expressed similar concerns approximately a year earlier in his opening statement at the Senate Committee on Rules and Administration hearing on Election Security Preparations held over two days on June 20, 2018, and July 11, 2018:

> According to the latest numbers, at least [forty-four] million Americans, and perhaps millions more, have no choice but to use insecure voting machines that make hackers and foreign governments salivate. . . . Five states exclusively use voting machines that do not produce a paper trail. The only record of the votes cast is a digital record, which could be hacked and which is impossible to audit reliably. That strikes me as a prescription for disaster.

Election Security Preparations Before the S. Comm. on Rules and Admin., 115th Cong. 132 (July 11, 2018) [hereinafter *Election Security Preparations*] (opening statement of Senator Ron Wyden), https://www.hsdl.org/c/ (search "election security preparations"; under the "Election Security Preparations, Hearings Before the Committee on Rules and Administration" heading, follow the "Open resource [pdf]" hyperlink).

mechanical malfunction.[74] In that statement, Senator Klobuchar called particular attention to the electronic voting systems in the forty states where the then-in-use machines were at least a decade old.[75] She also noted the absence of a paper ballot or adequate paper backup in twelve states and pointed to the absence of statewide audit requirements in sixteen states.[76] Emphasizing the uncertainty that such systems may potentially generate in the event of election irregularities, Senator Klobuchar's comments reflect an underlying concern about the broader implications of conducting elections with unreliable electronic voting systems that generate only a partial paper record or no paper record at all—namely that the actual outcome of a major election might be both unknown and unknowable,[77] thereby potentially casting doubt on the legitimacy of the election itself and fueling the erosion of voter confidence.[78]

C. The Purchase of New Voting Machines That Have Glitches

As technology develops, so, too, do computerized voting machines. Unfortunately, however, having the most recent vintage does not ensure the error-free execution of an election. In fact, in certain instances, these newer voting machines are, according to experts, even less secure than older models, and they are also more expensive.[79]

---

74. Karlin, *supra* note 67 ("Old equipment tends to fail at higher rates, . . . making malfunctioning machines a bigger concern than hackers." (citing Edgardo Cortes, Election Sec. Advisor to the Brennan Ctr. for Justice)).

75. *Oversight of the EAC*, *supra* note 73, at 2 (opening statement of Sen. Amy Klobuchar).

76. *Id.*

77. *Id.* ("[I]f something happened in a closed [sic] state or in one state, an entire Presidential election could be up in the air and we would not be able to prove what happened if we had no backup paper ballots.").

78. *Id.* ("[W]e know that one hack in one county in one state will jar people's confidence.").

79. Although many security experts believe that paper ballots are the most reliable, as well as the cheapest, method to vote, election officials are continuing to utilize digital voting methods. For example:

> [M]any state and local jurisdictions . . . are buying a new generation of computerized voting machines ahead of the 2020 presidential election that security experts say are less secure and cost more—about [twenty-four dollars] per voter, compared with [twelve dollars] per voter in jurisdictions using a mix of the two systems . . . .

Karkitay Mehrotra & Margaret Newkirk, *Expensive, Glitchy Voting Machines Expose 2020 Hacking Risks*, BLOOMBERG (Nov. 8, 2019), https://www.bloomberg.com/news/articles/2019-11-08/expensive-glitchy-voting-machines-expose-2020-hacking-risks

One such new voting machine—a touchscreen device for recording votes that also provides a paper record of votes cast for use in post-election audits—used in a Pennsylvania county for an election held in November 2019 malfunctioned so badly and caused so many votes to disappear that election officials removed the paper records stored within the machines to conduct an immediate re-count.[80] Troublingly, neither the voting machine vendor nor the election officials overseeing the election have been able to ascertain the cause of the malfunction.[81] More troublingly, at least one computer security expert believes that the paper trail generated by the voting machine, which uses touchscreen entry rather than hand-marked paper ballots for voter selection of candidates, does not provide a reliable record that accurately reflects voters' chosen candidates.[82]

D. New Forms of Voting, Vote-Tallying, and Vote-Reporting Technology

As if problems with existing technology were not enough, the 2020 election cycle has introduced new vulnerabilities with the use of online apps by some jurisdictions. The Democratic Caucuses in Iowa encountered difficulty with an app that was designed to report results from individual precincts to the Iowa Democratic Party.[83] A coding error in the app, however, resulted in the reporting of incorrect data, throwing

---

[http://web.archive.org/web/20200422214540/https://www.bloomberg.com/tosv2.html?vid=&uuid=9c235ce0-84e2-11ea-96c4-95d3957c2a6e&url=L25ld3MvYXJ0aWNsZXMvMjAxOS0xMS0wOC9leHBlbnNpdmUtZ2xpdGNoeS12b3RpbmctbWFjaGluZXMtZXhwb3NlLTIwMjAtaGFja2luZy1yaXNrcw==].

80. *Id.* Bloomberg reported that the paper-record recount revealed that one candidate had won his or her race by approximately 1000 votes, even though the voting machine's electronic record showed the candidate had received only a total of fifteen votes. *Id.* In another instance, malfunctioning computerized voting machines used in a local election in Indiana in 2018 raised the question of whether some voters had cast more than one ballot. Huseman, *supra* note 64.

81. Mehrotra & Newkirk, *supra* note 79.

82. *Id.* (quoting University of California-Berkeley statistics professor Philip Stark: "There's no reason to believe that the paper trail generated by the [voting machine used in the Pennsylvania county's election] accurately reflects voters' selections . . . .").

83. Casey Newton, *The Iowa Caucus Debacle Shows Why Tech and Voting Don't Mix*, VERGE (Feb. 5, 2020, 6:00 AM), https://www.theverge.com/2020/2/5/21122497/iowa-caucus-app-debacle-voting-election-technology [http://web.archive.org/web/20200422214920/https://www.theverge.com/2020/2/5/21122497/iowa-caucus-app-debacle-voting-election-technology].

the outcome into question and causing some to question its legitimacy.[84] In addition, researchers at the Massachusetts Institute of Technology have recently published a report that a mobile voting app used in West Virginia, Colorado, Washington, Oregon, and Utah has basic security flaws that researchers say would allow a cyber intruder to intercept and surreptitiously alter, block, or expose votes as they are transmitted from the smartphone app to the voting company's server—without the voter ever discovering the change.[85] The app, Voatz, was designed to facilitate voting by military and overseas voters and has come under scrutiny by Senator Ron Wyden, who in November 2019 wrote a letter to Secretary of Defense Mark Esper requesting a cybersecurity review of the app.[86]

E. Scattered Adoption of Risk-limiting Audits

Despite its status as a best practice, the post-election risk-limiting audit is not widely used in U.S. elections.[87] Growing awareness of the utility of risk-limiting audits has prompted some movement toward their adoption in scattered precincts throughout the country; nevertheless, few jurisdictions employ them, and fewer still mandate them.[88] According to the National Conference of State Legislatures, only ten states currently mandate or provide options for conducting risk-limiting audits.[89] In four

84. Jason Koebler & Emanuel Maiberg, *Here's the Shadow Inc. App That Failed in Iowa Last Night*, VICE (Feb. 4, 2020, 1:10 PM), https://www.vice.com/en_us/article/y3m33x/heres-the-shadow-inc-app-that-failed-in-iowa-last-night [http://web.archive.org/web/20200422215044/https://www.vice.com/en_us/article/y3m33x/heres-the-shadow-inc-app-that-failed-in-iowa-last-night].

85. *See, e.g.*, AJ Vicens, *Security Researchers Find Flaws in Online Voting System Tested in Five States*, MOTHER JONES (Feb. 13, 2020), https://www.motherjones.com/politics/2020/02/security-researchers-find-flaws-in-online-voting-system-tested-in-five-states/ [http://web.archive.org/web/20200422215656/https://www.motherjones.com/politics/2020/02/security-researchers-find-flaws-in-online-voting-system-tested-in-five-states/]; Kim Zetter, "*Sloppy" Voting Mobile App Used in Four States Has "Elementary" Security Flaws*, VICE (Feb. 13, 2020, 12:42 PM), https://www.vice.com/en_us/article/akw7mp/sloppy-mobile-voting-app-used-in-four-states-has-elementary-security-flaws [http://web.archive.org/web/20200422215456/https://www.vice.com/en_us/article/akw7mp/sloppy-mobile-voting-app-used-in-four-states-has-elementary-security-flaws].

86. Ben Popken, *Smartphone Voting App Needs Security Review, Senator Says*, NBC NEWS (Nov. 8, 2019), https://www.nbcnews.com/tech/security/smartphone-voting-app-needs-security-review-senator-says-n1079151 [http://web.archive.org/web/20200422220025/https://www.nbcnews.com/tech/security/smartphone-voting-app-needs-security-review-senator-says-n1079151].

87. *See Post-Election Audits*, *supra* note 26.

88. *Id.*

89. *Id.*

of those states (Colorado, Nevada, Rhode Island, and Virginia), risk-limiting audits are required by statute.[90] Two states (Georgia and Indiana) are required by statute to conduct risk-limiting audit pilots.[91] The remaining four states (California, Ohio, Oregon, and Washington) allow counties to use methods of post-election audits, including the option of a risk-limiting audit.[92] Additional states, including Michigan, Missouri, New Jersey, Ohio, and Pennsylvania, have indicated an openness to adopting risk-limiting audits in some manner.[93] The scarcity of state statutory requirements or of options for election officials to conduct risk-limiting audits indicates how much more work remains to be done on that front alone, though the method is relatively new and the adoption rate seems to be proceeding apace.[94]

F. Lack of Transparency and Accountability of Voting System Vendors

A potentially more intransigent problem is the lack of transparency and accountability of voting machine vendors, the cyber security practices of which remain opaque to public officials at all levels of government.[95] A report issued by the Brennan Center for Justice highlighted five primary areas in which voting machine vendors lack transparency: internal cybersecurity practices; foreign-entity ownership; personnel security policies and procedures; cybersecurity intrusion response plans and practices; and supply chain security.[96] To address these matters, the Brennan Center report recommended establishing a Technical Guidelines Development Committee to produce vendor certification guidelines, including best practices benchmarks that election

---

90. *Id.* Nevada is conducting pilot audits in 2020 and will require all counties to employ them in 2022. *Id.*

91. *Id.*

92. *Id.*

93. *2020 Election Security*, *supra* note 10, at 11 (prepared statement of Elizabeth L. Howard, Counsel, Democracy Program, Brennan Ctr. for Justice).

94. *Id.* at 10–11.

95. U.S. SENATE SELECT COMM. ON INTELLIGENCE, 115TH CONG., RUSSIAN TARGETING OF ELECTION INFRASTRUCTURE DURING THE 2016 ELECTION: SUMMARY OF INITIAL FINDINGS & RECOMMENDATIONS (2018), https://www.intelligence.senate.gov/publications/russia-inquiry [http://web.archive.org/web/20200422220535/https://www.intelligence.senate.gov/publications/russia-inquiry] ("State, local, territorial, tribal, and federal government authorities have very little insight into the cyber security practices of [election] vendors.").

96. LAWRENCE NORDEN ET AL., A FRAMEWORK FOR ELECTION VENDOR OVERSIGHT: SAFEGUARDING AMERICA'S ELECTION SYSTEMS 5 (Brennan Ctr. for Justice 2019).

vendors must meet in order to be certified by the Election Assistance Commission.[97]

Of the five areas of concern identified by the Brennan Center report, lack of foreign-ownership transparency is most relevant to the core argument of this Article. In recommending that the federal government establish a national structure for ensuring election integrity, the Brennan Center report argued that election vendors should be required to disclose all ownership interests of more than five percent and that "significant" foreign ownership of election system vendors be prohibited.[98] These requirements would serve both election security interests and anti-corruption principles. In addition to protecting against foreign influence over a voting system vendor, mandating disclosure of foreign ownership would limit avenues for corrupting local election authorities' processes and decision-making relating to certification and contracting.[99] The concern here is that, if permitted to continue to operate without such disclosures, vendors—and their relationships with government officials, including vendor-led influence campaigns—will not be subject to the kind of public scrutiny needed to deter public malfeasance, conflicts of interest, and more egregious forms of corruption.[100] In other words, without the proverbial disinfectant of sunlight, officials' decisions about which voting system to buy or what specifications to adopt might be made "in exchange for gifts or special treatment," neglecting the decisions that "would best facilitate free and fair elections."[101] Conversely, mandatory disclosures of and prohibitions on significant foreign ownership would provide the requisite degree of transparency to

---

97. *Id.* at 9 (listing the following areas that the guidelines should cover: "cybersecurity best practices; background checks and other security measures for personnel; transparent ownership; processes for reporting cyber incidents; and supply chain integrity").

98. *Id.* at 11.

99. *Id*. ("Transparency into ownership and control is required for the public to assess whether officials engaged in procurement and regulation have been improperly influenced.").

100. *Id*.

101. *Id*. Brennan Center Counsel Elizabeth L. Howard reiterated these concerns in her congressional testimony before the Committee on House Administration:

> [A]side from concerns with foreign influence and control, lack of insight into election vendor ownership also prevents the public from scrutinizing potential conflicts of interest. Some unscrupulous officials might award vendor contracts in exchange for gifts or special treatment rather than to those who best facilitate free and fair elections.

2020 Election Security, *supra* note 10, at 5–6 (prepared statement of Elizabeth L. Howard, Counsel, Democracy Program, Brennan Ctr. for Justice).

give voters confidence that vendors and election officials are making decisions in the public's interest in free and fair elections rather than the private interests of other actors.[102]

G. Public Officials' Conflicts of Interest

While the Brennan Center report raised the need for transparent foreign ownership disclosures, other potential conflicts, whether financial or political, may also distort public officials' decisions about contracting with voting-machine vendors and a host of related issues, including, for example, vendor oversight and post-election audits.[103] More specifically, public officials' conflicts of interest affecting vendor contracting and oversight as well as audit authorization and supervision, exist in the form of campaign contributions, whether direct or indirect; revolving-door relationships and professional opportunities; gifts and special treatment; and personal political incentives.[104]

As but one example of conflicts presented by campaign contributions, consider the following vignette from Georgia:

> In 2006, a bill requiring a verifiable paper record of each ballot, introduced in the Georgia legislature at the urging of election-integrity advocates, failed after the state's elections director, Kathy Rogers, opposed it. Rogers, of course, later went to work for [voting-machine vendor ES&S]. Election-integrity advocates sued in response, challenging the legality of the state's voting equipment. In the three years that the case wended its way through the courts, where it was eventually dismissed by the Georgia Supreme Court, the new secretary of state, Karen Handel, was found to have received twenty-five thousand dollars in campaign contributions from employees and family members associated with [a] lobbying firm [representing election machine vendors].[105]

---

102. NORDEN ET AL., *supra* note 96, at 11.

103. Breedon & Bryant, *supra* note 1, at 997-98; *see also* Mehrotra & Newkirk, *supra* note 79 ("Familiarity, practicality, professional relationships and campaign money compete with security concerns when purchasing decisions are made.").

104. Breedon & Bryant, *supra* note 1, at 997-1006.

105. Halpern, *supra* note 40 (documenting the relationship of election officials and voting machine lobbyists in Georgia and Delaware). In addition, since 2013, the same vendor has donated tens of thousands of dollars to a partisan political organization. *See id.* Journalist Jane Mayer, in her book, *Dark Money*, calls this "a catchall bank account

For an example involving similarly conflicted revolving-door relationships, consider the following, more recent scenario:

> In 2012, Charles Harper, a sod farmer who had been elected to the Georgia House of Representative a decade earlier, became a registered lobbyist in the office of the Georgia secretary of state, Brian Kemp, where he served as legislative director. At the end of 2017, as Kemp was ramping up his campaign for governor, Harper did not renew his lobbying credentials with the secretary of state. Instead, he registered to lobby for [ES&S]. Around the same time, John Bozeman, then the head of legislative affairs for Georgia's former governor, Sonny Perdue (who is now the Secretary of Agriculture in the Trump Administration), also registered to lobby on behalf of [ES&S]. After Kemp won the governor's race, in November, he named Harper, whose contract with [ES&S] ended in June, 2018, to his transition team. Harper is now [current Governor] Kemp's deputy chief of staff.[106]

In addition to the more common types of conflicts involving campaign contributions and revolving-door relationships, at least one voting machine vendor has introduced a new variety. In 2009, the country's largest manufacturer of voting machines started what it calls an "advisory board" of state election officials and has treated them to trips to vacation destinations, such as New York and Las Vegas, covering the costs of airfare, luxury accommodations, and tickets to live entertainment.[107] In March 2017, David Dove, the Chief of Staff to Georgia's then-Secretary of State Brian Kemp, participated in one such junket to Las Vegas during the very period that his office was seeking to replace all of the state's voting machines.[108] This advisory board relationship, in turn, created additional conflicts of its own. In August 2017, then-Secretary Kemp invited the vendor to operate a pilot version of a new voting system, which would ultimately be the one selected by a commission populated by appointees of then-Secretary Kemp and tasked with recommending which system to adopt to replace the state's current

---

for corporations interested in influencing state laws." JANE MAYER, DARK MONEY: THE HIDDEN HISTORY OF THE BILLIONAIRES BEHIND THE RISE OF THE RADICAL RIGHT 243 (2016).

106. Halpern, *supra* note 40 (documenting the relationship of election officials and voting machine lobbyists in Georgia and Delaware).

107. *Id.*

108. *Id*.

machines.[109] In circumstances calling the commission's independence further into question, the commission cast its final vote recommending the vendor's new system in the same week that Kemp, in his new capacity as Governor-elect, announced his appointment of a lobbyist for the vendor as his Deputy Chief of Staff.[110]

Vendors given the opportunity to conduct pilot projects have a distinct advantage over other vendors for two reasons. First is the simple competitive advantage they have in influencing lawmakers when the latter determine the terms for purchases by election officials. More insidiously, however, vendors can use their preferred position as pilot testers to persuade legislators to specify the terms for vendor bids in such detail that only the pilot vendor's products meet the specifications for procurement.[111]

In many cases involving conflicts of interest of these sorts, election officials disregard the consensus recommendations of cyber-security and election-integrity experts and procure voting machines that are more vulnerable to digital attacks and that lack an adequate voter-verifiable paper record for post-election audits. Moreover, these choices are sometimes made despite demonstrated voter preference for paper ballots.[112]

Finally, personal political motivations may improperly influence a public official's decisions about certification, audits, and recounts in contested elections or elections involving irregularities. Recent incidents illuminate these issues. In the 2016 and 2018 elections, public officials in three states oversaw contested elections in which they themselves were

---

109. *Id.*; Mark Niesse, *Georgia Panel Backs New Voting Machines Over Hand-Counted Paper Ballots*, THE ATLANTA J.-CONST. (Jan. 10, 2019), https://www.ajc.com/news/state--regional-govt--politics/georgia-panel-backs-new-voting-machines-over-hand-marked-paper-ballots/feF5QiAwnzl2l3BK055dtI/ [http://web.archive.org/web/20200422221811/https://www.ajc.com/news/state--regional-govt--politics/georgia-panel-backs-new-voting-machines-over-hand-marked-paper-ballots/feF5QiAwnzl2l3BK055dtI/].

110. Niesse, *supra* note 109.

111. Halpern, *supra* note 40.

112. Rich Garella, *High-Stakes Voting Machine Decision Deserves More Scrutiny*, PHILA. INQUIRER (Jan. 22, 2019, 7:01 AM), https://www.inquirer.com/opinion/commentary/philadelphia-voting-machines-city-commissioners-20190122.html [http://web.archive.org/web/20200422222049/https://www.inquirer.com/opinion/commentary/philadelphia-voting-machines-city-commissioners-20190122.html] (explaining that hand-marked ballots are "the overwhelming majority of those [voters] who attended the [City Commission] hearings [on the selection of a new voting system]"); Niesse, *supra* note 109 (describing preference of "voters who said paper ballots filled out by hand are more secure and less expensive").

not only candidates, but were also the declared victors.[113] In Florida, then-Governor Rick Scott, in a very close race for a U.S. Senate seat—which he ultimately won—recused himself from certifying his own election results only after public pressure, which was partly fueled by a lawsuit against him.[114] The same year, in Kansas, then-Secretary of State for the State of Kansas Kris Kobach, who was running for Governor, oversaw most of the primary race and recused himself only after he had secured victory in his primary race.[115] Finally, in 2018, then-Secretary of State for the State of Georgia Brian Kemp, who was a gubernatorial candidate in an exceedingly close election marred by numerous and pervasive irregularities, attracted public criticism for serving as the top state election official responsible for overseeing his own election.[116] At the time, Georgia did not require a post-election audit,[117] and the votes were cast and stored entirely on paperless machines. Even if the option of a post-election audit had been available, however, Kemp, having won his race, would have had a powerful personal motive for declining to call an audit to further his own political interest in allowing the vote tally to remain unexamined and unchanged.[118]

These examples barely scratch the surface, but they provide important data points for recognizing the scope of the potential problems, particularly as both actual conflicts and the appearance of conflicts can undermine public confidence in election results. More particularly, the public is more likely to harbor suspicions about the legitimacy of an

---

113. Breedon & Bryant, *supra* note 1, at 1003–04 (describing oversight of elections in Georgia, Florida, and Kansas by office-holders who were candidates in races they won).

114. Eliza Newlin Carney, *It's Time to Fix American Elections—Again*, AM. PROSPECT (Nov. 15, 2018), https://prospect.org/power/time-fix-american-elections/ [http://web.archive.org/web/20200422222341/https://prospect.org/power/time-fix-american-elections/].

115. *Id*.

116. No less a light than former President Jimmy Carter called on Kemp to resign his position as Secretary of State and hand oversight of the election to a neutral authority so as "to foster voter confidence in the upcoming election[.]" Letter from Former U.S. President Jimmy Carter to then-Sec'y of State for the State of Ga., Brian Kemp (Oct. 22, 2018), https://apnews.com/02bf11f29ada46d0833be6e3091b0c31 [http://web.archive.org/web/20200422222710/https://apnews.com/02bf11f29ada46d0833be6e3091b0c31]; Emily Dreyfuss, *Georgia Voting Machine Issues Heighten Scrutiny on Brian Kemp*, WIRED (Nov. 6, 2018, 4:54 PM), https://www.wired.com/story/georgia-voting-machine-issues-heighten-scrutiny-brian-kemp/ [http://web.archive.org/web/20200422222507/https://www.wired.com/story/georgia-voting-machine-issues-heighten-scrutiny-brian-kemp/].

117. The state legislature had eliminated the requirement for auditable paper trails in elections in 2002. Halpern, *supra* note 40.

118. Breedon & Bryant, *supra* note 1, at 1003.

election outcome in situations where the public official overseeing or certifying an election has a stake in the results.[119] In addition, the erosion of public trust in election outcomes is more likely where conflicted—or apparently conflicted—officials decline to follow cybersecurity or election-integrity experts' recommendations, or voters' preferences, and they select vendor-promoted systems that are less secure from tampering or hacking by malign actors.[120]

These examples also highlight three important aspects of election integrity that lend themselves well to increased congressional oversight: (1) financial incentives creating conflicts of interest or the appearance of conflicts of interest; (2) personal political incentives creating conflicts of interest or the appearance of conflicts of interest; and (3) revolving-door professional relationships creating conflicts of interest or the appearance of conflicts of interest. Although multiple committees in both houses of Congress have held numerous hearings on election security in the past few years, very little time or attention has been devoted to the first of these issues, and no time or attention has been devoted to the other two. A gap in oversight of this nature, while understandable in light of the complexity and dynamism of the subject writ large, is also unfortunate, especially in light of the informing function of oversight as a means to educate the public on important issues that either are not the current subject of pending legislation or that are the current subject of pending legislation but have not been fully explored or explained in hearings to date.

IV. CONGRESSIONAL OVERSIGHT TO DATE

In the aftermath of the 2016 election, a bright spotlight has been shone on vulnerabilities in our nation's election security, as public officials seek ways to bolster protections against cyber intrusions into voting systems and to minimize the potential for hostile foreign actors to attack our voting systems. In this fraught context, Congress has introduced scores of bills addressing election security, including, to list but a small sampling: House Bill 6188, the "Prevent Election Hacking Act of 2018";[121] House Bill 6093 and Senate Bill 3049 (companion bills

119. *Id*. at 1004.

120. *Id*. at 1005.

121. Prevent Election Hacking Act of 2018, H.R. 6188, 115th Cong. § 2(c)(3), (e), 115th Cong. § 1 (2018) (directing the Department of Homeland Security to create a "bug bounty" program to encourage election officials at the state and local levels and election service providers to work with independent technical experts in identifying "previously unidentified election cybersecurity vulnerabilities").

with identical language in the House and the Senate), both called the "Protecting American Votes and Elections Act of 2018" ("the PAVE Act");[122] and House Bill 6663 and Senate Bill 2261 (bills with similar—but not identical—language in the House and the Senate), both called the "Secure Elections Act";[123] and the Election Vendor Security Act of 2018.[124]

In January 2019, the House introduced and passed a comprehensive election integrity, election security, and anti-corruption bill, House Bill 1, the "For the People Act of 2019."[125] The multi-pronged framework of the For the People Act—among other things—requires the use of paper ballots; imposes a ban on state chief election officials from "participating in federal campaigns"; bars officials from using the power of their office to affect the results of elections; regulates vendors of election systems by establishing cybersecurity and other standards; creates a mechanism to provide grants to states for upgrading to and maintaining election systems, for adopting and using paper ballot systems, and for conducting post-election risk-limiting audits; and establishes an election systems vulnerability "bug bounty" program.[126]

---

122. Protecting American Votes and Elections Act of 2018, H.R. 6093, 115th Cong. (2018); Protecting American Votes and Elections Act of 2018, S. 3049, 115th Cong. (2018). Both versions of the PAVE Act would require the use of paper ballots and post-election risk-limiting audits for all federal elections. H.R. 6093 § 2(1)–(3); S. 3049 § 2(1)–(3).

123. Secure Elections Act, H.R. 6663, 115th Cong. (2018); Secure Elections Act, S. 2261, 115th Cong. (2018). The House and Senate versions of Secure Elections Act contain similar, though not identical, provisions. Both bills would provide grant money for states (1) to acquire and use voting machines that provide a paper record and (2) to conduct post-election audits. The Senate version would require the use of paper ballots, while the House version would allow votes to be cast electronically as long as the voting machine provides a paper record. Both versions would require post-election audits. S. 2261 § 5(d); H.R. 6663; § 5(d)(1)–(2).

124. Election Vendor Security Act, H.R. 6435, 115th Cong. (2018) (requiring election system vendors to be owned and controlled solely by citizens or lawful permanent residents of the United States, to employ cybersecurity best practices, and to report immediately to state and federal authorities any known or suspected cybersecurity breaches).

125. For the People Act, H.R. 1, 116th Cong. (2019). After passage in the House, the bill has stalled in the Senate.

126. *See* H.R. REP. NO. 116-15, at 59 (2019). Since then, both the House and the Senate have seen the introduction of a plethora of additional bills addressing election security issues, many of them with overlapping and redundant provisions. For a partial list, *see e.g.*, Stopping Harmful Interference in in Elections for a Lasting Democracy (SHIELD) Act, H.R. 4617, 116th Cong. (2019) (proposing an amendment to the Federal Election Campaign Act of 1971 to establish a duty to report acts of foreign election influence and to establish a reporting framework for the same; to place limitations on

Both before and after proposing these legislative remedies to secure our elections, the House and the Senate, across various committees and sub-committees, have held numerous hearings on a wide array of election security issues, with testimony from, for instance, Department of Homeland Security officials, Election Assistance Commission commissioners, cyber and election security experts, voting-machine vendors, state and local election officials, and voting integrity/voter advocates. For example, in the Senate, the Select Committee on Intelligence held open hearings on Election Security (March 2018),[127] and on Policy Response to the Russian Interference in the 2016 U.S. Elections (June 2018);[128] and the Committee on Rules and Administration held a hearing on Oversight of the U.S. Election Assistance Commission (May 2019)[129] and on Election Security Preparations (June and July 2018).[130] In the House, the Committee on Homeland Security held hearings on Defending Our Democracy: Building Partnerships to Protect America's Elections (February 2019)[131] and on DHS's Progress in Securing Election Systems and Other Critical Infrastructure (July 2018);[132] the Committee on Oversight and Government Reform held a hearing on Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System (July 2018);[133] and the Subcommittee on National Security of the Committee on Oversight and Reform held a hearing on Securing U.S. Election Infrastructure and

---

political spending by foreign entities; and to prohibit candidates from sharing certain campaign information with specified foreign entities); Securing America's Federal Elections (SAFE) Act, H.R. 2722, 116th Cong. (2019) (proposing funding for and requirements for voting systems, including voter-verified paper ballots and post-election rick-limiting audits) (passed in the House on June 27, 2019, and referred to the Senate (S. 2053) where it was received on June 28, 2019, and referred to the Committee on Rules and Administration); Defending Integrity of Voting Systems Act, S. 1321, 116th Cong. (2019) (proposing criminal prohibition against interference with voting systems under the Federal Computer Fraud and Abuse Act) (passed in the Senate on July 17, 2019, and, as of February 25, 2020, awaits action in the House); Protecting American Votes and Elections Act of 2019, S. 1472, 116th Cong. (2019) (an earlier version of this bill, Protecting American Votes Act of 2018, S. 3049, 116th Cong. (2019), was introduced in the Senate in a previous session of Congress, but was not enacted.).

127. *Open Hearing*, *supra* note 57.

128. *Id.*

129. *Oversight of the EAC*, *supra* note 73.

130. *Election Security Preparations*, *supra* note 73.

131. *Defending Our Democracy*, *supra* note 45.

132. *DHS's Progress*, *supra* note 54.

133. *Cyber-securing the Vote: Ensuring the Integrity of the U.S. Election System Before H. Comm. on Oversight and Gov't Reform*, 115th Cong. (2018) [hereinafter *Cyber-Securing the Vote*].

Protecting Political Discourse (May 2019).[134] Most recently, in January 2020, the House Committee on House Administration heard testimony from election vendors and experts in election integrity and cybersecurity.[135]

V. THEMES EMERGING FROM CONGRESSIONAL OVERSIGHT

In these hearings, several themes have emerged. The following are among the most relevant for purposes of this Article. First is the need for ongoing information-sharing between federal agencies and state election officials about cyber intrusions and other security breaches. At present, the Department of Homeland Security offers assistance to state election officials in multiple forms, including security advice, intelligence information, technical support, response-planning for cyber incidents, best practices for risk management, and on-site risk and vulnerability assessments.[136] These services are optional; no state is required to partake of them.[137] The voluntary nature of DHS's services finds support in Congress amid bipartisan concerns about federalism and the need to foster collaborative relationships in an area traditionally reserved to the states, as is the responsibility for conducting elections.[138]

The second theme is agreement among vendors, cyber security experts, and election integrity specialists, that the federal government should provide guidance on best practices for securing election systems.[139] Experts in election security have long decried the lack of federal oversight in this area.[140] During the House Committee on House

134. *Securing U.S. Election Infrastructure and Protecting Political Discourse Before H. Subcomm. on Nat'l Sec. (Comm. on Oversight and Reform)*, 116th Cong. (2019). Congressional committees and subcommittees have held a host of additional hearings on the subject of election security. This Article highlights those that include discussion of cybersecurity of election systems or of election officials' potential conflicts of interest and for which, with one exception, transcripts have been made public.

135. *2020 Election Security*, *supra* note 10.

136. *Open Hearing*, *supra* note 57 (statement of Sec. Kirstjen Nielsen, Dep't of Homeland Sec.).

137. *Id*.

138. *See, e.g*., *id.* (statement of Sen. James Lankford) ("The decentralization of our election systems is exceptionally important, and one of the key aspects that we've tried to work through on recommendations is maintaining the states' control of elections."); *Id.* (statement of Sen. Mark Warner) ("I'm sympathetic to the notion that you've got to have this collaborative relationship with the states, and I think the recommendations put forward by our members don't want to take over the federal elections.").

139. *2020 Election Security*, *supra* note 10.

140. NORDEN et al., *supra* note 96, at 9–10 (recommending the creation of a federal Technical Guidelines Development Committee to "craft cybersecurity best practices that

Administration's election security hearing earlier this year, election-system vendors testified that they would actively welcome federal guidelines and best practices, including greater regulation,[141] but that public position is at least in some tension with efforts by their lobbyists to weaken bills that would require some of those best practices.[142] Vendors' current testimonies are also in tension with their previous reluctance even to answer questions posed by Senator Ron Wyden about their cyber security practices[143] or to appear voluntarily when reportedly

---

include not only equipment- and service-related offerings but also internal information technology practices, cyber hygiene, data access controls, and the like").

141. *See* Emily Previti, *Congressional Hearing on Election Security: Top Takeaways*, PA POST (Jan. 10, 2020, 4:44 PM), https://papost.org/2020/01/10/congressional-hearing-on-election-security-top-takeaways/ [http://web.archive.org/web/20200423142944/https://papost.org/2020/01/10/congressional-hearing-on-election-security-top-takeaways/]; *see also 2020 Election Security*, *supra* note 10.

142. Derek Hawkins, *The Cybersecurity 202: Why the Latest Election Security Bill Is Stalled in Congress*, WASH. POST (Aug. 31, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/31/the-cybersecurity-202-why-the-latest-election-security-bill-is-stalled-in-congress/5b8829fb1b326b3f31919eaa/ [http://web.archive.org/web/20200423143112/https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/08/31/the-cybersecurity-202-why-the-latest-election-security-bill-is-stalled-in-congress/5b8829fb1b326b3f31919eaa/] (explaining why the bipartisan Secure Elections Act appears to have died in the Senate Committee on Rules and Administration); Derek B. Johnson, *Senators Duel Over Audit Requirements in Election Security Bill*, FCW (Aug. 21, 2018), https://fcw.com/articles/2018/08/21/election-paper-ballots-bill.aspx [http://web.archive.org/web/20200423143303/https://fcw.com/articles/2018/08/21/election-paper-ballots-bill.aspx] (reporting that comments from some senators indicated that "state election officials and voting machine manufacturers have been putting increasing pressure on lawmakers to water down the bill").

143. Derek B. Johnson, *Report: Election Vendors Need More Federal Oversight*, FCW (Nov. 12, 2019), https://fcw.com/articles/2019/11/12/brennan-election-vendor-oversight.aspx [http://web.archive.org/web/20200423143624/https://fcw.com/articles/2019/11/12/brennan-election-vendor-oversight.aspx] ("For years, election security specialists have criticized the outsized role that a handful of private vendors have played in the way U.S. election technology is managed and administered. These companies have historically spurned calls to conduct independent testing of their equipment and threatened legal action against security researchers who point out vulnerabilities."); *see also Open Hearing*, *supra* note 57 (statement of Sen. Ron Wyden) (noting that at the time of his statement, "[forty-three] percent of American voters use voting machines that researchers have found have serious security flaws, including backdoors" and that the voting-machine vending companies "won't answer basic questions about their cyber security practices, and the biggest companies won't answer any questions at all"); *see also 2020 Election Security*, *supra* note 10 (statement by Elizabeth L. Howard) ("[This hearing] will be the first congressional hearing at which representatives of the three primary voting systems

requested to do so by the Senate Committee on Rules and Administration in 2018.[144] Nevertheless, the vendors' present public indications of a desire for greater oversight suggest a change in position.[145]

A third theme that has emerged during the congressional oversight hearings on election security is the problem presented by supply chain vulnerabilities.[146] Professor Matt Blaze explained that hostile foreign intelligence operatives have the capacity to exploit such vulnerabilities in equipment or components, before they are shipped to vendors and then to election officials, by extracting confidential source code, for example, or securing clandestine access to equipment.[147] Jake Braun, Executive Director of the Cyber Policy Initiative, testified last year that the supply chain for voting-machine hardware and software is global, and the several components are manufactured in adversarial nations.[148] His testimony provides additional details on the election security implications of an insecure supply chain: "[N]ation-state hackers could put malware on firmware for these machines and other devices used to implement elections, and hack whole classes of machines all across the United States, all at once . . . ."[149] During an oversight hearing in 2018,

---

vendors will appear jointly to publicly answer questions about their ownership, operations and conduct, which impact the security of our democracy.").

144. Letter from Nat'l Election Def. Coal. et al. to S. Comm. on Rules and Admin. & S. Comm. on House Admin. (Aug. 26, 2019), https://www.lwv.org/sites/default/files/2019-08/Congressional.hearing.vendors-2_1.pdf?utm_source=LeagueUpdate&utm_medium=email&utm_campaign=082919 [https://web.archive.org/web/20200622152217/https://www.lwv.org/sites/default/files/2019-08/Congressional.hearing.vendors-2_1.pdf] (asking those committees to schedule additional hearings on election security and to require vendors' appearance and stating that in 2018, when several vendors were invited to testify before the Senate Committee on Rules and Administration, only one of the top three vendors appeared).

145. It will bear watching whether the vendors' lobbyists will continue to make efforts to dissuade lawmakers from enacting legislative requirements in this regard or to shape requirements in a way that lack force or effect.

146. *See, e.g.*, *2020 Election Security*, *supra* note 10 (statement of Elizabeth L. Howard) (comparing the requirements for supply chain integrity and security standards for Department of Defense contractors with those of the election vendor industry and observing that the election vendor industry lacks any such requirements).

147. *Id.* at 13 (opening statement of Matt Blaze).

148. *Defending Our Democracy*, *supra* note 45 (statement of Jake Braun).

149. *Id*. (noting that foreign nation-states are known to "hack parts in the supply chain all the time"). As Professor Blaze notes, however, a malign actor need only disrupt an election in order to create doubt about the legitimacy of an election result, and so even if no results were in fact compromised, the goal of sowing chaos and undermining democracy can be achieved through exploitation of supply chain vulnerabilities. *2020 Election Security*, *supra* note 10, at 13 (opening statement of Matt Blaze). In her statement, Elizabeth Howard pointed to a separate but related vector of attack through the

then-Secretary of the Department of Homeland Security Kirstjen Nielsen, in response to an inquiry from Senator Mark Warner, acknowledged the problem and testified that DHS had initiated a voluntary supply chain program for voting-machine vendors to help vendors recognize potential vulnerabilities of the components in the machines they sell in the U.S. market.[150]

Another major theme that the oversight hearings highlighted is the need for increased and ongoing federal funding for states to obtain and maintain secure voting systems, to conduct post-election audits, and to retain qualified cybersecurity staff. Again and again, witnesses emphasized that the election security demands placed upon state and local election officials require both more—and more reliable—funding, not only in the short-term, but also as a regular part of the federal budget. For example, a letter from a bipartisan group of twenty-one State Attorneys General, entered into the record for a 2018 House Committee on Oversight and Administration hearing on the cybersecurity of elections, expressed the group's need for additional funding to ensure the integrity of the nation's election system: "We are concerned that many states lack the resources and tools they need to protect the polls. Additional funding for voting infrastructure will not only allow States to upgrade election systems but will also allow for a comprehensive security risk assessment."[151] In the same hearing, Ricky Hatch, County Auditor for Weber County, Utah, testified that congressional omnibus funding had been helpful in advancing local governments' efforts to upgrade aging election equipment and to improve cybersecurity defenses but that combatting cyber threats would require "a dedicated, predictable Federal funding stream" for local governments.[152] After the renewed national attention on the need to ensure the security of our election

---

supply chain: the potential for a corrupt employee to engage in malicious conduct affecting hardware or software. Although her statement focuses on vendor employees, the same logic applies to the employees of contractors throughout the supply chain. Thus, election integrity can be undermined by a malign insider, as well as a hostile foreign nation. *Id.* at 5 (statement of Elizabeth L. Howard) ("If an employee of a major election vendor were vulnerable to bribery or other improper influence, they could severely impact election integrity and public confidence by undertaking malicious acts against their employer.")

150. *Open Hearing*, *supra* note 57 (statement of Sec. Kirstjen Nielsen, Dep't of Homeland Sec.).

151. *Cyber-Securing the Vote*, *supra* note 133 (letter for the record from twenty-one State Att'ys Gen., submitted by Ranking Member Elijah E. Cummings).

152. *Id.* (statement of Ricky Hatch) (explaining that county officials work daily, year-round, to protect against cyber intrusions and other security threats that could undermine the integrity of an election).

systems, Congress authorized $380 million for that purpose in 2018 and another $425 million in December 2019.[153] The Secretary of State for the State of California stated bluntly: "Let's be honest, elections are underfunded and are often a low priority for Federal, State, and local governments."[154] He, too, called for "consistent Federal support for election security and administration" and for increases in such funding.[155] In her testimony earlier this year, Elizabeth L. Howard told members of the House Committee on House Administration that Congress would need to allocate "consistent funding for election security" to enable states to implement best practices.[156]

Finally, and most pertinently for purposes of this Article, a theme that received some, but not enough, attention is that of potential conflicts of interest (or the appearance of conflicts) involving vendors and government officials. Most of the testimony relating to conflicts of interest or other corrupt conduct by election officials focused on the lack of transparency about ownership of voting-system vendors, but little attention was explicitly given to the ways in which foreign ownership of voting-machine vendors could compromise election security by improperly influencing public officials who are responsible for decision-making relating to procurement and regulation of voting systems.[157] An additional conflicts-related gap in congressional oversight hearings includes fulsome inquiry into campaign contributions by voting system

153. Gopal Ratnam, *Voting Machine Makers Open to Congressional Oversight*, GOV'T TECH. (Jan. 10, 2020), https://www.govtech.com/security/Voting-Machine-Makers-Open-to-Congressional-Oversight.html [http://web.archive.org/web/20200423145355/https://www.govtech.com/security/Voting-Machine-Makers-Open-to-Congressional-Oversight.html].

154. *Defending Our Democracy*, *supra* note 45 (statement of Alex Padilla).

155. *Id*.

156. *2020 Election Security*, *supra* note 10, at 14 (statement of Elizabeth L. Howard, Counsel, Democracy Program, Brennan Ctr. for Justice). Howard also argues in favor of meaningful congressional oversight over federal funding allocated for election security in 2020. *Id*. at 12. In a 2019 report on election security costs, the Brennan Center for Justice conservatively estimated that it would cost $834 million over five years to replace paperless and older paper-based voting machines to conduct post-election, risk-limiting audits, excluding estimates for protecting voter registration infrastructure and additional state and local cybersecurity assistance. Lawrence Norden & Edgardo Cortes, *What Does Election Security Cost?*, BRENNAN CTR. FOR JUST. (Aug. 15, 2019), https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost [https://web.archive.org/web/20200604084152/https://www.brennancenter.org/our-work/analysis-opinion/what-does-election-security-cost].

157. *See supra* Part II; *see also 2020 Election Security*, *supra* note 10, at 5–6 (statement of Elizabeth L. Howard, Counsel, Democracy Program, Brennan Ctr. for Justice).

vendors. During one hearing, Representative Jamie Raskin asked the three major vendors about their campaign contribution practices.[158] One answered that its high-level officers were prohibited from making direct campaign contributions, but that that prohibition did not apply to its lobbyists; one responded that it prohibited all employees from making such contributions, but that it did hire lobbyists to advance its interests; and one stated that its lobbying activities were limited to "self-education" with local officials. In a follow-up question, Representative Raskin asked one vendor, ES&S, to respond to public reports that Louisiana Governor Bel Edwards cancelled a procurement contract with another vendor after ES&S raised objections and that ES&S's lobbyist donated more than $13,000 to Louisiana Edwards. Testifying on behalf of ES&S, Tom Burt explained that his company had objected to the procurement specifications, which were tailored to only one particular vendor, because they effectively ruled out all competing vendors. This line of inquiry should be pursued in greater detail in future oversight hearings, both because it implicates the potentially corrupt practice of writing procurement specifications to exclude all but a favored vendor and because it implicates potential conflicts of interest by election officials who may be beholden to campaign contributors.

Additional areas of inquiry relating to corruption and conflicts of interest which seem thus far to have garnered little oversight attention and which warrant a great deal more, include the following: first is the potential for conflicts of interest (and the appearance of conflicts of interest) resulting from election officials' membership on vendors' advisory boards that cover those officials' expenses for high-end travel to vacation destinations and other perquisites.[159] Second are the revolving-door relationships that exist between government positions, vendors' lobbyists, and vendors themselves. These relationships raise all manner of red flags pertaining to conflicts of interest or the appearance thereof, but they are seldom subject to regulation or oversight.[160] Moreover, potentially conflicted relationships may transcend the normal revolving-door type. For example, Donald Palmer, a former state-election administrator in two states, currently serves as a commissioner on the U.S. Election Assistance Commission (EAC), the federal organization responsible for certifying election equipment, after having previously served on the advisory board for one of the largest voting-machine

158. *2020 Election Security*, *supra* note 10 (question of Rep. Jamie Raskin).

159. See *supra* Part II.

160. *See* Breedon & Bryant, *supra* note 1, at 1016 (arguing for state-level regulation of revolving-door relationships).

vendors.[161] Although this observation is in no way intended to insinuate untoward decision-making about election equipment certification by the EAC or any of its commissioners, a commissioner's past membership on an advisory board known to provide luxury trips for its members should be disclosed during oversight hearings pertaining to vendor conduct.

Last, is the potential for personal political conflicts by public officials who are responsible for overseeing the election integrity of races in which they themselves are candidates. To date, congressional hearings have paid little attention to personal political conflicts or the appearance of conflicts that arise when candidates for any public office are also election officials who are purchasing insecure equipment, overseeing vote tallies, and conducting or calling for audits or recounts of their own races.[162]

As the foregoing discussion suggests, more—indeed, much more—oversight is needed in these areas because members of the public should have information about the vectors for corrupt or conflicted decision-making by government official relating to election security practices, and if past experience provides any indication, at least some of this information is more likely to come to light in the context of legislative oversight hearings.

VI. THE PROMISE OF CONGRESSIONAL OVERSIGHT AS A SOLUTION

The serious vulnerabilities and impediments to the election system's correction detailed above[163] cry out for solution. A "federal fix" could take at least two distinct, though not incompatible, forms. First, Congress could respond with command and control legislation, directing the adoption of the best practices that analysts have urged, too often in vain, upon state and local election officials. Alternatively, Congress could employ its oversight authority to spur those same officials to action. For reasons both theoretically pure and brutally practical, oversight seems the superior path.

Giving priority to the loftier rationales, we note that the United States has from its founding devolved authority over the administration of federal elections to state and local authorities.[164] The wisdom of this

161. Halpern, *supra* note 40.

162. *See supra* Parts III.F–G; notes 157–61 and accompanying text.

163. *See also* Breedon & Bryant, *supra* note 1.

164. *See* U.S. CONST. art. 1, § 4 ("The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators"); *see also* Justin Weinstein-Tull, *Election Law*

allocation has largely been borne out in the ensuing centuries. State and local control of elections has permitted adaptation to local circumstances and cultures,[165] which has strengthened community involvement in politics and very likely enhanced voter turnout as well.[166] This devolution has also provided an important vector for the realization of the Constitution's "political safeguards of federalism" at the same time it has served as an engine for enhancing the fitness and facilitating the regeneration of political parties.[167] More basically, but perhaps most importantly, "decentralization . . . makes it harder for any single interest to 'steal' an election."[168] Drifting even further from the theoretical to the practical, the fact of local control is also at present, for better or worse, a deeply entrenched aspect of American political life that generates its own inertia opposing congressional adoption of sweeping, top-down reforms.

To that ever-present inertia must be added the even more real-politique observation that, in an election year that coincides with a global pandemic and a divided Congress, enactment of substantive legislation of any sort, let alone bills that tinker with the mechanisms for exercising the franchise, is exceedingly unlikely. Putting these observations together, the conclusion seems overdetermined. A federal legislative fix imposing uniformity in an important aspect of election administration would run counter to a long-standing and commendable commitment to local control of such matters. And it seems all but impossible as a political

---

Federalism, 114 MICH. L. REV. 747, 752 (2016) (noting that "[e]lections are themselves 'hyperfederalized'; that is, many key election decisions are made at the local level" and that "[t]he Constitution initiates decentralization by placing the primary responsibility for holding elections with states.").

165. *See, e.g.*, PRESIDENTIAL COMM'N ON ELECTION ADMIN., THE AMERICAN VOTING EXPERIENCE 9 (2014). The report states:

> Given the complexity and variation in local election administration, the argument goes, no set of practices can be considered 'best' for every jurisdiction. Some reforms that work well in certain contexts will be unnecessary or fail in others. There is certainly merit to this position; no one can doubt the limits of nationwide reforms of the American electoral system when local institutions, rules, and cultures differ considerably.

Id.

166. *Cf.* Weinstein-Tull, *supra* note 164, at 797 (urging local tailoring of election law as a means to "more successfully engage citizens in the voting process").

167. *See generally* Larry Kramer, *Putting Politics Back into the Political Safeguards of Federalism*, 100 COLUM. L. REV. 215, 278–87 (2000) (discussing the relationship between American federalism and the structure and operation of the major political parties).

168. Daniel P. Tokaji, *The Future of Election Reform: From Rules to Institutions*, 28 YALE L. & POL'Y REV. 125, 141 (2009).

matter in any event. With the first path thus closed, the oversight route prevails by default.

But an oversight solution has more to recommend it than just being the last option standing. Not only can vigorous oversight occur in a bi-cameral legislature divided between the major parties, but oversight also has the advantage of reserving for local officials the ultimate decisions about how to address election insecurities, thus preserving a structure that facilitates flexibility and local tailoring to meet both present and future challenges.

To be clear, the object of congressional oversight in this area would be largely—if not exclusively—to shine a light on the problems identified above and, in so doing, it is hoped, create political pressure on state and local officials to act where and how they have to date neglected to do so. In other words, the purpose of oversight would be to reveal unredressed problems and, by informing the public of their existence and drawing unwelcome attention to those principally tasked to fix such problems, spur officials to action. Using oversight to inform the public has long been extolled, but it would be a blindness to ignore that Congress has at times in our history employed the oversight spotlight to work great harm. In the next section, we explore this tension both by exploring the Supreme Court's somewhat equivocal treatment of informing-function oversight and by suggesting guidelines to differentiate its proper use from its dangerous abuse.[169]

VII. INFORMING OR EXPOSING

A. Congress's "Informing Function": In Theory and in Early Supreme Court Case Law

In a now-canonical passage in his 1885 doctoral dissertation-turned-treatise, *Congressional Government: A Study in American Politics*, then-scholar Woodrow Wilson extolled Congress as an educative body.[170] We here quote the relevant statement in full not only because of its obvious historical significance but also because of its uncanny relevance to present-day oversight in areas such as election security. Wilson wrote that:

169. *See infra* Part VII.

170. WOODROW WILSON, CONGRESSIONAL GOVERNMENT: A STUDY IN AMERICAN POLITICS 303 (1885).

> It is the proper duty of a representative body to look diligently into every affair of government and to talk much about what it sees. It is meant to be the eyes and the voice, and to embody the wisdom and will of its constituents. Unless Congress have and use every means of acquainting itself with the acts and the disposition of the administrative agents of the government, the country must be helpless to learn how it is being served; and unless Congress both scrutinize these things and sift them by every form of discussion, the country must remain in embarrassing, crippling ignorance of the very affairs which it is most important that it should understand and direct. The informing function of Congress should be preferred even to its legislative function. The argument is not only that discussed and interrogated administration is the only pure and efficient administration, but, more than that, that the only really self governing people is that people which discusses and interrogates its administration.[171]

As oft-quoted as Wilson's declaration has been, the Supreme Court's acceptance of a congressional "informing function" has nevertheless been hesitant and indecisive. Early cases concerning Congress's investigatory authority could even be read as hostile to the idea. For example, in *Kilbourn v. Thompson*, decided five years before Wilson wrote his dissertation, the Supreme Court ruled against a House effort to compel obedience to a subpoena on the ground that the underlying inquiry exceeded the powers of Congress.[172] The House had authorized examination of "a real-estate pool," which had apparently swallowed substantial U.S. assets that the Secretary of the Navy had improvidently entrusted to a firm since gone bankrupt.[173] The Court, after coming frighteningly close to the conclusion that Congress was altogether lacking in power to punish for contempt of its proceedings,[174] instead flatly declared that neither House possessed "the general power of

171. *Id.*

172. Kilbourn v. Thompson, 103 U.S. 168 (1881).

173. *Id*. at 193–95.

174. After concluding that a review of the relevant precedent gave little "aid . . . to the doctrine that [the contempt] power exists as one necessary to enable either House of Congress to exercise successfully their function of legislation," the Court veered away from the precipice, declaring the issue was "one which we do not propose to decide in the present case, because we are able to decide it without passing upon the existence or non-existence of such a power in aid of the legislative function." *Id.* at 189.

making inquiry into the private affairs of the citizen."[175] *Kilbourn* received "weighty criticism,"[176] and decades later, Supreme Court rulings arising out of congressional investigations into the "Teapot Dome" scandal were more solicitous of Congress's need for information.[177] Though even then, the Court's emphasis was on Congress's need for intelligence to enlighten its own exercise of its legislative authority—the need for it not to legislate "in the dark."[178] The Court did not mention a congressional role in educating the nation.[179]

In fact, the Supreme Court's treatment of congressional investigative authority did not explicitly embrace Wilson's notion of a congressional informing function until nearly three quarters of a century later. Rather, as we have seen, the foundational cases concerning Congress's implied authority to investigate stressed the need for a connection between congressional inquiry and congressional consideration of the necessity for, and, where appropriate, the content of some federal legislation. As late as the middle 1950s, a thoroughly researched Note in the *Harvard Law Review* blandly asserted that "the courts have never accepted the view that informing the public is a proper congressional function."[180] Ironically, it was not until congressional *abuse* of its investigative power had reached its grossest flood tide that the Supreme Court finally acknowledged the propriety of Congress investigating for the purpose of informing the public, albeit while, at the same time, seeking to protect individuals from the power's misuse.

---

175. *Id.* at 190. This broad assertion was unnecessary to resolve the case, which involved congressional inquiry into a matter then pending before a federal court. Hence, it has been sagely suggested that "*Kilbourn* . . . may only stand for the proposition that the Congress, through its investigative powers, cannot interfere with or attempt to alter a judicial proceeding." William P. Marshall, *The Limits on Congress's Authority to Investigate the President*, 2004 U. ILL. L. REV. 781, 802–03 (2004).

176. United States v. Rumely, 345 U.S. 41, 46 (1953).

177. *Id.*

178. McGrain v. Daugherty, 273 U.S. 135, 175 (1927).

179. *See id*.

180. *The Power of Congress to Investigate and Compel Testimony*, 70 HARV. L. REV. 671, 672 (1957). Indeed, it appears that Professors Redish and McFadden have persisted in this view. Martin H. Redish & Christopher R. McFadden, *HUAC, the Hollywood Ten, and the First Amendment Right of Non-Association*, 85 MINN. L. REV. 1669, 1723 n.174 (2001) (reading the constitutional history and the relevant Supreme Court cases as not supporting a congressional power to inquire for the purposes of informing the public independent of any authority to investigate for the purposes of exercising some Article I authority). We hasten to add that, given the breadth of congressional authority, the issue may be moot in many instances.

B. The Double-Edged Sword of Watkins

In the heart of the McCarthy Era, the Court decided a series of cases arising out of contempt prosecutions for failure to answer questions posed at inquisitorial congressional committee proceedings focused on communist infiltration into various aspects of American life and culture.

In the first, *United States v. Rumley*, Justice Frankfurter, writing for the Court in his inimitably impenetrable fashion, quoted Wilson's celebration of Congress's informing function at length, though in a manner that left it unclear whether the Court concurred in Wilson's views or merely cited them as a cautionary illustration of how vast and potentially invasive congressional assertions of a power of inquiry might become.[181] The latter interpretation drew strength from Justice Frankfurter's swiftly added censure that, in the words of his idol Holmes:

> All rights tend to declare themselves absolute to their logical extreme . . . [y]et all in fact are limited by the neighborhood of principles of policy which are other than those on which the particular right is founded, and which become strong enough to hold their own when a certain point is reached.[182]

In plainer language, Congress's partisans might claim the world, but these bold assertions would need to be tempered with a dose of reality when other values came into play.

And, as Frankfurter explained, in cases such as *Rumley*, which arose out of congressional efforts to identify and publicize the names of the persons to whom Rumley, a publisher, had sent controversial political tracks, the Constitution's protections of "the Freedom of Speech, and of the Press" came into play:

> President Wilson did not write in light of the history of events since he wrote; more particularly he did not write of the investigative power of Congress in the context of the First Amendment. And so, we would have to be that "blind" Court, against which Mr. Chief Justice Taft admonished in a famous passage, that does not see what "all others can see and understand" not to know that there is wide concern, both in and

181. United States v. Rumely, 345 U.S. 41, 43 (1953).

182. *Id.* at 43–44 (quoting Hudson County Water Co. v. McCarter, 209 U.S. 349, 355 (1908)).

> out of Congress, over some aspects of the exercise of the congressional power of investigation.[183]

In an effort to accommodate "these contending principles," or more precisely, in order to avoid having to reconcile them, the Court construed the resolution authorizing the committee to investigate "lobbying activities" narrowly by reading it literally, limiting its reach to encompass only "representations made directly to the Congress, its members, or its committees."[184] Having excluded Rumley's dissemination of "books of a particular political tendentiousness"[185] (in his case, extreme right wing propaganda) from the committee's charge, the Court was able to, in turn, conclude that Rumley's refusal to answer had come in response to an impertinent question, thus relieving him from criminal liability for contempt.[186]

For our effort to trace the Supreme Court's treatment of Congress's informing function, *Rumley* is an ambiguous case, both acknowledging Wilson's description but also recoiling from its potential implications. On both these points, the Court would settle more firmly four years later in its far more salient decision, *Watkins v. United States*.

There, John Watkins, a labor organizer and fellow traveler with (but *not* card-carrying member of) the Communist Party, was asked by the infamous House Un-American Activities Committee to identify other persons whom he knew to have belonged to the party.[187] After questioning the pertinency of the questions to the committee's task, Watkins declined to name any "persons who may in the past have been Communist Party members or otherwise engaged in Communist Party activity but who to [his] best knowledge and belief ha[d] long since removed themselves from the Communist movement."[188] His recalcitrance resulted in a criminal conviction for contempt.[189] When Chief Justice Earl Warren had finished his opinion for the Court, it was

---

183. *Rumley*, 345 U.S. at 44 (quoting Bailey v. Drexel Furniture Co. (Child Labor Tax Case), 259 U.S. 20, 37 (1922)).

184. *Id.* at 44–47.

185. *Id*. at 42.

186. *Id.* at 48. Justice Douglas, in an opinion joined by Justice Black, found the Court's narrow reading of the committee's authorization untenable in the light of its context. They would have met the First Amendment issue, which the majority avoided squarely, and invalidated Rumley's conviction on that basis. *Id.* at 48–58 (Douglas, J., concurring).

187. Watkins v. United States, 354 U.S. 178, 185 (1957).

188. *Id.*

189. *Id*.

clear that the conviction would not stand, though why and how the House might have more properly proceeded in its inquiry was less obvious.[190] Closer parsing of the Court's opinion suggests that, out of a solicitude for the same constitutional values that informed the *Rumley* Court's invocation of the avoidance canon, the *Watkins* Court employed a requirement that the full House authorize such sensitive intrusions by its subparts with an unmistakable clarity, analogous to comparable tools employed to enforce similar, otherwise under-enforced constitutional norms in the context of congressional delegations of authority to the executive branch.[191]

In any event, along the way, the Court provided both its theretofore least ambiguous endorsement of a congressional informing function and its theretofore strongest admonition that this power not be improperly perverted to impermissible objectives. As to the former, the Court described the investigatory powers of Congress in perhaps the most sweeping terms to be found in U.S. Reports:

> The power of the Congress to conduct investigations is inherent in the legislative process. That power is broad. It encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes. It includes conducting surveys of defects in our social, economic, and political systems for the purpose of enabling the Congress to remedy them. It probes into departments of the Federal Government to expose corruption, inefficiency, and waste.[192]

To this expansive characterization, the Court added, in a footnote, that the instant case did not concern "the power of the Congress to inquire into and publicize corruption, maladministration or inefficiency in agencies of the Government."[193] After asserting that such *governmental* corruption, maladministration, or inefficiency was all that Wilson had envisioned in celebrating Congress's informing function, the Court acknowledged that "[f]rom the earliest times in its history, the Congress has assiduously performed an 'informing function' of this

190. Alexander M. Bickel, *The Supreme Court 1960 Term Foreword: The Passive Virtues*, 75 HARV. L. REV. 40, 66 (1961) (critiquing the proffered rationale for the Court in *Watkins*).

191. Philip P. Frickey, *Getting from Joe to Gene (McCarthy): The Avoidance Canon, Legal Process Theory, and Narrowing Statutory Interpretation in the Early Warren Court*, 93 CALIF. L. REV. 397, 455–62 (2005).

192. *Watkins*, 354 U.S. at 187.

193. *Id.* at 200 n.33.

nature."[194] These passages, it is to be presumed, are the ones that have supported numerous commentators,[195] and at times, at least in dicta, the justices themselves,[196] in concluding that "[t]he Supreme Court has embraced Wilson's characterization of Congress's informing function."[197]

If so, the Court's embrace was of the sort that holds the embraced at a calculated distance. For in the same breath in which Chief Justice Warren articulated the passages recognizing a congressional informing function, he hastened to add that "broad as is this power of inquiry, it is not unlimited," stressing that "[t]here is no general authority to expose the private affairs of individuals without justification in terms of the functions of the Congress."[198] The Chief Justice explained this conclusion, in part, by referring to the same separation-of-powers principles that gave it life. The Congress, he lectured, was not "a law enforcement or trial agency"; rather, "[t]hese are functions of the executive and judicial departments of government."[199] The lesson concluded with a none-too-subtle reproach:

> No inquiry is an end in itself; it must be related to, and in furtherance of, a legitimate task of the Congress. Investigations conducted solely for the personal aggrandizement of the investigators or to "punish" those investigated are indefensible.[200]

Thus, *Watkins* is at once the best—but still a rather dubious—foundation for a congressional informing function. Some informing was good but exposing for exposure's sake was forbidden. Attempting to delimit the line between the two, and essaying what the distinction means

---

194. *Id.*

195. Several scholars have so concluded. *See, e.g.*, Howard R. Sklamberg, *Investigation Versus Prosecution: The Constitutional Limits on Congress's Power to Immunize Witnesses*, 78 N.C. L. REV. 153, 201 (1999); Marshall, *supra* note 175, at 797 (noting that "in one respect, the later cases appear to go even further than *McGrain* in supporting Congress's power to investigate: they explicitly maintain that the investigative power is not limited to aiding legislation but also includes the 'informing function,' or the power to expose corruption and misfeasance"). But not all concur. *See* Redish & McFadden, *supra* note 180, at 1723 n.174.

196. *See, e.g.*, Doe v. MacMillan, 412 U.S. 306, 314–17 (1973) (assuming the established validity of congressional inquiry for the purposes of informing the public).

197. Sklamberg, *supra* note 195, at 201.

198. *Watkins*, 354 U.S. at 187.

199. *Id.*

200. *Id.*

for oversight as a remedy for election insecurity, are this Article's next objects.[201]

C. Charting the Vague Boundary Between "Informing" and "Exposing"

As others before us have observed, one person's "informing" might be another's "exposing," especially considering that informing the public of mischief often requires first uncovering it.[202] This potential for overlap gives us pause, as one of our chief prescriptions is that the mechanisms of congressional oversight be employed for the purpose of revealing both the non-feasance and the mal-feasance that has led to laxity in protecting this year's—and future years'—elections from attack. Are we advocating the kind of abuse that *Watkins* counseled against? Or, in other, more urgent words: what is the (we hope not too) hypothetical constitutionally conscientious legislator to do?

We offer below some reflections on this conundrum in two forms. First, we identify "safe harbors," by which we mean avenues of inquiry that ought to be beyond reproach as clearly falling on the correct side of the informing-exposing divide. Second, coming at the matter from the opposite direction, we list some indicia that might signal that a congressional inquiry threatens to go too far, crossing into the forbidden realm of exposing for exposure's sake. We hope these observations will prove of value not only for those engaged in oversight for the goal of improving election security but also for conscientious legislators engaged in any inquiry with informing the public as one its objectives. Indeed, we think that this issue has received surprisingly scant attention in the scholarly literature to date and suggest the considerations we identify as the first step towards a more robust, theoretical exploration of this role for congressional oversight, though obviously that goal exceeds the scope of this short, focused study. For that reason, we wrap up by making explicit what our identified considerations might mean for the specific problem of congressional oversight of contemporary threats to election security.

---

201. *See infra* Part VII.C.

202. *See, e.g.*, R.S. Ghio, Note, *The Iran-Contra Prosecutions and the Failure of Use Immunity*, 45 STAN. L. REV. 229, 233 (1992) (noting that "[t]he line between exposing and informing . . . may prove difficult to draw").

1. Safe Harbors: Signs That an Inquiry Is Properly "Informing"

As the cases discussed above indicate, the safest of safe harbors for congressional inquiry is a genuine *legislative* purpose.[203] To the extent that a congressional investigation actually seeks to inform potential legislation, including adjustments in levels of appropriations or even to determine the existence *vel non* of a need to do any of the above, the investigation deserves the greatest respect and most indulgent deference from citizens and other governmental actors, including most notably judges.[204] To this distillation of the case law, we add merely that this respect and deference should not be diminished by the fact that a legislator may doubt the likelihood of a successful outcome to the legislative effort. Tilting at windmills may literally (pun intended) be ridiculous, but in Congress—no less than elsewhere in life—success requires endeavor that risks failure. Or as the Court itself has sagely observed of congressional inquiry: "The very nature of the investigative function—like any research—is that it takes the searchers up some 'blind alleys' and into nonproductive enterprises. To be a valid legislative inquiry there need be no predictable end result."[205] Accordingly, a good-faith belief in the possibility of a legislative outcome should suffice to supply the foundation for congressional inquiry, even if the political prognosis is pessimistic. Nor should the fact that members of Congress might prefer that the need for new federal legislation be obviated by the actions of other officials, whether in the federal bureaucracy or at the levels of state and local government (perhaps for some of the reasons identified above),[206] undercut the constitutional significance of the potential for a federal legislative outcome. The conscientious legislator should proceed with confidence wherever she can say in truth that an investigation could reveal information relevant to a conceivable exercise of an Article I power.

2. Red Flags: Indicia That an Inquiry May Be Veering Towards Improper "Exposure"

Having discussed the purpose—informing the future exercise of legislative power—that sets a congressional inquiry on the firmest of foundations, we highlight now a contrasting purpose that such an

203. *See supra* notes 172–200 and accompanying text.
204. *Id.*
205. Eastland v. U.S. Servicemen's Fund, 421 U.S. 491, 509 (1975).
206. *See supra* notes 164–168 and accompanying text.

investigation ought never serve: punishing past conduct. Fundamental separation-of-powers principles teach that this objective is not within the powers entrusted to the legislative branch but rather is the province of the executive acting under the close supervision of the judiciary.[207] History reinforces the wisdom of this allocation, as many of the worst harms inflicted by the McCarthy Era abuses of Congress's investigatory authority were the consequences of, at best, thinly veiled efforts to punish persons perceived to be disloyal by exposing them to retribution, often imposed by the independent action of private parties.[208] A conscientious legislator ought to be ever mindful of the need to avoid a repetition of those cruelties.

A caveat is necessary. Although punitive exposure is an illegitimate *purpose*, the fact that a legitimate legislative inquiry undertaken for constitutionally valid purposes might incidentally expose misconduct cannot be permitted to frustrate the inquiry. The Supreme Court rightfully rebuffed such an effort in *McGrain v. Daugherty*,[209] its landmark affirmation of congressional investigative authority. There, the Court rejected the claim of the former Attorney General that a Senate inquiry into his failures in connection with Teapot Dome scandal, an inquiry the Court had earlier in the opinion blessed as relevant to Congress's obligation to oversee and fund the U.S. Department of Justice, would in effect punish him by sullying his good reputation. Quoting favorably the colorful language of one Senator speaking in support of the resolution authorizing the inquiry, the Court decisively disposed of the former Attorney General's plea and all others like it:

> Shall we say the legislative branch of the government shall stickle and halt and hesitate because a man's public reputation, his public character, may suffer because of that legislative action? . . . [I]s the Senate to hesitate, is the Senate to refuse to do its duty merely because the public character or the public reputation of some one who is investigated may be thereby smirched, to use the term that has been used so often in the debate?[210]

---

207. *See supra* note 200 and accompanying text.

208. *See* MARTIN H. REDISH, THE LOGIC OF PERSECUTION: FREE EXPRESSION AND THE MCCARTHY ERA 37 (2005).

209. McGrain v. Daugherty, 273 U.S. 135 (1927).

210. *Id.* at 179 (quoting CONG. REC. 68th Cong. 1st Sess. 3397, 3398 (statement of Sen. George)).

Although the Court's cases make clear that "smirching" of reputations is serious business that lies entirely outside the legitimate *objectives* of congressional inquiry, at least since *McGrain*, it has been equally clear that such a consequence must be endured where it is incidental to a congressional investigation in service of a constitutionally proper end.

Still, any legislative attempt to punish as an end in itself violates the division of powers at the core of our Constitution's design. But during the McCarthy Era, this constitutional distortion was gravely compounded by the fact that much of the conduct exposed by congressional committees to facilitate its often-private punishment was itself *protected* by the Constitution.[211] Accordingly, that history supplies an additional lesson for the conscientious legislator: that constitutionally protected activity, however unpopular, should never be made the target of congressional inquiry as part of an effort to chill the exercise of the underlying freedoms.

To summarize, proverbial "red flags" signal danger whenever a congressional investigation veers from informing the prospective exercise of an Article I power towards the retrospective sanction of unpopular conduct, and the cause for concern is enlarged when the conduct is sheltered by a constitutional shield. We next apply these insights to the informing-function oversight that we have prescribed.

3. Significance of These Considerations for Election-Security Oversight

Oversight expected to reveal continuing vulnerabilities in our electronic election infrastructure fits comfortably within the tradition of laudatory use of Congress's inquisitorial powers. First and perhaps foremost, inquiries into election insecurity probe problems clearly within the constitutional authority of Congress to remedy with legislation, including appropriations measures.[212] To be sure, we have argued that a federal command-and-control solution might be inferior to permitting correction by state and local authorities.[213] Moreover, we have acknowledged that, in any event, in the next several months, enactment of a federal fix seems so unlikely as to be fantastic. But neither of these reservations undermine the constitutional case for federal authority. Nor

---

211. This is the insight of Professor Redish's magisterial work on the McCathy Era Smith Act prosecutions. *See generally* REDISH, *supra* note 208, at 7.

212. *See supra* note 126 and accompanying text (discussing possible legislative responses to electronic election vulnerabilities).

213. *See supra* notes 164–168 and accompanying text.

do they make the envisioned federal legislative response pretextual because it remains the residual option should state and local authorities remain intransigent and legislators must be permitted to strive to change the political equilibrium lest it become disconnected from the needs and desires of the people nominally being represented.

The oversight we propose also avoids the pitfalls indicative of the abuse of Congress's investigative authority. The objective remains entirely prospective, with the focus squarely on revealing uncorrected vulnerabilities to spur their correction rather than punishing past neglect. To the extent that revelation may prove embarrassing to some, that consequence is incidental in precisely the manner that the Supreme Court blessed nearly a century ago.[214] Nor is the genuine target of any inquiry the exposure of detested albeit constitutionally protected activity, the obvious misuse of investigative authority at the heart of so many Red-Scare Era injustices.[215] While our capacity to explore the tension between appropriate informing-function oversight and improper investigation for the purpose of "exposure" has been circumscribed by the specific focus of this Article, we do hope that this brief essay on the boundary between the two may spur subsequent, more thorough and theoretically rich explorations of this tension by whoever gets there first.

VIII. CONCLUSION

The prospect that an election could be "hacked," or even credibly denounced as "hacked," should disturb all Americans of whatever political affiliation. Yet vulnerabilities to such an outcome remain unaddressed and have, to date, stirred surprisingly little public concern considering all that is at stake.

It was the prospect of public enlightenment as to just these sorts of governmental failings to which Woodrow Wilson alluded to in his oft-repeated salute to Congress's informing function. Acknowledging, as both history and Supreme Court jurisprudence require, that a congressional power to publicize can be perverted to a demagogue's desire to punish the vulnerable, we have argued above that the use and abuse of this congressional authority can be distinguished. Further, we have sought to identify markers to do so and have applied them to our calls for informing-function oversight in the service of reliable, trust-worthy, and widely trusted elections, even in the most divisive of contests.

---

214. *See supra* notes 209–210 and accompanying text.
215. *See supra* notes 208, 211 and accompanying text.