EXHIBIT I

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I have reviewed the expert disclosures prepared by Dr. Juan Gilbert and Dr. Benjamin Adida for State Defendants. Neither Dr. Gilbert not Dr. Adida offers any rebuttal to the numerous, critical vulnerabilities in Georgia's BMDs that I described in my July 1, 2021 expert report. Dr. Adida did not respond to my report at all; State Defendants reissued prior declarations from him previously provided in this litigation. Neither of them disputes the presence of any of the serious

vulnerabilities I detail in my report or the steps I describe for exploiting those vulnerabilities to alter individual votes and election outcomes in Georgia. Nor does either of them claim to have examined any of the voting equipment used in Georgia to evaluate whether the vulnerabilities I identified—or others—have been exploited in any past election. Although each of them presumably could do this with the permission of State Defendants, who I understand engaged them as experts in this case, there is no indication either has undertaken any such inquiry or asked to do so. As a result, neither Dr. Gilbert nor Dr. Adida has anything to say about the reliability of the voting equipment used in Georgia elections. This is surprising, given that they have had at least the last year to examine Georgia's voting equipment.

3. State Defendants urgently need to engage with the findings in my report and address the vulnerabilities it describes before attackers exploit them. Nothing in Dr. Gilbert's or Dr. Adida's responses indicates that State Defendants understand the seriousness of these problems or have taken any measures to address them and their implications for the Plaintiffs' individual votes in future elections. Established practice in the security field would require State Defendants to promptly subject Georgia's voting system to rigorous testing in response to my report, to assess the extent and significance of each of the vulnerabilities I described, and to identify and *promptly implement* specific measures (where possible) to eliminate or mitigate each

of those vulnerabilities. Neither Dr. Gilbert nor Dr. Adida indicates any such efforts on their own part or on the part of State Defendants or anyone else. Again, Dr. Adida did not respond to my report.

4. In my report—a 25,000-word document that is the product of twelve weeks of intensive testing of the Dominion equipment provided by Fulton County—I find that Georgia's BMDs contains multiple severe security flaws. Attackers could exploit these flaws to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. I explain in detail how such malware, once installed, could alter voters' votes while subverting all the procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs). Finally, I describe working proof-of-concept malware that I am prepared to demonstrate in court.

5. My report concludes, *inter alia*, that Georgia's BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to target future elections in the state; that the BMDs' vulnerabilities compromise the auditability of Georgia's paper ballots; that the BMDs can be compromised to the same extent as or more easily than the DREs they replaced; and that using these vulnerable BMDs for all in-person voters, as Georgia

does, greatly magnifies the level of security risk compared to using hand-marked paper ballots and providing BMDs to voters who need or request them.

Reply to Declaration of Dr. Juan Gilbert

6. Rather than engage with the facts in my report, Dr. Gilbert responds largely with vague generalities. He gives no indication that he has ever used an ICX BMD, let alone tested its security. He begins by conceding that "any computer can be hacked," but he contends that "this general statement is largely irrelevant," because hand-marked paper ballot systems use computers too (to scan the ballots) (¶ 6). His position is inconsistent with accepted standards for election security and with the facts of the particular voting system used in Georgia.

7. My testing has shown that the BMDs used in Georgia suffer from specific, highly exploitable vulnerabilities that allow attackers to change votes despite the State's purported defenses. There is no evidence that Georgia's ballot scanners suffer from the same extraordinary degree of exploitability, nor does Dr. Gilbert contend they do. He ignores the relative ease with which Georgia's BMDs can be hacked, including by a voter in a voting booth in mere minutes. That extreme difference in security as compared to other voting technologies, particularly hand-marked paper ballots, is far from "irrelevant" as Dr. Gilbert implies.

8. Furthermore, even if the scanners were just as insecure as the BMDs, Georgia's practice of requiring essentially all in-person voters to use highly vulnerable BMDs would needlessly give attackers *double* the opportunity to change the personal votes of individual Georgia voters, since malware could strike either the BMDs or the scanners. Accepted standards in election security compel reducing points of attack for bad actors, not unnecessarily expanding them—a point Dr. Gilbert ignores.

9. Lastly, Dr. Gilbert also ignores that accepted election security protocols include an effective measure to protect against hacks of ballot scanners when the ballots are hand-marked rather than generated by BMDs—namely, reliable risk-limiting audits (RLAs), which would have a high probability of detecting any outcome-changing attack on the scanners. Not only do Georgia's BMDs defeat the efficacy of RLAs, but Dr. Gilbert continues to ignore the fact that Georgia requires an RLA of just one statewide contest every two years (and, to my knowledge, has not adopted specific, adequate procedures to ensure a reliable RLA for that one audit every other year).

10. Dr. Gilbert goes on to discuss issues related to voter verification of BMD ballots (which I respond to below). Yet he fails to address the potential for attackers to cheat by changing only the QR codes printed by Georgia's BMDs.

Voters cannot read the QR codes, but they are the only part of the ballots that the scanners count. My report details several routes by which malicious hardware or software can manipulate the QR codes and cause the recorded votes to differ from voters' selections. In principle, a rigorous risk-limiting audit would be likely to detect such an attack if the attacker changed enough votes to alter the outcome of the contest being audited, but again Georgia rules require such an audit in only a single statewide contest once every two years. As my report explains, this leaves the vast majority of elections and contests in Georgia vulnerable to QR code (and others) attacks, yet Dr. Gilbert says nothing about this threat.

11. Instead, Dr. Gilbert focuses exclusively on a different threat: attacks that change *both* the QR codes and the ballot text. In addition to the barcode-only attacks I just discussed, my report demonstrates that Georgia's BMDs can be manipulated so that both the barcodes and the printed text indicate the same fraudulent selections. No audit or recount can catch such fraud, because all records of the voter's intent would be wrong. The only reliable way to detect it would be if enough voters carefully reviewed their ballots, noticed that one or more selections differed from their intent, and reported the problems to election officials, *and* if Georgia officials then discerned from the pattern of voter reports that the BMDs were systematically misbehaving. Thus, Dr. Gilbert is mistaken when he contends that the distinction

between "voter-verifiable" and "voter-verified" paper ballots "only matters in principle" (¶ 7). All BMD ballots are potentially voter-verifiable, but unless enough BMD ballots are actually voter-*verified*, BMD-based attacks could alter election outcomes even in the rare instances where the State conducts a risk-limiting audit. And unless *every* BMD ballot is actually voter-*verified*, BMD-based attacks could alter individual voters' selections without detection..

12. A large body of recent scientific evidence has established that few voters are likely to catch errors caused by malicious BMDs. I have reviewed this evidence in previous declarations.[1] It comes from both field observations (which report how long real voters review their ballots during real elections) and laboratory tests (which report the fraction of errors that subjects detect when voting on hacked BMDs in simulated elections). These methodologies are complementary, and results to-date from all studies of both kinds point to a low rate of voter-verification.

13. Dr. Gilbert criticizes field observations because "[t]ime spent reviewing a ballot has little to do with whether it was actually verified" (¶ 9). This claim is inconsistent with accepted election security principles. Of course, they are not exactly the same question, but obviously the time spent reviewing a ballot can

---

[1] *Halderman decl.* (Dec. 16, 2019), Dkt. 682 at 23-33; *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 6-8, 55.

provide important insight into whether it was likely verified. For example, we can conclude that a voter who spends only a second or two reviewing a lengthy, complicated ballot is unlikely to have reliably verified each of their selections on the ballot. And of course, the same is true for a voter who spends no time at all reviewing their ballot. Review time is both practical to measure and clearly correlated with the error detection success, making it a valuable and relevant metric, as multiple studies confirm.

14. Dr. Gilbert seems to contend, without evidence, that a casual glance is sufficient to review Georgia-style ballots because selections are printed together with party affiliations (¶ 9). He cites no research (and I am unaware of any) that supports this conclusion, particularly when, as in Georgia, the party affiliations are printed in small type and in a different horizontal position for each contest. A real BMD ballot is reproduced on page 15 of my expert report. This is just one example of such a ballot; they can be longer and more confusing. Dr. Gilbert provides no basis for believing that voters would likely catch deliberate errors caused by compromised BMDs when voting such a ballot.

15. Dr. Gilbert references my award-winning peer-reviewed study about voter verification behavior, which found very poor rates of error detection and

reporting in a mock election using BMDs that my team hacked (¶ 10).[2] He contends that my study "ignores the reaction to such manipulation in an actual election, particularly one as heated in the public domain as the 2020 Election." (¶ 11). He does not explain how or why such circumstances would be expected to materially increase voter verification of their respective BMD ballots, nor does he cite any support for his claim to believe they would. And, just last week, the Atlanta Journal-Constitution obtained a study (under the Georgia Open Records Act) commissioned by the Secretary of State's Office in which researchers from the University of Georgia observed Georgia voters during the November 2020 election and reported how long they spent reviewing their BMD ballots.[3] Although it appears the Secretary of State had this study at the time of Dr. Gilbert's response to my report, he does not address or acknowledge it. The new study suggests that voters in the real world review their ballots *even less carefully* than voters in recent laboratory studies—despite the reminders election workers are supposed to give them to carefully review

---

[2] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" In *41st IEEE Symposium on Security and Privacy* (May 2020). Available at https://ieeexplore.ieee.org/document/9152705.

[3] Mark Niesse, "Under half of Georgia voters checked their paper ballots, study shows," *Atlanta Journal-Constitution* (July 27, 2021). Available at https://www.ajc.com/politics/under-half-of-georgia-voters-checked-their-paper-ballots-study-shows/6HSVHHFOBRBDPODRZXLIBTUS64/.

their ballots at the polling sites, which Dr. Gilbert emphasizes as a remedy for poor voter verification of BMD ballots.[4]

16. The University of Georgia researchers report that 20% of voters they observed did not check their ballots at all.[5] Only about 49% examined their ballots for at least one second, and only 19% did so for more than five seconds. This is significantly worse performance than observed in my study, which found that when voters were verbally prompted to review their ballots before casting them, as should occur in Georgia, 63% of voters reviewed their ballots for only *two* seconds or more, compared to 19-49% in the new study.

17. This suggests that laboratory studies like mine tend to *overestimate* the rate at which real Georgia voters would detect errors on their BMD ballots. Since real Georgia voters were observed to review their ballots even less carefully than the

---

[4] Secretary Raffensperger appears to disagree with Dr. Gilbert about the value of measuring voter review time for assessing voter verification performance. He told the Atlanta Journal-Constitution that the new study "shows voters do indeed review their ballots for accuracy before casting them" and offers "proof the votes that were counted were for the candidates the voters intended." (*Id.*). I agree that the new study provides valuable insights about voter behavior, but, contrary to the Secretary's pronouncements, the results indicate that real Georgia voters are even less likely to detect errors caused by compromised BMDs than previous studies have suggested.

[5] Audrey A. Haynes and M.V. Hood III, "Georgia Voter Verification Study" (January 22, 2021). Available at https://s3.documentcloud.org/documents/21017815/gvvs-report-11.pdf.

participants in my study, it is reasonable to infer that real voters would catch an even smaller fraction of errors. The participants in my study who were similarly prompted to review their ballots caught 14% of errors. Therefore, real voters in Georgia are likely to catch substantially less than 14% of errors.

18. How often would voters have to detect errors on their BMD ballots to effectively safeguard against attacks? The answer depends on the margin of victory, since an outcome-changing attack would need to change fewer votes in a close contest. The model from my study shows that, given the margin of victory from the 2020 Presidential contest in Georgia, voters would need to have detected 46% of errors for there to be even one error report per 1000 voters, under a hypothetical scenario where the election outcome had been changed by hacked BMDs.[6] The University of Georgia observations show that barely 49% of voters looked at their ballots for even a second, let alone studied them carefully enough to reliably spot errors.

---

[6] To reiterate, the November presidential race was the only state-wide contest subjected to a risk-limiting audit. In other contests, attackers could change the outcome by tampering with only the ballot QR codes, and voters would have no practical way to detect this manipulation regardless of how diligently they reviewed their ballots.

19. Dr. Gilbert performs a similar calculation using the baseline error detection rate measured in my study. He finds that an outcome changing attack on Georgia's Presidential contest would have resulted in only 832 voters noticing that their BMD ballots showed the wrong selection. Dr. Gilbert suggests that there have not been such complaints from any voters, and says he finds it implausible that so many voters would have "simply not said anything or otherwise simply corrected their ballot and thought nothing of it then or since" (¶ 12).

20. This is an oddly constructed hypothetical, since Curling Plaintiffs do not claim here that the Presidential outcome was altered by hacking the BMDs. And Dr. Gilbert does not indicate any effort to determine the total number of spoiled ballots in Georgia's Presidential contest, which he presumably could have explored with State Defendants. Neither does he provide any basis to believe there were only 832 or fewer spoiled ballots. But suppose for the sake of argument that the Presidential election outcome in Georgia had been altered by hacking the BMDs, and there *were* complaints from the 832 voters that Dr. Gilbert has calculated. What then? It seems all but certain that these complaints would have been dismissed or drowned out in the cacophonous aftermath of the election or simply disregarded by election workers at the polling sites as voter errors. Yet the official count, the risk-limiting audit, and the recount would all have found the wrong winner, and there would be no

way to recover any altered vote or correct the election outcome short of rerunning the election. With a mere 832 complaints among 5 million participating voters (amidst a sea of other complaints, real and imagined), it is unlikely that poll workers or election officials, including State Defendants, would realize or even suspected there was a systemic problem with the BMDs, and it is completely implausible that they would take the drastic but necessary step of asking Georgians to vote again. Georgia's election system is susceptible to this extraordinary risk as long as it remains vulnerable to the attacks I described in my report (and potentially others).

21. To get to the point of making a decision to rerun an election, State Defendants (among others, perhaps) would first need to know how many voters discovered a problem when verifying their ballots. As Dr. Gilbert points out, the number of spoiled BMD ballots provides an upper bound on the number of voters who discovered and corrected an error (¶ 12). He does not say how many spoiled ballots there actually were in November 2020. If State Defendants knew the number was less than 832, they likely would have shared this fact with Dr. Gilbert, and he would have stated it in his report. It is reasonable to infer that either there were more than 832 spoiled ballots (and the attack is plausible) or State Defendants *do not know* how many BMD ballots were spoiled during the election, eight months later, despite

what Dr. Gilbert acknowledges those ballots would suggest about the reliability of the election.

22. That State Defendants may not know this information is consistent with gaps in other important election data that Georgia counties report to the Secretary of State. State Defendants recently produced electronic data (election projects) that I understand were required to be returned to them by counties after the November 2020 and January 2021 elections. In both elections, a large fraction of counties failed to return any data, returned the wrong data, or omitted data necessary for assessing the security and integrity of the result, such as election databases or ballot images. More than six months after these elections, the Secretary of State has not been able to assemble these electronic records and has not indicated any effort or willingness to do so. Yet the only way that State Defendants could use the number of spoiled ballots as a defense against BMD-based cheating would be if the poll workers accurately tracked it, counties accurately aggregated it, and the Secretary's Office received such data from across the state before the election result was determined. Even then, it is unlikely that the Secretary would be prepared to react by *rerunning the election* if the number of spoiled ballots exceeded the number predicted in an outcome-changing attack.

23. Given the ineffectiveness of such defenses and the critical security problems in Georgia's BMDs, I (like Dr. Appel) recommend that BMDs be reserved for voters who need or request them, as is the case in most states. Dr. Gilbert responds by claiming, without evidence, that "[d]isabled voters are even less likely to identify an error on their printed ballot" (¶ 14). I am unaware of any study that supports this sweeping indictment of voters with disabilities, which encompasses a vast array of disabilities that would not impact the ability of the voter to identify an error on their printed ballot in any way. He also contends that blind voters cannot detect errors on their ballot at all, but this is not true. Many blind voters use assistive technology to read printed text and likely could do so to verify their ballots. Moreover, only some voters who need BMDs are blind. For instance, those with motor impairments that prevent them from marking a ballot by hand would not necessarily have any greater difficulty verifying the printed text than any other voter. In any case, if BMDs are used primarily by voters with disabilities (as in most jurisdictions that use BMDs), they will represent a *much* smaller target,[7] and an

---

[7] Although Dr. Gilbert cites a figure that would imply that 10% of Georgians who voted in 2020 were disabled, data from Maryland, where BMDs are available upon request, suggests that only about 1.8% of voters would request to use BMDs if they were offered a hand-marked ballot first. (*Halderman decl.*, Aug. 19, 2020, Dkt. 785-2 at 49.) Dr. Gilbert's citation to the number of all Georgia voters with disabilities is highly misleading since, again, very few of those voters would be

outcome-changing attack on any given election will be detectable with a much lower rate of voter error detection than when all in-person voters use BMDs as they do in Georgia today. This in turn creates a strong disincentive for bad actors to attempt hacking an election (the risk likely is not worth the reward when the outcome is highly unlikely to be changed), which means individual votes would be less likely to be altered by hacking.

24. In his only direct response to my expert report, Dr. Gilbert states that he is not aware that I have "provided equipment marred by 'undetectable' hacks to any other independent researcher" (¶ 15).[8] This is a curious and ironic criticism coming from Dr. Gilbert, since he evidently chose not to evaluate my findings through an examination of the voting equipment himself, which he does not explain. Moreover, Dr. Gilbert misreads my report. It does not claim that malicious software infecting a BMD would be undiscoverable by any possible means. If an individual BMD is

---

unable to vote on a hand-marked paper ballot, consistent with the number reported in Maryland.

[8] Dr. Gilbert ignores that, as I understand it, State Defendants have objected to my report and the underlying work being shared with third parties (except Dominion), including other independent researchers, with whom I am eager to share my work for review. I am confident in my findings and believe they should be shared promptly with appropriate election security researchers and officials in an effort to mitigate the critical vulnerabilities in Georgia's voting equipment that I describe. I invite Dr. Gilbert to join me in seeking State Defendants' consent to do that.

known to contain malware, there will likely be some level of detailed forensic scrutiny that can detect where the malware is, perhaps requiring months of expert analysis per machine at extraordinary expense. It would be completely infeasible to perform this level of analysis on every machine before every election, much less between an election and the deadline for certification of its results. (And after manipulating ballots, malware could remove all traces of its presence from a machine, defeating any possible post-election examination of the device.) What my report shows is that vote-stealing malware of the type I have constructed would not be detected by any of the defenses that State Defendants purport to practice. I describe in detail how such malware would defeat QR code authentication, logic and accuracy testing, on-screen hash validation, and external APK validation (as was used by Pro V&V after the November election). Dr. Gilbert offers no rebuttal to these findings. He does not dispute them or even address them.

25. Moreover, there is already an example of an "undetectable" attack entered into testimony: exploitation of the Drupal vulnerability discovered by Logan Lamb in the Center for Election Systems server. As Lamb attested, the developers of the primary tool for detecting this vulnerability stated that "[n]either [the defensive tool] nor an expert can guarantee a website has *not* been compromised. They can only

confirm with certainty a website *has* been compromised."[9] Furthermore, the Drupal developers state that any server running the vulnerable software after the initial disclosure of the vulnerability should be assumed to have been compromised unless it was patched within *hours* of disclosure. According to the timeline presented in Lamb's declaration, he found the KSU server to be in a vulnerable state on August 28, 2016, nearly two years after the initial announcement of the critical vulnerability (October 15, 2014).[10] The KSU server image also contains evidence that a second vulnerability, the so-called Shellshock flaw, was exploited on December 2, 2014.[11] This vulnerability was publicly disclosed more than two months earlier and widely publicized in the media as a critical vulnerability, yet the KSU server remained unpatched.

26. An attacker who compromised the KSU server could therefore have maintained undetected access to the compromised server. Since the server remained in a vulnerable state undetected for almost two years, it is highly likely that it was successfully attacked at some point in time. An attacker who did so would have been able to move laterally to other systems within the CES network and to other

---

[9] *Lamb decl.*, Dkt. 258-1 at 19.
[10] See "Drupal Core - Highly Critical - Public Service announcement" (Oct. 29, 2014), available at https://www.drupal.org/PSA-2014-003.
[11] *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 23.

components of Georgia's voting system. As I have previously pointed out, many election system components that could have been compromised in this way are still in use in Georgia today, where they provide a means by which attackers could spread vote-stealing malware to the BMDs.

27. Rather than address the many threats to Georgia's voting system, Dr. Gilbert persists in drawing illogical comparisons between BMDs and hand-marked paper ballots. For instance, he questions why Plaintiffs have presented no research "regarding voters' proclivity to review [hand-marked paper ballots] to ensure their ballots are marked and will count as intended" (¶ 8). Much like Dr. Gilbert's earlier testimony that "[i]n essence, a BMD is nothing more than an ink pen,"[12] one does not need expertise in election security to find fault with this reasoning. Preventing voters from making accidental mistakes is a completely different problem from preventing their selections from being deliberately and systematically changed by an attacker who has compromised the BMDs. There is abundant evidence that voters do sometimes make errors whether filling out a ballot by hand or by machine. Bad ballot design exacerbates this problem with both voting modalities, but following ballot design best practices can greatly reduce it. Both

[12] *Gilbert decl.*, Dkt. No. 658-3 at 60.

BMDs and scanners that count hand-marked ballots can also be configured to reject overvotes and to warn voters about undervotes, the most common kinds of voter errors. Moreover, unlike older technologies for counting hand-marked ballots, the scanners used in Georgia (when properly configured) can detect improperly or incompletely marked bubbles and present them to human operators to adjudicate whether the marks should count as votes. Election officials can use all of these options to help protect voters from their own mistakes, but none of them offers protection against a BMD that deliberately changes the selections printed on a voter's ballot (or those encoded in the ballot barcode). The central problem with Georgia's highly vulnerable BMD system—that attackers can change all records of the voter's intent without being detected by election officials—has no parallel in a hand-marked paper ballot system.

28. Dr. Gilbert concludes as he started, with vague and sweeping generalities. "Simply put, BMD elections systems are no more insecure than [hand-marked] systems" (¶ 16). It is unclear whether he is claiming that *all* BMD systems are at least as secure as all hand-marked systems or merely that some specific BMD system (such as the one he recently developed himself to address some of the reliability problems that exist with Georgia's BMDs) is at least as secure as some hand-marked system, but this is of little consequence. The only BMD system that is

relevant here is the Dominion ICX as used in Georgia. As my expert report details, Georgia's BMD system suffers from numerous, severe vulnerabilities. These vulnerabilities would have little potential to change election outcomes if use of BMDs were limited to voters who need or request them, as Curling Plaintiffs desire, and they would be far less likely to affect the personal votes of individual Georgia voters.

Reply to Declarations of Dr. Benjamin Adida

29. The declarations by Dr. Adida that State Defendants have submitted predate my expert report, so Dr. Adida's opinions are not informed by the critical vulnerabilities in Georgia's BMD equipment that my analysis has revealed or by anything else in my lengthy, detailed report. Nor are they informed by any events that occurred in the year since he first provided these declarations, such as any aspect of the November 2020 election in Georgia or the Secretary of State's study indicating that few voters verified their respective ballots in that election.

30. Nevertheless, Dr. Adida's first declaration is correct that "Running a risk-limiting audit is one of the most important advances states can take in improving election integrity—without an RLA, we are effectively trusting computerized scanners to count our paper ballots" (Dkt. 834-2 at ¶ 5). This is true, but, as my expert report shows, without a risk-limiting audit Georgia is also trusting its critically

vulnerable BMDs to generate ballots with QR codes that correctly reflect voters' selections. Obviously compromised BMDs and compromised scanners could change individual votes and election outcomes. But again, nothing suggests that Georgia's scanners suffer from such easily exploitable critical vulnerabilities as the BMDs do.

31. Dr. Adida and I also agree that RLAs are important for discovering whether compromised BMDs have manipulated enough ballot QR codes to change the outcome of an election (¶ 12). Although RLAs are, as Dr. Adida says, "of the utmost importance" (¶ 6), Georgia does not require an RLA in the vast majority of elections and the vast majority of contests, leaving both election outcomes and individual voters' votes susceptible to manipulation via BMD malware. Additionally, it is insufficient for states to merely (in Dr. Adida's words) "take meaningful steps to implement RLAs"; rather, states have to *actually conduct* reliable RLAs, which Georgia does not intend to do for the vast majority of its elections (or perhaps any of its elections, depending on the reliability of the audit procedures it implements).

32. In his second declaration, Dr. Adida refers to a "dispute amongst academics regarding whether voters verify their ballots using ballot-marking devices" (Dkt. 912-1 at ¶ 11). This statement reflects a misunderstanding of the state of research today. I am not aware of any scientific research that supports the proposition that Georgia voters would likely detect more than a small fraction of

errors caused by BMD malware. In contrast, the past two years have seen a wave of laboratory studies and multiple field observation studies addressing this question, all of which strongly indicate the opposite, that few voters carefully review their ballots and so the vast majority of errors caused by BMD malware would likely to go undiscovered and uncorrected. Although there once was uncertainty about whether most voters carefully verify their BMD ballots, there is no longer any serious scientific dispute that they do not. It is the hallmark of good science (and of good public policy) that it evolves based on new evidence, such as the University of Georgia study commissioned by the Secretary of State that I discussed above—which Dr. Adida has not addressed.

33. Georgia's election system needs to evolve as well. Due to the critical vulnerabilities in Georgia's BMDs that are described in my expert report, Georgia voters face an extreme risk that BMD-based attacks could manipulate their individual votes and alter election outcomes. Even in the rare contests for which the State requires a risk-limiting audit, the scientific evidence about voter verification shows that attackers who compromise the BMDs could likely change individual votes and even the winner of a close race without detection. Georgia can eliminate or greatly mitigate these risks by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving

BMDs for voters who need or request them. Absent security improvements such as this, it is my opinion that Georgia's voting system does not satisfy accepted security standards. Neither Dr. Gilbert nor Dr. Adida offers a contrary opinion in their respective declarations, instead ignoring the critical issue of whether the *voting system used in Georgia*—which neither claims to have examined—reliably protects the right to vote for individual Georgia voters.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 2nd day of August, 2021 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

EXHIBIT J

116TH CONGRESS
1st Session

SENATE

REPORT
116-XX

REPORT

OF THE

SELECT COMMITTEE ON INTELLIGENCE

UNITED STATES SENATE

ON

RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION

VOLUME 1: RUSSIAN EFFORTS AGAINST ELECTION INFRASTRUCTURE

WITH ADDITIONAL VIEWS

CONTENTS

I. (U) INTRODUCTION 3
II. (U) FINDINGS 3
III. (U) THE ARC OF RUSSIAN ACTIVITIES 5
IV. (U) ELEMENTS OF RUSSIAN ACTIVITIES 10
A. (U) Targeting Activity 10
B. (U) Russian Access to Election Infrastructure 21
1. (U) Russian Access to Election Infrastructure: Illinois 22
2. [redacted] Russian Access to Election Infrastructure: [redacted] 24
C. [redacted] Russian Efforts to Research U.S. Voting Systems, Processes, and Other Elements of Voting Infrastructure 28
D. [redacted] Russian Activity Directed at Voting Machine Companies 29
E. [redacted] Russian Efforts to Observe Polling Places 30
F. [redacted] 32
G. [redacted] Russian Activity Possibly Related to a Misinformation Campaign on Vote[redacted] 32
H. (U) Two Unexplained Events 33
1. (U) Cyber Activity in State 22 33
2. (U) Cyber Activity in State 4 34
V. (U) RUSSIAN INTENTIONS 35
VI. (U) NO EVIDENCE OF CHANGED VOTES OR MANIPULATED VOTE TALLIES. ... 38
VII. (U) SECURITY OF VOTING MACHINES 40
VIII. (U) THE ROLE OF DHS AND INTERACTIONS WITH THE STATES 46
A. (U) DHS's Evolution 46
B. (U) The View From the States 49
C. (U) Taking Advantage of DHS Resources 52
IX. (U) RECOMMENDATIONS 54

Russian Efforts Against Election Infrastructure

I. (U) INTRODUCTION

(U) From 2017 to 2019, the Committee held hearings, conducted interviews, and reviewed intelligence related to Russian attempts in 2016 to access election infrastructure. The Committee sought to determine the extent of Russian activities, identify the response of the U.S. Government at the state, local, and federal level to the threat, and make recommendations on how to better prepare for such threats in the future. The Committee received testimony from state election officials, Obama administration officials, and those in the Intelligence Community and elsewhere in the U.S. Government responsible for evaluating threats to elections.

II. (U) FINDINGS

1. [redacted] The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against U.S. election infrastructure[1] at the state and local level. [redacted] The Committee has seen no evidence that any votes were changed or that any voting machines were manipulated.[2]

2. [redacted]

---

[1] **(U)** The Department of Homeland Security (DHS) defines *election infrastructure* as "storage facilities, polling places, and centralized vote tabulation locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments, " according to the January 6, 2017 statement issued by Secretary of Homeland Security Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector, available at https://www.dhs.gov/news/2017/10/06/statement-secretary-johnson-designation-election-infrastructure-critical. Similarly, the Help America Vote Act (HAVA), Pub. L. No. 107-252, Section 301(b)(1) refers to a functionally similar set of equipment as "voting systems," although the definition excludes physical polling places themselves, among other differences, 52 U.S.C. §21081(b). This report uses the term *election infrastructure* broadly, to refer to the equipment, processes, and systems related to voting, tabulating, reporting, and registration.

[2] [redacted] The Committee has reviewed the intelligence reporting underlying the Department of Homeland Security (DHS) assessment from early 2017 [redacted] The Committee finds it credible.

[3] **(U)** The names of the states the Committee spoke to have been replaced with numbers. DHS and some states asked the Committee to protect state names before providing the Committee with information. The Committee's goal was to get the most information possible, so state names are anonymized throughout this report. Where the report refers to public testimony by Illinois state election officials, that state is identified.

3. **(U)** While the Committee does not know with confidence what Moscow's intentions were, Russia may have been probing vulnerabilities in voting systems to exploit later. Alternatively, Moscow may have sought to undermine confidence in the 2016 U.S. elections simply through the discovery of their activity.

4. **(U)** Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states. The U.S. intelligence apparatus is, by design, foreign-facing, with limited domestic cybersecurity authorities except where the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) can work with state and local partners. State election officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor.

5. **(U)** DHS and FBI alerted states to the threat of cyber attacks in the late summer and fall of 2016, but the warnings did not provide enough information or go to the right people. Alerts were actionable, in that they provided malicious Internet Protocol (IP) addresses to information technology (IT) professionals, but they provided no clear reason for states to take this threat more seriously than any other alert received.

6. **(U)** In 2016, officials at all levels of government debated whether publicly acknowledging this foreign activity was the right course. Some were deeply concerned that public warnings might promote the very impression they were trying to dispel—that the voting systems were insecure.

7. **(U)** Russian activities demand renewed attention to vulnerabilities in U.S. voting infrastructure. In 2016, cybersecurity for electoral infrastructure at the state and local level was sorely lacking; for example, voter registration databases were not as secure as they could have been. Aging voting equipment, particularly voting machines that had no paper record of votes, were vulnerable to exploitation by a committed adversary. Despite the focus on this issue since 2016, some of these vulnerabilities remain.

8. **(U)** In the face of this threat and these security gaps, DHS has redoubled its efforts to build trust with states and deploy resources to assist in securing elections. Since 2016, DHS has made great strides in learning how election procedures vary across states and how federal entities can be of most help to states. The U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), the National Association of State Election Directors (NASED), and other groups have helped DHS in this effort. DHS's work to bolster states' cybersecurity has likely been effective, in particular for those states that have leveraged DHS's cybersecurity assessments for election infrastructure, but much more needs to be done to coordinate state, local, and federal knowledge and efforts in order to harden states' electoral infrastructure against foreign meddling.

9. **(U)** To assist in addressing these vulnerabilities, Congress in 2018 appropriated $380 million in grant money for the states to bolster cybersecurity and replace vulnerable

voting machines.[4] When those funds are spent, Congress should evaluate the results and consider an additional appropriation to address remaining insecure voting machines and systems.

10. **(U)** DHS and other federal government entities remain respectful of the limits of federal involvement in state election systems. States should be firmly in the lead for running elections. The country's decentralized election system can be a strength from a cybersecurity perspective, but each operator should be keenly aware of the limitations of their cybersecurity capabilities and know how to quickly and properly obtain assistance.

III. (U) THE ARC OF RUSSIAN ACTIVITIES

[redacted] In its review of the 2016 elections, the Committee found no evidence that vote tallies were altered or that voter registry files were deleted or modified, though the Committee and IC's insight into this is limited. Russian government-affiliated cyber actors conducted an unprecedented level of activity against state election infrastructure in the run-up to the 2016 U.S. elections [redacted] Throughout 2016 and for several years before, Russian intelligence services and government personnel conducted a number of intelligence-related activities targeting the voting process. [redacted] the Committee found ample evidence to suggest that the Russian government was developing and implementing capabilities to interfere in the 2016 elections, including undermining confidence in U.S. democratic institutions and voting processes.[5]

[redacted]

- [redacted]

---

[4] **(U)** Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, 132 Stat. 348, 561-562.

[5] **(U)** The Committee has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases. These activities are routinely carried out in the context of private sector breaches.

[6] [redacted] FBI LHM, [redacted]

[7] [redacted] FBI LHM, [redacted]

[8] [redacted] DHS Homeland Intelligence Brief, [redacted]

[9] [redacted] FBI LHM, [redacted]

- [redacted]
- [redacted]

[redacted] Evidence of scanning of state election systems first appeared in the summer prior to the 2016 election. In mid-July 2016, Illinois discovered anomalous network activity, specifically a large increase in outbound data, on a Illinois Board of Elections' voter registry website.[12] Working with Illinois, the FBI commenced an investigation.[13] [redacted] The attack resulted in data exfiltration from the voter registration database.[16]

(U) On August 18, 2016, FBI issued an unclassified FLASH[17] to state technical-level experts on a set of [redacted] suspect IP addresses identified from the attack on Illinois's voter registration databases.[18] [redacted] The FLASH product did not attribute the attack to Russia or any other particular actor.[21]

---

[10] **(U/**[redacted]**)** FBI Electronic Communication, [redacted]

[11] [redacted] FBI LHM, [redacted]

[12] **(U)** DHS briefing for SSCI staff, March 5, 2018.

[13] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 113.

[14] **(U**[redacted]**)** According to the United States Computer Emergency Readiness Team (US-CERT), an SQL injection is "an [redacted] technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code."

[15] **(U)** DHS IIR 4 0050006 17, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016

[16] **(U**[redacted]**)** DHS briefing for SSCI staff, March 5, 2018.

[17] **(U)** FBI FLASH alerts are notifications of potential cyber threats sent to local law enforcement and private industry so that administrators are able to guard their systems against the described threat. FLASHs marked TLP: AMBER are considered sharable with members of the recipients own organization and those with direct need to know.

[18] [redacted] Number T-LD1004-TT, TLP-AMBER, [redacted]

[19] **(U)** *Ibid.*

[20] **(U)** *Ibid.*

[21] R[redacted]wned [redacted]

(U/[redacted]) After the issuance of the August FLASH, the Department of Homeland Security (DHS) and the Multi-State-Information Sharing & Analysis Center (MS-ISAC)[22] asked states to review their log files to determine if the IP addresses described in the FLASH had touched their infrastructure. This request for voluntary self-reporting, in conjunction with DHS analysis of NetFlow activity on MS-ISAC internet sensors, identified another 20 states whose networks had made connections to at least one IP address listed on the FLASH.[23] DHS was almost entirely reliant on states to self-report scanning activity.

[redacted] Former Special Assistant to the President and Cybersecurity Coordinator Michael Daniel said, "eventually we get enough of a picture that we become confident over the course of August of 2016 that we're seeing the Russians probe a whole bunch of different state election infrastructure, voter registration databases, and other related infrastructure on a regular basis."[25] Dr. Samuel Liles, Acting Director of the Cyber Analysis Division within DHS's Office of Intelligence and Analysis (I&A), testified to the Committee on June 21, 2017, that "by late September, we determined that internet-connected election-related networks in 21 states were potentially targeted by Russian government cyber actors."[26]

[redacted]

[22] **(U)** The MS-ISAC is a DHS-supported group dedicated to sharing information between state, local, tribal, and territorial (SLTT) government entities. It serves as the central cybersecurity resource for SLTT governments. Entities join to receive cybersecurity advisories and alerts, vulnerability assessments, incident response assistance, and other services.

[23] **(U/[redacted])** DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Governments to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.

[24] **(U)** SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 41.

[25] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on August 31, 2017, p. 39.

[26] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 12.

(U) DHS and FBI issued a second FLASH and a Joint Analysis Report in October that flagged [redacted] suspect IP addresses, many unrelated to Russia.[27] DHS briefers told the Committee that they were intentionally over-reporting out of an abundance of caution, given their concern about the seriousness of the threat. DHS representatives told the Committee, "We were very much at that point in a sort of duty-to-warn type of attitude . . . where maybe a specific incident like this, which was unattributed at the time, wouldn't have necessarily risen to that level. But . . . we were seeing concurrent targeting of other election-related and political figures and political institutions . . . [which] led to what would probably be more sharing than we would normally think to do."[28]

[redacted]

[redacted] DHS assessed that the searches, done alphabetically, probably included all 50 states, and consisted of research on "general election-related web pages, voter ID information, election system software, and election service companies."[31]

[redacted]

---

[27] **(U/**[redacted]**)** FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems,* October 14, 2016.

[28] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 9-10.

[29] [redacted] FBI LHM, [redacted]

[30] [redacted]

[31] [redacted] DHS Homeland Intelligence Brief, *Update:* [redacted]

[32] [redacted] NSA [redacted] DIRNSA, May 5, 2017. This information was not available to the U.S. government until April 2017.

[33] [redacted]

[34] **(U)** NSA [redacted] DIRNSA, May 5, 2017.

The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials. [37] In objecting to these tactics, then-Assistant Secretary of State for European and Eurasian Affairs Victoria Nuland reminded the Russian Ambassador that Russia had refused invitations to participate in the official OSCE mission that was to observe the U.S. elections.[38]

---

[35] **(U)** FBI IIR ; FBI IIR

[36] **(U)** *Ibid.*

[37] **(U)** DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 221-222.

[38] Email, sent November 4, 2016; from ; to: , , . Subject: Kislyak Protest of FBI Tactics.

[39] **(U)** NSA DIRNSA, May 5, 2017.

[40] **(U)** *Ibid.*

[41]

[42]

[43]

(U) The Committee found no evidence of Russian actors attempting to manipulate vote tallies on Election Day, though again the Committee and IC's insight into this is limited.

(U/[redacted]) In the years since the 2016 election, awareness of the threat, activity by DHS, and measures at the state and local level to better secure election infrastructure have all shown considerable improvement. The threat, however, remains imperfectly understood. In a briefing before Senators on August 22, 2018, DNI Daniel Coats, FBI Director Christopher Wray, then-DHS Secretary Kirstjen Nielsen, and then-DHS Undersecretary for the National Protection and Programs Division Christopher Krebs told Senators that there were no known threats to election infrastructure. However, Mr. Krebs also said that top election vulnerabilities remain, including the administration of the voter databases and the tabulation of the data, with the latter being a much more difficult target to attack.[44] Relatedly, several weeks prior to the 2018 mid-term election, DHS assessed that "numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election."[45]

[redacted]

IV. (U) ELEMENTS OF RUSSIAN ACTIVITIES

A. (U) Targeting Activity

[redacted] Scanning of election-related state infrastructure by Moscow was the most widespread activity the IC and DHS elements observed in the run up to the 2016 election.[48]

- [redacted] In an interview with the Committee, Mr. Daniel stated: "What it mostly looked like to us was reconnaissance. . . . I would have characterized it at the time as sort of conducting the reconnaissance to do the network mapping, to do the topology mapping so

---

[44] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[45] **(U/[redacted])** Homeland Security Intelligence Assessment: Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure, October 11, 2018.
[46] **(U)** DTS 2019-1368, NIC 2019-01, Intelligence Community Assessment: A Summary of the Intelligence Community Report on Foreign Interference as Directed by Executive Order 13848, March 29, 2019. p. 2-3.
[47] **(U)** *Ibid.*
[48] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 12.

that you could actually understand the network, establish a presence so you could come back later and actually execute an operation."[49]

- **(U)** Testifying before the Committee, Dr. Liles characterized the activity as "simple scanning for vulnerabilities, analogous to somebody walking down the street and looking to see if you are home. A small number of systems were unsuccessfully exploited, as though somebody had rattled the doorknob but was unable to get in . . . [however] a small number of the networks were successfully exploited. They made it through the door."[50]

[redacted] DHS and FBI assessments on the number of affected states evolved since 2016. In a joint FBI/DHS intelligence product published in March 2018, and coordinated with the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), the Department of State, the National Intelligence Council, the National Security Agency (NSA), and the Department of Treasury, DHS and FBI assessed [redacted] that Russian intelligence services conducted activity [redacted].[51] [redacted]

- [redacted] DHS arrived at their initial assessment by evaluating whether the tactics, techniques, and procedures (TTPs) observed were consistent with previously observed Russian TTPs, whether the actors used known Russian-affiliated malicious infrastructure, and whether a state or local election system was the target.[53]

- **(U)** The majority of information examined by DHS was provided by the states themselves. The MS-ISAC gathered information from states that noticed the suspect IPs pinging their systems. In addition, FBI was working with some states in local field offices and reporting back FBI's findings.

- **(U)** If some states evaluated their logs incompletely or inaccurately, then DHS might have no indication of whether they were scanned or attacked. As former-Homeland Security Adviser Lisa Monaco told the Committee, "Of course, the law enforcement and the intelligence community is going to be significantly reliant on what the holders and

---

[49] **(U)** SSCI Transcript of the Interview of Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 44.
[50] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[51] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]
[52] **(U)** *See* chart, *infra*, for information on successful breaches.
[53] **(U)** DHS did not count attacks on political parties, political organizations, or NGOs. For example, the compromise of an email affiliated with a partisan State 13 voter registration organization was not included in DHS's count.

owners and operators of the infrastructure sees on its system [sic] and decides to raise their hand."[54]

[redacted] However, both the IC and the Committee in its own review were unable to discern a pattern in the affected states, [redacted]

(U) Mr. Daniel told the Committee that by late August 2016, he had already personally concluded that the Russians had attempted to intrude in all 50 states, based on the extent of the activity and the apparent randomness of the attempts. "My professional judgment was we have to work under the assumption that they've tried to go everywhere, because they're thorough, they're competent, they're good."[55]

[redacted] Intelligence developed later in 2018 bolstered Mr. Daniel's assessment that all 50 states were targeted. [redacted]

- [redacted]

---

[54] **(U)** SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 38.
[55] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 40.
[56] [redacted] DHS/FBI Homeland Intelligence Bulletin, [redacted]
[57] **(U)** *Ibid.*
[58] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[59] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, pp. 11-12.
[60] **(U)** DHS briefing for SSCI staff, March 5, 2018.

- [redacted]
- [redacted]

[redacted]

(U) However, IP addresses associated with the August 18, 2016 FLASH provided some indications the activity might be attributable to the Russian government, particularly the GRU:

- [redacted]
- [redacted]
- **(U/[redacted])** One of the Netherlands-based [redacted] "exhibited the same behavior from the same node over a period of time. . . . It was behaving like . . . the same user or group of users was using this to direct activity against the same type of targets," according to DHS staff.[69]

---

[61] **(U)** *Ibid.*
[62] **(U)** *Ibid.*
[63] **(U)** *Ibid.*
[64] **(U)** *Ibid.*
[65] [redacted]
[66] FBI IIR [redacted]
[67] **(U)** Cyber Threat Intelligence Integration Center (CTIIC) Cyber Threat Intelligence Summary, October 7, 2016.
[68] **(U)** *Ibid.*
[69] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.

- [redacted]

[redacted] The IC's confidence level about the attribution of the attacks evolved over 2017 and into 2018. [redacted]

- [redacted]

- [redacted]

[redacted] The Committee reached out to the 21 states that DHS first identified as targets of scanning activity to learn about their experiences. Election officials provided the Committee

---

[70] **(U)** DHS Electronic Communication, December 19, 2016, email from: DHS/NCCIC; to: CIA.
[71] [redacted]
[72] [redacted]
[73] [redacted] DHS Intelligence Assessment, *Hostile Russian Cyber Targeting of Election Infrastructure in 2016; Probable Non-State Actors Attempt Disruption*, May 3, 2017.
[74] **(U)** *Ibid.*
[75] **(U)** SSCI interview of representatives from DHS and CTIIC, February 27, 2018, p. 13.
[76] [redacted] DHS arrived at their initial assessment of 21 states affected by adding the eleven plus seven states, plus the three where scanning activity appeared directed at less specifically election-focused infrastructure.
[77] **(U)** SSCI conference call with DHS and FBI, March 29, 2018.

details about the activity they saw on their networks, and the Committee compared that accounting to DHS's reporting of events.[78] Where those accounts differed is noted below. The scanning activity took place from approximately June through September 2016.

STATE	OBSERVED ACTIVITY[79]
Illinois	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 2	**(U)** *See infra,* "Russian Access to Election-Related Infrastructure" for a detailed description.
State 3	**(U)** According to State 3 officials, cyber actors using infrastructure identified in the August FLASH conducted scanning activity.[80] State 3 officials noticed "abnormal behavior" and took action to block the related IP addresses.[81] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[82]
State 4	**(U)** *See infra,* "Two Unexplained Events" for a detailed description.
State 5	**(U)** Cyber actors using infrastructure identified in the August FLASH scanned "an old website and non-relevant archives," according to the State 5 Secretary of State's office.[83] The following day, State 5 took action to block the IP address.[84] [redacted] DHS, however, reported GRU scanning activity on two separate State 5 Secretary of State websites, plus targeting of a District Attorney's office[85] in a particular city.[86] Both the websites appear to be current addresses for the State 5 Secretary of State's office.
State 6	**(U)** According to State 6 officials, cyber actors using infrastructure identified in the August FLASH scanned[87] the entire state IT infrastructure, including by using the Acunetix tool, but the "affected systems" were the Secretary of State's

[78] **(U)** DHS briefed Committee staff three times on the attacks, and staff reviewed hundreds of pages of intelligence assessments.

[79] **(U)** Slight variation between what states and DHS reported to the Committee is an indication of one of the challenges in election cybersecurity. The system owners—in this case, state and local administrators—are in the best position to carry out comprehensive cyber reviews, but they often lack the expertise or resources to do so. The federal government has resources and expertise, but the IC can see only limited information about inbound attacks because of legal restrictions on operations inside the United States.

[80] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.

[81] **(U)** *Ibid.*

[82] **(U)** DHS briefing for Committee staff on March 5, 2018.

[83] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.

[84] **(U)** *Ibid.*

[85] **(U/**[redacted]**)** Briefers suggested the "most wanted" list housed on the District Attorney's website may have in some way been connected to voter registration. The exact nature of this connection, including whether it was a technical network connection or whether databases of individuals with felony convictions held by the District Attorney's office had voting registration implications, is unclear.

[86] **(U)** DHS briefing for Committee staff on March 5, 2018.

[87] **(U)** State 6 officials did not specify, but in light of the DHS assessment, they likely meant SQL injection.

	web application and the election results website.[88] If the penetration had been successful, actors could have manipulated the unofficial display of the election tallies.[89] State officials believed they would have caught any inconsistency quickly.[90] State 6 became aware of this malicious activity and alerted partners.[91] [redacted] DHS reported that GRU actors scanned State 6, then unsuccessfully attempted many SQL injection attacks. State 6 saw the highest number of SQL attempts of any state.
State 7	**(U)** According to State 7 officials, cyber actors using infrastructure identified in the August FLASH scanned public-facing websites, including the "static" election site.[92] It seemed the actors were "cataloging holes to come back later," according to state election officials.[93] State 7 became aware of this malicious activity after receiving an FBI alert.[94] [redacted] DHS reported GRU scanning attempts against two separate domains related to election infrastructure.[95]
State 8	**(U)** According to State 8 officials, cyber actors using infrastructure identified in the August FLASH scanned a State 8 public election website on one day.[96] State 8 officials described the activity as heightened but not particularly out of the ordinary.[97] State 8 became aware of this malicious activity after receiving an alert.[98] [redacted]
State 9	**(U)** According to State 9 officials, cyber actors using infrastructure identified in an October MS-ISAC advisory[101] scanned the statewide voter registration

[88] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[89] **(U)** *Ibid.*
[90] **(U)** *Ibid.*
[91] **(U)** *Ibid.*
[92] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[93] **(U)** *Ibid.*
[94] **(U)** *Ibid.*
[95] **(U)** DHS briefing for Committee staff on March 5, 2018.
[96] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[97] **(U)** *Ibid.*
[98] **(U)** *Ibid.*
[99] **(U)** DHS briefing for Committee staff on March 5, 2018.
[100] **(U)** *Ibid.*
[101] **(U)** While the Committee was unable to review the specific indicators shared with State 9 by the MS-ISAC in October, the Committee believes at least one of the relevant IPs was originally named in the August FLASH because of technical data held by DHS which was briefed to the Committee.

	system.[102] Officials used the analogy of a thief casing a parking lot: they said the car thief "didn't go in, but we don't know why."[103] State 9 became aware of this malicious activity after receiving an alert.[104] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[105]
State 10	**(U)** According to State 10 officials, cyber actors using infrastructure identified in the August FLASH conducted activity that was "very loud," with a three-pronged attack: a Netherlands-based IP address attempted SQL injection on all fields 1,500 times, a U.S.-based IP address attempted SQL injection on several fields, and a Poland-based IP address attempted SQL injection on one field 6-7 times.[106] State 10 received relevant cybersecurity indictors from MS-ISAC in early August, around the same time that the attacks occurred.[107] State 10's IT contractor attributed the attack to Russia and suggested that the activity was reminiscent of other attacks where attackers distract with lots of noise and then "sneak in the back."[108] **(U)** State 10, through its firewall, blocked attempted malicious activity against the online voter registration system and provided logs to the National Cybersecurity and Communications Integration Center (NCCIC)[109] and the U.S. Computer Emergency Readiness Team (US-CERT).[110] State 10 also brought in an outside contractor to assist.[111] [redacted] DHS confirmed GRU SQL injection attempts against State 10's voter services website on August 5 and said that the attack was blocked after one day by State 10's firewall.[112]
State 11	**(U)** According to State 11 officials, they have seen no evidence of scanning or attack attempts related to election infrastructure in 2016.[113] While State 11 officials noted an IP address "probing" state systems, activity which was "broader than state election systems," State 11 election officials did not provide specifics on which systems.[114]

[102] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[103] **(U)** *Ibid.*
[104] **(U)** *Ibid.*
[105] **(U)** DHS briefing for Committee staff on March 5, 2018.
[106] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 10], November 29, 2017.
[107] **(U)** *Ibid.*
[108] **(U)** *Ibid.*
[109] **(U)** NCCIC is DHS's cyber watch center.
[110] **(U)** *Ibid.*
[111] **(U)** *Ibid.*
[112] **(U)** DHS briefing for Committee staff on March 5, 2018.
[113] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[114] **(U)** *Ibid.*

	[redacted] DHS reported GRU scanning activity on the Secretary of State domain.[115]
State 12	**(U)** Cyber actors using infrastructure identified in the August FLASH conducted scanning activity that "lasted less than a second and no security breach occurred," according to State 12 officials.[116] State 12 became aware of this malicious activity after being alerted to it.[117] [redacted] DHS reported that because of a lack of sensor data related to this incident, they relied on NetFlow data, which provided less granular information.[118] DHS's only clear indication of GRU scanning on State 12's Secretary of State website came from State 12 self-reporting information to MS-ISAC after the issuance of the August FLASH notification.[119]
State 13	**(U)** According to State 13 officials, they have seen no evidence of scanning or attack attempts related to state-wide election infrastructure in 2016.[120] [redacted]
State 14	[redacted] MS-ISAC passed DHS reports of communications between a suspect IP address used by the GRU at the time and the State 14 election commission webpage, but no indication of a compromise.[123] In addition, DHS was informed of activity relating to separate IP addresses in the August FLASH,

---

[115] **(U)** DHS briefing for Committee staff on March 5, 2018.
[116] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[117] **(U)** *Ibid.*
[118] **(U)** DHS briefing for Committee staff on March 5, 2018.
[119] **(U)** *Ibid.*
[120] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[121] **(U)** FBI IIR [redacted] DHS briefing for Committee staff on March 5, 2018.
[122] [redacted]; DHS briefing for Committee staff on March 5, 2018. For more information on decisions by DHS to exclude certain activity in its count of 21 states, *see* text box, *infra*, "DHS Methodology for Identifying States Touched by Russian Cyber Actors."
[123] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]; DHS briefing for Committee staff on March 5, 2018.

	including attempted Domain Name System (DNS) lookups and potentially malicious emails, some dating back to January 2016.[124]
State 15	**(U)** State 15 officials were not aware that the state was among those targeted until they were notified.[125] State 15's current lead election official was not in place during the 2016 election so they had little insight into any scanning or attempted intrusion on their systems. State 15 officials said that generally they viewed 2016 as a success story because the attempted infiltration never got past the state's four layers of security. [redacted] DHS reported broad GRU scanning activity on State 15 government domains.[126]
State 16	**(U)** According to State 16 officials, cyber actors using infrastructure identified in the October FLASH conducted scanning activity against a state government network.[127] [redacted] DHS reported information on GRU scanning activity based on a self-report from State 16 after the issuance of the October FLASH.[128]
State 17	**(U)** State 17 officials reported nothing "irregular, inconsistent, or suspicious" leading up to the election.[129] While State 17 IT staff received an MS-ISAC notification, that notification was not shared within the state government.[130] [redacted] DHS reported GRU scanning activity on an election-related domain.[131]
State 18	**(U)** State 18 election officials said they observed no connection from the IP addresses listed in the election-related notifications.[132] [redacted] DHS reported indications of GRU scanning activity on a State 18 government domain.[133]
State 19	**(U)** According to State 19 officials, cyber actors using infrastructure identified in October by MS-ISAC conducted scanning activity. State 19 claimed this activity was "blocked," but did not elaborate on why or how it was blocked.[134]

---

[124] **(U/**[redacted]**)** DHS IIR 4 019 0012 17, *Cyber Activity Targeting [State 14] Government Networks from Internet Protocol Addresses Associated with Targeting State Elections Systems*, October 21, 2016.
[125] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 15], March 12, 2018.
[126] **(U)** DHS briefing for Committee staff on March 5, 2018.
[127] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[128] **(U)** DHS briefing for Committee staff on March 5, 2018.
[129] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[130] **(U)** *Ibid.*
[131] **(U)** DHS briefing for Committee staff on March 5, 2018.
[132] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 18], December 8, 2017.
[133] **(U)** DHS briefing for Committee staff on March 5, 2018.
[134] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 19], December 1, 2017.

	[redacted] DHS reported indications of GRU scanning activity on two separate State 19 government domains.[135]
State 20	**(U)** According to State 20 officials, cyber actors using infrastructure identified in October by MS-ISAC were "knocking" on the state's network, but no successful intrusion occurred.[136] [redacted] DHS reported GRU scanning activity on the Secretary of State domain.[137]
State 21	**(U)** State 21 officials received indicators from MS-ISAC in October 2016. They said they were not aware the state was among those targeted until notified.[138] [redacted] DHS reported GRU scanning activity on an election-related domain as well as at least one other government system connected to the voter registration system.[139]

[redacted] Neither DHS nor the Committee can ascertain a pattern to the states targeted, lending credence to DHS's later assessment that all 50 states probably were scanned. DHS representatives told the Committee that "there wasn't a clear red state-blue state-purple state, more electoral votes, less electoral votes" pattern to the attacks. DHS acknowledged that the U.S. Government does not have perfect insight, and it is possible the IC missed some activity or that states did not notice intrusion attempts or report them.[140] [redacted]

[redacted]

---

[135] **(U)** DHS briefing for Committee staff on March 5, 2018.
[136] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[137] **(U)** DHS briefing for Committee staff on March 5, 2018.
[138] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.
[139] **(U)** DHS briefing for Committee staff on March 5, 2018.
[140] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 25.
[141] [redacted]
[142] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 21.

(U/[redacted]) As of October 2018, the IC and DHS were looking for evidence of threats to election systems, [redacted]. An October 11, 2018 DHS Intelligence Assessment reported the following:

> *We judge that numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election. We are aware of a growing volume of malicious activity targeting election infrastructure in 2018, although we do not have a complete baseline of prior years to determine relative scale of the activity. Much of our understanding of cyber threats to election infrastructure is due to proactive sharing by state and local election officials, as well as more robust intelligence and information sharing relationships amongst the election community and within the Department. The observed activity has leveraged common tactics—the types of tactics that are available to nation-state and non-state cyber actors, alike—with limited success in compromising networks and accounts. We have not attributed the activity to any foreign adversaries, and we continue to work to identify the actors behind these operations. At this time, all these activities were either prevented or have been mitigated.*

(U/[redacted]) Specifically:

> *Unidentified cyber actors since at least April 2018 and as recently as early October continue to engage in a range of potential elections-related cyber incidents targeting election infrastructure using spear-phishing, database exploitation techniques, and denial of service attacks, possibly indicating continued interest in compromising the availability, confidentiality, and integrity of these systems. For example, on 24 August 2018, cybersecurity officials detected multiple attempts to illegally access the State of Vermont's Online Voter Registration Application (OLVR), which serves as the state's resident voter registration database, according to DHS reporting. The malicious activity included one Cross Site Scripting attempt, seven Structured Query Language (SQL) injection attempts, and one attempted Denial of Service (DoS) attack. All attempts were unsuccessful.*[143]

(U/[redacted]) In summarizing the ongoing threat to U.S. election systems, DHS further said in the same product, "We continue to assess multiple elements of U.S. election infrastructure are potentially vulnerable to cyber intrusions."[144]

B. (U) Russian Access to Election Infrastructure

---

[143] **(U/[redacted])** DHS, Homeland Security Intelligence Assessment, *Cyber Actors Continue to Engage in Influence Activities and Targeting of Election Infrastructure*, October 11, 2018.
[144] **(U)** *Ibid.*

(U) The January 6, 2017 Intelligence Community Assessment (ICA), "Assessing Russian Activities and Intentions in Recent U.S. Elections," states:

> *Russian intelligence obtained and maintained access to elements of multiple U.S. state or local electoral boards. DHS assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying.*[145]

[redacted] Based on the Committee's review of the ICA, the Committee concurs with this assessment. The Committee found that Russian-affiliated cyber actors gained access to election infrastructure systems across two states, including successful extraction of voter data. However, none of these systems were involved in vote tallying.

1. (U) Russian Access to Election Infrastructure: Illinois

(U) In June 2016, Illinois experienced the first known breach by Russian actors of state election infrastructure during the 2016 election.[146] As of the end of 2018, the Russian cyber actors had successfully penetrated Illinois's voter registration database, viewed multiple database tables, and accessed up to 200,000 voter registration records.[147] The compromise resulted in the exfiltration of an unknown quantity of voter registration data.[148] Russian cyber actors were in a position to delete or change voter data, but the Committee is not aware of any evidence that they did so.[149]

- [redacted] DHS assesses with high confidence that the penetration was carried out by Russian actors.[150]
- **(U/**[redacted]**)** The compromised voter registration database held records relating to 14 million registered voters, [redacted]. The records exfiltrated included information on each voter's name, address, partial social security number, date of birth, and either a driver's license number or state identification number.[151]

---

[145] **(U)** Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. iii.
[146] **(U/**[redacted]**)** DHS IIR 4 005 0006, *An IP Address Targeted Multiple U.S. State Government's to Include Election Systems*, October 4, 2016; DHS briefing for SSCI staff, March 5, 2018.
[147] **(U)** "Illinois election officials say hack yielded information on 200,000 voters," [Local Newspaper], August 29, 2016.
[148] **(U)** DHS IIR [redacted] SCI Open Hearing on June 21, 2017, p 110
[149] **(U)** State Board of Elections, *Illinois Voter Registration System Records Breached*, August 31, 2016. As reflected elsewhere in this report, the Committee did not undertake its own forensic analysis of the Illinois server logs to corroborate this statement; SSCI interview with DHS and CTIIC, February 27, 2018, p. 24.
[150] **(U)** *See infra*, "Russian Scanning and Attempted Access to Election-Related Infrastructure" for a complete discussion on attribution related to the set of cyber activity linked to the infrastructure used in the Illinois breach.
[151] **(U/**[redacted]**)** FBI IIR [redacted] DHS Intelligence Assessment, May 3, 2017, 0144-17, p. 2.

- [redacted] DHS staff further recounted to the Committee that "Russia would have had the ability to potentially manipulate some of that data, but we didn't see that." [152] Further, DHS staff noted that "the level of access that they gained, they almost certainly could have done more. Why they didn't . . . is sort of an open-ended question. I think it fits under the larger umbrella of undermining confidence in the election by tipping their hand that they had this level of access or showing that they were capable of getting it."[153]

- **(U)** According to a Cyber Threat Intelligence Integration Center (CTIIC) product, Illinois officials "disclosed that the database has been targeted frequently by hackers, but this was the first instance known to state officials of success in accessing it."[154]

(U) In June 2017, the Executive Director of the Illinois State Board of Elections (SBE), Steve Sandvoss, testified before the Committee about Illinois's experience in the 2016 elections.[155] He laid out the following timeline:

- **(U)** On June 23, 2016, a foreign actor successfully penetrated Illinois's databases through an SQL attack on the online voter registration website. "Because of the initial low-volume nature of the attack, the State Board of Election staff did not become aware of it at first."[156]

- **(U)** Three weeks later, on July 12, 2016, the IT staff discovered spikes in data flow across the voter registration database server. "Analysis of the server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of our paperless online voter application website."[157]

- **(U)** On July 13, 2016, IT staff took the website and database offline, but continued to see activity from the malicious IP address.[158]

- **(U)** "Firewall monitoring indicated that the attackers were hitting SBE IP addresses five times per second, 24 hours a day. These attacks continued until August 12th [2016], when they abruptly ceased."[159]

---

[152] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 14.
[153] **(U)** *Ibid.*
[154] **(U)** CTIIC Cyber Threat Intelligence Summary, August 18, 2016.
[155] **(U)** SSCI Open Hearing on June 21, 2017. The Committee notes that, in his testimony, Mr. Sandvoss said Illinois still had not been definitively told that Russia perpetrated the attack, despite DHS's high confidence. The Committee also notes that DHS eventually provided a briefing to states during which DHS provided further information on this topic, including the DHS high-confidence attribution to Russia.
[156] **(U)** *Ibid.*, p. 110.
[157] **(U)** *Ibid.*
[158] **(U)** *Ibid.*, p. 111.
[159] **(U)** *Ibid.*

- **(U)** On July 19, 2016, the election staff notified the Illinois General Assembly and the Attorney General's office.
- **(U)** Approximately a week later, the FBI contacted Illinois.[160]
- **(U)** On July 28, 2016, both the registration system and the online voter registration became fully functional again.[161]

2. (U) Russian Access to Election Infrastructure: State 2

[redacted]

[redacted] Separately, GRU cyber actors breached election infrastructure in State 2. [redacted]

- [redacted]

---

[160] **(U)** *Ibid.*, p. 113.
[161] **(U)** *Ibid.*, p. 112.
[162] **(U/[redacted])** FBI Electronic Communication, [redacted]
[163] **(U)** *Ibid.*
[164] [redacted]
[165] **(U)** FBI Briefing on [State 2] Election Systems, June 25, 2018.
[166] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[167] **(U)** *Ibid.*
[168] **(U)** *Ibid.*
[169] **(U)** *Ibid.*
[170] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 16.
[171] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, compartmented session.

[redacted]

[redacted]

(U) FBI and DHS Interactions with State 2[179]	
August 18, 2016	**(U)** FBI FLASH notification identified IP addresses targeting election offices.[180]
August 24, 2016	**(U)** State 2 Department of State received the FLASH from National Association of Secretaries of State.[181]
August 26, 2016	**(U)** State 2 Department of State forwarded FLASH to counties and advised them to block the IP addresses.[182] [redacted] Separately, [redacted] determined one of the listed IP addresses scanned its system.[183] [redacted] subsequently discovered suspected intrusion activity and contacted the FBI.[184]

[172] **(U)** *Ibid.*
[173] **(U)** *Ibid.*
[174] **(U)** *Ibid.*
[175] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[176] **(U)** *Ibid.*
[177] [redacted] *Ibid. See also* EB-0004893-LED
[178] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 42.
[179] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 7.
[180] **(U)** FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER, [redacted]
[181] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 4.
[182] **(U)** *Ibid.*, pp. 4-5.
[183] **(U)** *Ibid.*, p. 5.
[184] **(U)** *Ibid.*

August 31, 2016	[redacted] FBI opened its investigation on the [redacted] and "conducted outreach to State 2 county election officials to discuss individual security postures and any suspicious activity."[185] FBI outreach reveals that one State 2 county—County A—was scanned.[186]
September 30, 2016	[redacted] FBI held a conference call with county election officials to advise of the attempt to probe County A.[187] FBI also notified state and local officials of available DHS services.[188]
October 4, 2016	[redacted] County B's IT administrator contacted FBI regarding a potential intrusion.[189] According to the FBI, "Of particular concern, the activity included a connection to a county voting, testing, and maintenance server used for poll worker classes."[190]
October 14, 2016	**(U)** FBI shared County B indicators by issuing a FLASH.[191]
December 29, 2016	**(U)** DHS and FBI released a Joint Analysis Report (JAR) on the "GRIZZLY STEPPE" intrusion set; report represents the first IC attribution of state election-related systems to the Russians.[192]
[redacted]	[redacted]
June 2017	**(U)** DHS notified State 2 counties of a possible intrusion "as part of a broader notification to 122 entities identified as spearphishing victims in an intelligence report."[194]

[185] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 5.
[186] **(U)** *Ibid.*
[187] **(U)** *Ibid.*, pp. 5-6.
[188] **(U)** *Ibid.*, p. 6.
[189] **(U)** *Ibid.*
[190] **(U)** *Ibid.*
[191] **(U//**[redacted]**)** FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]
[192] **(U)** DHS/FBI, Joint Analysis Report, JAR-16-20296A, GRIZZLY STEPPE – Russian Malicious Cyber Activity, December 29, 2016.
[193] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[194] **(U)** *Ibid.*

July 2017	**(U)** FBI published a FLASH report warning of possible spearphishing.[195]
November 2017	**(U)** FBI and DHS participated in the first meeting of the State 2 elections task force.[196]
February 2018	**(U)** FBI requested direct engagement with Counties B, C, and D, including a reminder of available DHS services.[197]
March 2018	**(U)** FBI reports that "our office engaged" the affected counties through the local FBI field office.[198] The FBI could not provide any further detail on the substance of these engagements to the Committee.
May 29, 2018	[redacted] FBI provided a SECRET Letterhead Memo to DHS "formally advising of our investigation into the intrusion [redacted], the reported intrusion at County B, and suspected compromises of Counties C and D."[199]
June 11, 2018	**(U)** FBI reports that as of June 11, 2018, Counties A, B, C, and D had not accepted DHS services.[200]

[redacted]

[redacted]

---

[195] **(U)** FBI FLASH, Alert Number EB-000083-LD, TLP-AMBER, [redacted]. *See* DTS 2018-3174.
[196] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, p. 7.
[197] **(U)** *Ibid.*, p. 6.
[198] **(U)** *Ibid.*, p. 34.
[199] **(U)** *Ibid.*, pp. 8-9.
[200] **(U)** *Ibid.*, p. 20.
[201] [redacted] DTS 2018-2416; FBI Briefing on [State 2] Election Systems, June 25, 2018, pp. 20-21.
[202] [redacted] DHS briefing for SSCI staff, March 5, 2018.

- **(U)** State 2's Secretary of State and Election Director told the Committee in December 2017 that there was "never an attack on our systems." "We did not see any unusual activities. I would have known about it personally."[203] State 2 did not want to share with the Committee its cybersecurity posture, but state officials communicated that they are highly confident in the security of their systems.[204]

- **(U)** State 2's election apparatus is highly decentralized, with each county making its own decisions about acquiring, configuring, and operating election systems.[205]

- **(U)** As of August 9, 2018, DHS was complimentary of the steps State 2 had taken to secure its voting systems, including putting nearly all counties on the ALBERT sensor system, joining the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and using congressionally appropriated funds plus additional state funds to hire cybersecurity advisors.[206]

C. (U) Russian Efforts to Research U.S. Voting Systems, Processes, and Other Elements of Voting Infrastructure

[redacted]

- [redacted]

---

[203] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 2], December 1, 2017.
[204] **(U)** *Ibid.*
[205] **(U)** *Ibid.*
[206] **(U)** DTS 2018-2581, Memorandum for the Record, Telephone call with DHS, August 9, 2018.
[207] [redacted] FBI LHM, [redacted]
[208] **(U)** *Ibid.*, p. 5.
[209] [redacted] Note: "FISA" refers to electronic surveillance collected on a foreign power or an agent of a foreign power pursuant to the Foreign Intelligence Surveillance Act of 1978. This collection could have come from landlines, electronic mail accounts, or mobile phones used by personnel at a foreign embassy (i.e., an "establishment" FISA) or used by personnel associated with a foreign power (i.e., "agents of a foreign power"). This FISA collection would have been approved by the Foreign Intelligence Surveillance Court ("FISC"), effectuated by FBI, and then could also have been shared with NSA or CIA, or both, depending on the foreign target.

- It is unknown if Tarantsov attended the events.

D. (U) Russian Activity Directed at Voting Machine Companies

---

210 FBI LHM,
211 FBI LHM,
212 **(U)** *Ibid.*
213 **(U)** *Ibid.*, p. 3.
214 **(U)** *Ibid.*, p. 4.
215 **(U)** *Ibid.*
216 **(U)** *Ibid.*, p. 5.
217

[redacted] Russian government actors engaged in [redacted] attacks on election systems, [redacted].

- [redacted] FBI reported that "between December 2015 and June 2016, [redacted] DHS further told the Committee that malicious cyber actors had scanned [redacted] a widely-used vendor of election systems.[219]

- [redacted]

E. (U) Russian Efforts to Observe Polling Places

[redacted] Department of State were aware that Russia was attempting to send election observers to polling places in 2016. The true intention of these efforts is unknown.

- [redacted]

---

[218] [redacted] FBI Electronic Communication, [redacted]
[219] **(U)** DHS briefing for SSCI staff, March 5, 2018.
[220] [redacted]
[221] **(U)** *Ibid.*
[222] **(U)** *Ibid.*
[223] **(U)** NSA [redacted] DIRNSA, May 5, 2017, p. 3.
[224] **(U)** *Ibid.*, pp. 1-3.
[225] **(U)** FBI IIR [redacted]
[226] **(U)** *Ibid.*

- The Russian Embassy placed a formal request to observe the elections with the Department of State, but also reached outside diplomatic channels in an attempt to secure permission directly from state and local election officials.[227] For example, in September 2016, the State 5 Secretary of State denied a request by the Russian Consul General to allow a Russian government official inside a polling station on Election Day to study the U.S. election process, according to State 5 officials.[228]

n mission.[231]

nterfere

-

---

[227] (U) DTS 2018-2152, SSCI Transcript of the Interview of Andrew McCabe, Former Deputy Director of the Federal Bureau of Investigation, February 14, 2018, pp. 221-222.
[228] (U) *Ibid.*
[229] (U) *Ibid.*
[230] (U) *Ibid.*
[231] Email, sent November 4, 2016; from ; to: , , , ; subject: Kislyak Protest of FBI Tactics.
[232] Email, sent: September 13, 2016; from: subject: Russia visas/travel.
[233] (U) *Ibid.*
[234] (U) *Ibid.*
[235] Email Sent: Monday, November 7, 2016, 8:11 AM; from: ; to: subject: RE: Kislyak Protest of FBI Tactics --- SECRET//NOFORN.

F.

G. (U) Russian Activity Possibly Related to a Misinformation Campaign on Voter

---

236 DTS 2018-3952; MFR of Interview with Randy Coleman, December 5, 2018.
237 **(U)** NSA DIRNSA, May 5, 2017.
238 **(U)** *Ibid.*
239 **(U)** SSCI Interview with DHS and CTIIC, February 27, 2018, pp. 47-48.
240 FBI IIR
241 **(U/**) FBI LHM,
242 **(U)** *Ibid.*

(U) The declassified, January 6, 2017, Intelligence Community Assessment also highlighted preparations related to voter fraud, noting that Russian diplomats "were prepared to publicly call into question the validity of the results" and that "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory, judging from their social media activity."[245]

(U) During a 2017 election, State 17 saw bot activity on social media, including allegations of voter fraud, in particular on Reddit. State 17 had to try to prove later that there was no fraud.[246]

H. (U) Two Unexplained Events

1. (U) Cyber Activity in State 22

---

[243]
[244]
[245] **(U)** Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections*, January 6, 2017, p. 2.
[246] **(U)** *See* Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018. The Committee notes it is conducting a related investigation into the use of social media by Russian-government affiliated entities.
[247] **(U)** The Fusion Center model is a partnership between DHS and state, local, tribal, and territorial entities. They serve as a focal point for "the receipt, analysis, gathering, and sharing of threat-related information."
[248] **(U)** CTIIC Cyber Threat Intelligence Summary/Cyber Threats in Focus, Malicious Cyber Activity on Election-Related Computer Networks Last Spring Possibly Linked to Russia, October 7, 2016; DHS, IIR 4 019 0147 16, September 28, 2016.
[249] **(U)** *Ibid.*
[250] **(U)** *Ibid.*

[redacted]

2. (U) Cyber Activity in State 4

(U[redacted]) State 4 officials, DHS, and FBI in the spring and summer of 2016, struggled to understand who was responsible for two rounds of cyber activity related to election infrastructure. Eventually, one set of cyber activity was attributed to Russia and one was not.

(U[redacted]) First, in April of 2016, a cyber actor successfully targeted State 4 with a phishing scam. After a county employee opened an infected email attachment, the cyber actor stole credentials, which were later posted online.[251] Those stolen credentials were used in June 2016 to penetrate State 4's voter registration database.[252] A CTIIC product reported the incident as follows: "An unknown actor viewed a statewide voter registration database after obtaining a state employee's credentials through phishing and keystroke logging malware, according to a private-sector DHS partner claiming secondhand access. The actor used the credentials to access the database and was in a position to modify county, but not statewide, data."[253]

(U[redacted]) DHS analysis of forensic data provided by a private sector partner discovered malware on the system, and State 4 shut down the voter registration system for about eight days to contain the attack.[254] State 4 officials later told the Committee that that while the cyber actor was able to successfully log in to a workstation connected to election related infrastructure, additional credentials would have been needed for the cyber actor to access the voter registration database on that system.[255]

(U) At first, FBI told State 4 officials that the attack may have originated from Russia, but the ties to the Russian government were unclear. "The Bureau described the threat as 'credible' and significant, a spokesman for State 4 Secretary of State said."[256] State 4 officials also told press that the hacker had used a server in Russia, but that the FBI could not confirm the

---

[251] **(U)** [redacted].

[252] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 38.

[253] [redacted] Cyber Threat Intelligence Integration Center (CTIIC), Compromised State Election Networks, November 2, 2016, p. 1.

[254] **(U[redacted])** DHS IIR 4 005 0829 16, *A [redacted] U.S. State Government's Election System Targeted by Malicious Activity*, September 9, 2016; Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[255] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 4], December 1, 2017.

[256] **(U)** [redacted]

attack was tied to the Russian government.[257] DHS and FBI later assessed it to be criminal activity, with no definitive tie to the Russian government.[258]

[redacted] Subsequently, Russian actors engaged in the same scanning activity as seen in other states, but directed at a domain affiliated with a public library.[259] Officials saw no effective penetration of the system. DHS has low confidence that this cyber activity is attributable to the Russian intelligence services because the target was unusual and not directly involved in elections.[260] [redacted]

V. (U) RUSSIAN INTENTIONS

(U) Russian intentions regarding U.S. election infrastructure remain unclear. Russia might have intended to exploit vulnerabilities in election infrastructure during the 2016 elections and, for unknown reasons, decided not to execute those options. Alternatively, Russia might have sought to gather information in the conduct of traditional espionage activities. Lastly, Russia might have used its activity in 2016 to catalog options or clandestine actions, holding them for use at a later date. Based on what the IC knows about Russia's operating procedures and intentions more broadly, the IC assesses that Russia's activities against U.S. election infrastructure likely sought to further their overarching goal: undermining the integrity of elections and American confidence in democracy.

- **(U)** Former-Homeland Security Adviser Lisa Monaco told the Committee that "[t]here was agreement [in the IC] that one of the motives that Russia was trying to do with this active measures campaign was to sow distrust and discord and lack of confidence in the voting process and the democratic process."[262]

- [redacted] DHS representatives told the Committee that "[w]e see . . . Russians in particular obviously, gain access, learn about the environment, learn about what systems are interconnected, probing, the type of intelligence preparation of the environment that you would expect from an actor like the Russians. So certainly the context going forward

---

[redacted]

[258] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 40.

[259] **(U)** [redacted].

[260] [redacted] DHS/FBI Homeland Intelligence Brief, [redacted]

[261] **(U)** *Ibid.*

[262] **(U)** SSCI Transcript of the Interview with of Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 30.

is a concern of what they might have learned and how much more they know about the systems."[263]

- [redacted] Mr. McCabe told the Committee that it seemed to him like "classic Russian cyber espionage. . . . [They will] scrape up all the information and the experience they possibly can," and "they might not be effective the first time or the fifth time, but they are going to keep at it until they can come back and do it in an effective way."[264]

- [redacted] Mr. Daniel told the Committee:

> *While any one voting machine is fairly vulnerable, as has been demonstrated over and over again publicly, the ability to actually do an operation to change the outcome of an election on the scale you would need to, and do it surreptitiously, is incredibly difficult. A much more achievable goal would be to undermine confidence in the results of the electoral process, and that could be done much more effectively and easily. . . . A logical thing would be, if your goal is to undermine confidence in the U.S. electoral system—which the Russians have a long goal of wanting to put themselves on the same moral plane as the United States . . . one way would be to cause chaos on election day. How could you start to do that? Mess with the voter registration databases.*[265]

- [redacted] Ms. Monaco further echoed that concern:

> *Well, one of the things I was worried about—and I wasn't alone in this—is kind of worst-case scenarios, which would be things like the voter registration databases. So if you're a state and local entity and your voter registration database is housed in the secretary of state's office and it is not encrypted and it's not backed up, and it says Lisa Monaco lives at Smith Street and I show up at my [polling place] and they say 'Well we don't have Ms. Monaco at Smith Street, we have her at Green Street,' now there's difficulty in my voting. And if that were to happen on a large scale, I was worried about confusion at polling places, lack of confidence in the voting system, anger at a large scale in some areas, confusion, distrust. So there was a whole sliding scale of*

---

[263] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, p. 15.
[264] **(U)** DTS 2018-2152, SSCI Transcript of the Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, pp. 224-225.
[265] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, pp. 27, 34.

horribles just when you're talking about voter registration databases.[266]

- [redacted]

(U) Chaos on Election Day: Three Scenarios

[redacted] Mr. Daniel said that in the early fall of 2016, a policy working group was looking at three scenarios:

> *One was, could the Russians do something to the voter registration databases that could cause problems on Election Day? An example of that would be, could you go in and flip the digits in everybody's address, so that when they show up with their photo ID it doesn't match what's in the poll book? It doesn't actually prevent people from voting. In most cases you'll still get a provisional ballot, but if this is happening in a whole bunch of precincts for just about everybody showing up, it gives the impression that there's chaos.*[268]
>
> *A second one was to do a variant of the penetrating voting machines, except this time what you do is you do a nice video of somebody conducting a hack on a voting machine and showing how you could do that hack and showing them changing a voting outcome, and then you post that on YouTube and you claim you've done this 100,000 times across the United States, even though you haven't actually done it at all.*[269]
>
> *Then the third scenario that we looked at was conducting a denial of service attack on the Associated Press on Election Day, because pretty much everybody, all those nice maps that everybody puts up on all the different news services, is in fact actually based on Associated Press stringers at all the different precincts and locations. . . . It doesn't actually change anything, but it gives the impression that there's chaos.*[270]

---

[266] (U) SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, August 10, 2017, p. 28.
[267] [redacted]
[268] (U) SSCI Transcript of the Interview with Michael Daniel, Former Assistant to the President and Cybersecurity Coordinator, National Security Council, August 31, 2017, p. 33.
[269] (U) *Ibid.*, pp. 34-35.
[270] (U) *Ibid.*, p. 35.

VI. (U) NO EVIDENCE OF CHANGED VOTES OR MANIPULATED VOTE TALLIES

(U) In its review, the Committee has seen no indications that votes were changed, vote-tallying systems were manipulated, or that any voter registration data was altered or deleted, although the Committee and IC's insight is limited. Poll workers and voting monitors did not report widespread suspicious activity surrounding the 2016 election. DHS Assistant Secretary Jeanette Manfra said in the Committee's open hearing in June 2017 that "I want to reiterate that we do have confidence in the overall integrity of our electoral system because our voting infrastructure is fundamentally resilient." Further, all three witnesses in that hearing—Ms. Manfra, Dr. Liles, and FBI Assistant Director for Counterintelligence Bill Priestap—agreed that they had no evidence that votes themselves were changed in any way in the 2016 election.[271]

- **(U)** Dr. Liles said that DHS "assessed that multiple checks and redundancies in U.S. election infrastructure, including diversity of systems, non-internet connected voting machines, pre-election testing and processes for media, campaign and election officials to check, audit, and validate the results—all these made it likely that cyber manipulation of the U.S. election systems intended to change the outcome of the national election would be detected."[272] He later said "the level of effort and scale required to change the outcome of a national election would make it nearly impossible to avoid detection."[273]
- [redacted]
- **(U)** States did not report either an uptick in voters showing up at the polls and being unable to vote or a larger than normal quantity of provisional ballots.

(U) The Committee notes that nationwide elections are often won or lost in a small number of precincts. A sophisticated actor could target efforts at districts where margins are already small, and disenfranchising only a small percentage of voters could have a disproportionate impact on an election's outcome.

(U) Many state election officials emphasized their concern that press coverage of, and increased attention to, election security could create the very impression the Russians were seeking to foster, namely undermining voters' confidence in election integrity. Several insisted that whenever any official speaks publicly on this issue, they should state clearly the difference between a "scan" and a "hack," and a few even went as far as to suggest that U.S. officials stop

---

[271] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017.
[272] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 13.
[273] **(U)** *Ibid.*, p. 47.

talking about the issue altogether. One state official said, "We need to walk a fine line between being forthcoming to the public and protecting voter confidence."[274]

(U) Mr. Brennan described a similar concern in IC and policy discussions:

> *We know that the Russians had already touched some of the electoral systems, and we know that they have capable cyber capabilities. So there was a real dilemma, even a conundrum, in terms of what do you do that's going to try to stave off worse action on the part of the Russians, and what do you do that is going to . . . [give] the Russians what they were seeking, which was to really raise the specter that the election was not going to be fair and unaffected.*[275]

(U) Most state representatives interviewed by the Committee were confident that they met the threat effectively in 2016 and believed that they would continue to defeat threats in 2018 and 2020. Many had interpreted the events of 2016 as a success story: firewalls deflected the hostile activity, as they were supposed to, so the threat was not an issue. One state official told the Committee, "I'm quite confident our state security systems are pretty sound."[276] Another state official stated, "We felt good [in 2016]," and that due to additional security upgrades, "we feel even better today."[277]

(U) However, as of 2018, some states were still grappling with the severity of the threat. One official highlighted the stark contrast they experienced, when, at one moment, they thought elections were secure, but then suddenly were hearing about the threat.[278] The official went on to conclude, "I don't think any of us expected to be hacked by a foreign government."[279] Another official, paraphrasing a former governor, said, "If a nation-state is on the other side, it's not a fair fight. You have to phone a friend."[280]

(U) In the month before Election Day, DHS and other policymakers were planning for the worst-case scenario of efforts to disrupt the vote itself. Federal, state, and local governments created incident response plans to react to possible confusion at the polling places. Mr. Daniel said of the effort: "We're most concerned about the Russians, but obviously we are also concerned about the possibility for just plain old hacktivism on Election Day. . . . The incident response plan is actually designed . . . to help us [plan for] what is the federal government going to do if bad things start to happen on Election Day?"

[redacted] Mr. Daniel added that this was the first opportunity to exercise the process established under Presidential Policy Directive-41. "We asked the various agencies with lead

---

[274] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[275] **(U)** SSCI Transcript of the Interview with John Brennan, Former Director, CIA, held on Friday, June 23, 2017, p. 54.
[276] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.
[277] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[278] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 20], November 17, 2017.
[279] **(U)** *Ibid.*
[280] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.

responsibility, all right, give us your Election Day plan." That led to the creation of an Election Day playbook; steps included enhanced watch floor procedures, connectivity between FBI field offices and FBI and DHS, and an "escalation path" if "we needed to get to Lisa [Monaco] or Susan [Rice] in a hurry" on Election Day.[281]

VII. (U) SECURITY OF VOTING MACHINES

(U) The Committee review of Russian activity in 2016 highlighted potential vulnerabilities in many voting machines, with previous studies by security researchers taking on new urgency and receiving new scrutiny. Although researchers have repeatedly demonstrated it is possible to exploit vulnerabilities in electronic voting machines to alter votes,[282] some election officials dispute whether such attacks would be feasible in the context of an actual election.

- **(U)** Dr. Alex Halderman, Professor of Computer Science at the University of Michigan, testified before the Committee in June 2017 that "our highly computerized election infrastructure is vulnerable to sabotage and even to cyber attacks that could change votes."[283] Dr. Halderman concluded, "Voting machines are not as distant from the internet as they may seem."[284]

- **(U)** When State 7 decommissioned its Direct-Recording Electronic (DRE) voting machines in 2017, the IT director led an exercise in attempting to break into a few of the machines using the access a "normal" voter would have in using the machines.[285] The results were alarming: the programmed password on some of the machines was ABC123, and the testers were able to flip the machines to supervisor mode, disable them, and "do enough damage to call the results into question."[286] The IT director shared the results with State 21 and State 24, which were using similiar machines.[287]

- **(U)** In 2017, DEFCON[288] researchers were able to find and exploit vulnerabilities in five different electronic voting machines.[289] The WinVote machines, those recently decertified by State 7, were most easily manipulated. One attendee said, "It just took us a couple of hours on Google to find passwords that let us unlock the administrative

---

[281] **(U)** *Ibid.*, p. 82.
[282] **(U)** *See also, infra,* "Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities."
[283] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 117.
[284] **(U)** *Ibid.*, p. 110.
[285] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[286] **(U)** *Ibid.* The machines used were WinVote voting machines.
[287] **(U)** *Ibid.*
[288] **(U)** DEFCON is an annual hacker conference held in Las Vegas, Nevada. In July 2017, at DEFCON 25, the conference featured a Voting Machine Hacking Village ("Voting Village") which acquired and made available to conference participants over 25 pieces of election equipment, including voting machines and electronic poll books, for generally unrestricted examination for vulnerabilities.
[289] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, pp. 8-13.

functions on this machine."[290] A researcher was able to hack into the WinVote over WiFi within minutes using a vulnerability from 2003.[291] Once he had administrator-level access, he could change votes in the database. Researchers also discovered available USB ports in the machine that would allow a hacker to run software on the machine.[292] One said "with physical access to back [sic] of the machine for 15 seconds, an attacker can do anything."[293] Hackers were less successful with other types of machines, although each had recorded vulnerabilities.[294]

- **(U)** The 2018 DEFCON report found similar vulnerabilities, in particular when hackers had physical access to the machines. For example, hackers exploited an old vulnerability on one machine, using either a removable device purchasable on eBay or remote access, to modify vote counts.[295]

- **(U/[redacted])** DHS briefed the Committee in August 2018 that these results were in part because the hackers had extended physical access to the machines, which is not realistic for a true election system. Undersecretary Krebs also disagreed with reporting that a 17-year-old hacker had accessed voter tallies.[296] Some election experts have called into question the DEFCON results for similar reasons and pointed out that any fraud requiring physical access would be, by necessity, small scale, unless a government were to deploy agents across thousands of localities.

- **(U)** ES&S Voting Systems disclosed that some of its equipment had a key security vulnerability. ES&S installed remote access software on machines it sold in the mid-2000s, which allowed the company to provide IT support more easily, but also created potential remote access into the machines. When pressed by Senator Ron Wyden of Oregon, the company admitted that around 300 voting jurisdictions had the software. ES&S says the software was not installed after 2007, and it was only installed on election-management systems, not voting machines.[297] More than 50 percent of voters vote on ES&S equipment, and 41 states use its products.

---

[290] **(U)** Elizabeth Wise, "Hackers at DefCon Conference Exploit Vulnerabilities in Voting Machines," *USA Today*, July 30, 2017, https://www.usatoday.com/story/tech/2017/07/30/hackers-defcon-conference-exploit-vulnerabilities-voting-machines/523639001/.
[291] **(U)** Matt Blaze, et. al., *DEFCON 25: Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, September 2017, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20report.pdf, p. 4.
[292] **(U)** *Ibid.*, p. 9.
[293] **(U)** *Ibid.*
[294] **(U)** *Ibid.*, pp. 8-13.
[295] **(U)** Robert McMillian and Dustin Volz, "Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds," *Wall Street Journal*, September 27, 2018. The machine referenced is the ES&S Model 650, which ES&S stopped making in 2008 but is still available for sale.
[296] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018
[297] **(U)** Hacks, Security Gaps And Oligarchs: The Business of Voting Comes Under Scrutiny. Miles Parks, NPR, September 21, 2018.

(U) Advocates of electronic voting point out the flaws in paper ballots, like the potential for the introduction of fraudulent ballots or invalidated votes due to stains or extra marks. The Committee believes that any election system should be protected end-to-end, including against fraud.

(U) Direct-Recording Electronic (DRE) Voting Machine Vulnerabilities

(U) While best practices dictate that electronic voting machines not be connected to the internet, some machines are internet-enabled. In addition, each machine has to be programmed before Election Day, a procedure often done either by connecting the machine to a local network to download software or by using removable media, such as a thumb drive. These functions are often carried out by local officials or contractors. If the computers responsible for writing and distributing the program are compromised, so too could all voting machines receiving a compromised update. Further, machines can be programmed to show one result to the voter while recording a different result in the tabulation. Without a paper backup, a "recount" would use the same faulty software to re-tabulate the same results, because the primary records of the vote are stored in computer memory.[298]

(U) Dr. Halderman said in his June 2017 testimony before SSCI:

> *I know America's voting machines are vulnerable because my colleagues and I have hacked them repeatedly as part of a decade of research studying the technology that operates elections and learning how to make it stronger. We've created attacks that can spread from machine to machine, like a computer virus, and silently change election outcomes. We've studied touchscreen and optical scan systems, and in every single case we found ways for attackers to sabotage machines and to steal votes. These capabilities are certainly within reach for America's enemies.*
>
> *Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at the time the most widely used touch-screen DRE in the country and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win.*[299]

---

[298] **(U)** "Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots." Written Statement by J. Alex Halderman, June 21, 2017, citing S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots," *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop,* August 2007; B. Campbell and M. Byrne, "Now do Voters Notice Review Screen Anomalies?" *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop,* August 2009.

[299] **(U)** The machine was the Diebold AccuVote TS, which was still used statewide in at least one state as of 2017.

> *Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in* every single case, *they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes. That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk.*[300]

(U) In speaking with the Committee, federal government officials revealed concerns about the security of voting machines and related infrastructure. Former Assistant Attorney General for National Security John Carlin told the Committee:

> *"I'm very concerned about . . . our actual voting apparatus, and the attendant structures around it, and the cooperation between some states and the federal government."*[301] *Mr. Carlin further stated, "We've literally seen it already, so shame on us if we can't fix it heading into the next election cycles. And it's the assessment of every key intel professional, which I share, that Russia's going to do it again because they think this was successful. So we're in a bit of a race against time heading up to the two-year election. Some of the election machinery that's in place should not be."*[302]

(U) Mr. McCabe echoed these concerns, and noted that, in the last months before the election, FBI identified holes in the security of election machines, saying "there's some potential there."[303]

(U) As of November 2016, five states were using exclusively DRE voting machines with no paper trail, according to open source information.[304] An additional nine states used at least some DRE voting machines with no paper trail.[305]

- **(U)** State 20 has 21-year-old DRE machines. While the state is in the process of replacing its entire voting system, including these machines, State 20 is aiming to have the updates ready for the 2020 elections.

- **(U)** In State 21, 50 of 67 counties as of November 2017 used DRE voting machines.[306]

---

[300] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, pp. 116-117.
[301] **(U)** SSCI Transcript of the Interview with John Carlin, Former Assistant Attorney General for National Security, held on Monday, September 25, 2017, p. 86.
[302] **(U)** *Ibid.*, pp. 86-87.
[303] **(U)** DTS 2018-2152, SSCI Interview with Andrew McCabe, Former Deputy Director of the FBI, February 14, 2018, p. 221.
[304] **(U)** BallotPedia, *Voting Methods and Equipment By State*, https://ballotpedia.org/Voting_methods_and_equipment_by_state.
[305] **(U)** *Ibid.*
[306] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 21], November 17, 2017.

- **(U)** State 5 used paper-backed voting in only about half its machines and DRE voting machines without paper backup in the other half.[307]

- **(U)** Some states are moving to a hybrid model—an electronic voting machine with a paper backup, often in the form of a receipt that prints after the voter submits their vote. For example, State 12 uses some DREs, but all equipment is required to have a paper trail, and the paper ballot is the ballot of record.[308] State 12 also conducts a mandatory state-wide audit.[309] Similarly, State 13 uses some paper-based and some electronic machines, but all are required to have a paper trail.[310]

(U) The number of vendors selling voting machines is shrinking, raising concerns about a vulnerable supply chain. A hostile actor could compromise one or two manufacturers of components and have an outsized effect on the security of the overall system.

- [redacted] "My job," said Ms. Monaco when asked whether she was worried about voting machines themselves getting hacked, "was to worry about every parade of horribles. So I cannot tell you that that did not cross my mind. We were worried about who, how many makers. We were worried about the supply chain for the voting machines, who were the makers? . . . Turns out I think it's just Diebold—and have we given them a defensive briefing? So to answer your question, we were worried about it all."[311]

- [redacted] Mr. McCabe pointed out that a small number of companies have "90%" of the market for voting machines in the U.S. Before the 2016 election, [redacted] briefed a few of the companies on vulnerabilities,[312] but a more comprehensive campaign to educate vendors and their customers is warranted.

(U) Voluntary Voting System Guidelines

(U) Part of the voting reform implemented under The Help America Vote Act of 2002 was a requirement that the Election Assistance Commission create a set of specifications and requirements against which voting systems can be tested, called the Voluntary Voting System Guidelines (VVSG). The EAC adopted the first VVSG in December 2005. The EAC then tasked the Technical Guidelines Development Committee, chaired by the National Institute of Standards and Technology (NIST) and including members from NASED, with updating the guidelines. In March 2015, the EAC approved VVSG 1.1; in January 2016, the EAC adopted

---

[307] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 5], December 1, 2017.
[308] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[309] **(U)** *Ibid.*
[310] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[311] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 31.
[312] **(U)** SSCI Transcript of the Interview with Andy McCabe, Deputy Director of the FBI, held on Wednesday, February 14, 2018, pp. 220-221.

an implementation plan requiring that all new voting systems be tested against the VVSG 1.1 beginning in July 2017. VVSG 1.1 has since been succeeded by version 2.0, which was released for a 90-day public comment period on February 15, 2019. The EAC will compile the feedback for Commissioners to review shortly thereafter.[313] VVSG 2.0 includes the following minimum security guidelines:

- **(U)** An error or fault in the voting system software or hardware cannot cause an undetectable change in election results. (9.1)
- **(U)** The voting system produces readily available records that provide the ability to check whether the election outcome is correct and, to the extent possible, identify the root cause of any irregularities. (9.2)
- **(U)** Voting system records are resilient in the presence of intentional forms of tampering and accidental errors. (9.3)
- **(U)** The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations. (11.3)
- **(U)** The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records. (13.1)
- **(U)** The voting system limits its attack surface by reducing unnecessary code, data paths, physical ports, and by using other technical controls. (14.2)
- **(U)** The voting system employs mechanisms to protect against malware. (15.3)
- **(U)** A voting system with networking capabilities employs appropriate, well-vetted modern defenses against network-based attacks, commensurate with current best practice. (15.4)

(U) As of March 2018, 35 states required that their machines be certified by EAC, but compliance with the VVSG standards is not mandatory. Secretary Nielsen testified before the Committee that the United States should "seek for all states" to use the VVSG standards.[314]

---

[313] **(U)** *EAC Commissioners Unanimously Vote to Publish VVSG 2.0 Principles and Guidelines for Public Comment;* https://www.eac.gov/news/2019/02/15/eac-commissioners-unanimously-vote-to-publish-vvsg-20-principles-and-guidelines-for-public-comment/; February 15, 2019

[314] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 47.

VIII. (U) THE ROLE OF DHS AND INTERACTIONS WITH THE STATES

(U) The federal government's actions to address election security threats evolved significantly from the summer of 2016 through the summer of 2018. Contemporaneous with the Russian attacks, DHS and FBI were initially treating the situation as they would a typical notification of a cyber incident to a non-governmental victim. By the fall of 2016, however, DHS was attempting to do more extensive outreach to the states. Then in the fall of 2017, DHS undertook an effort to provide a menu of cyber support options to the states.

A. (U) DHS's Evolution

[redacted] For DHS and other agencies and departments tasked with intelligence collection or formulating policy options through the interagency process, the full scope of the threat began to emerge in the summer of 2016. Secretary Johnson told the Committee that "I know I had significant concerns by [summer of 2016] about doing all we could to ensure the cybersecurity of our election systems."[315] Mr. Daniel said in his interview that by the end of July, the interagency was focused on better protecting electoral infrastructure as part of a "DHS and FBI-led domestic effort."[316]

[redacted] Policymakers quickly realized, however, that DHS was poorly positioned to provide the kind of support states needed. Mr. Daniel said that interagency discussions about the threat "start[ed] a process of us actually realizing that, frankly, we don't actually have very much in the way of capability that we can directly offer the states"—a fact that the states themselves would later echo.[317]

- [redacted] Ms. Monaco said that DHS initially found a "pretty alarming variance in the number of voting registration databases and lack of encryption and lack of backup for all of these things."[318] Ms. Monaco added that "[i]n light of what we were seeing, in light of the intelligence we were getting briefed on, this was a very specific direction and decision to say we need to really accelerate this, put a significant push on resources and engagement at the senior-most levels."[319]

- [redacted] Mr. Daniel and the working group identified DHS's cyber teams as possible assistance to the states. "DHS had teams that could go and provide that support to the private sector. We've been doing that. That's a program that existed for years for critical

---

[315] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[316] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 28.
[317] **(U)** *Ibid.*, p. 38.
[318] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 19.
[319] **(U)** *Ibid.*, p. 21.

infrastructure companies. And we realized that we could repurpose [some of those teams], but we don't have that many of them . . . four or five. It was not very many."[320]

(U) DHS attempted a nuanced outreach to the states on the threat. Ms. Monaco highlighted a delicate balancing act with the interactions with states:

> *I know we tried very hard to strike a balance between engaging state and local officials and federal officials in the importance of raising cyber defenses and raising cybersecurity . . . and not sowing distrust in the system, both because, one, we believed it to be true that the system is in fact quite resilient because of what I mentioned earlier, which is the diffuse nature; and because we did not want to, as we described it, do the Russians' work for them by sowing panic about the vulnerability of the election.*[321]

(U) In an August 15, 2016, conference call with state election officials, then-Secretary Johnson told states, "we're in a sort of a heightened state of alertness; it behooves everyone to do everything you can for your own cybersecurity leading up to the election." He also said that there was "no specific or credible threat known around the election system itself. I do not recall—I don't think, but I do not recall, that we knew about [State 4] and Illinois at that point."[322] The Committee notes that this call was two months after State 4's system was breached, and more than a month after Illinois was breached and the state shut down its systems to contain the problem. During this call, Secretary Johnson also broached the idea of designating election systems as critical infrastructure.

(U) A number of state officials reacted negatively to the call. Secretary Johnson said he was "surprised/disappointed that there was a certain level of pushback from at least those who spoke up. . . . The pushback was: This is our—I'm paraphrasing here: This is our responsibility and there should not be a federal takeover of the election system."[323]

- **(U)** The call "does not go incredibly well," said Mr. Daniel. "I was not on the call, no, but all of the reporting back and then all of the subsequent media reporting that is leaked about the call shows that it did not go well." Mr. Daniel continued: "I was actually quite surprised . . . in my head, there is this: yes, we have this extremely partisan election going on in the background; but the Russians are trying to mess with our election. To me, that's a national security issue that's not dependent on party or anything else."[324]

---

[320] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 41.
[321] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, p. 29.
[322] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 13.
[323] **(U)** *Ibid.*, pp. 13-14.
[324] **(U)** *Ibid.*, p. 48.

- **(U)** Ms. Monaco also related how DHS received significant push back from the states and decided to "focus our efforts on really pushing states to voluntarily accept the assistance that DHS was trying to provide."[325]

- **(U)** States also reported that the call did not go well. Several states told the Committee that the idea of a critical infrastructure designation surprised them and came without context of a particular threat. Some state officials also did not understand what a critical infrastructure designation meant, in practical terms, and whether it would give the federal government the power to run elections. DHS also did not anticipate a certain level of suspicion from the states toward the federal government. As a State 17 official told the Committee, "when someone says 'we're from the government and we're here to help,' it's generally not a good thing."[326]

(U) Critical Infrastructure Designation

(U) One of the most controversial elements of the relationship between DHS and the states was the decision to designate election systems as critical infrastructure. Most state officials relayed that they were surprised by the designation and did not understand what it meant; many also felt DHS was not open to input from the states on whether such a designation was beneficial.

(U) Secretary Johnson remembers the first time he aired the possibility of a designation was on August 3, 2016. He went to a reporters' breakfast sponsored by the Christian Science Monitor and publicly "floated the idea of designating election infrastructure as critical infrastructure."[327] Then, on August 15, 2016, Secretary Johnson had a conference call with election officials from all 50 states. "I explained the nature of what it means to be designated critical infrastructure. It's not a mandatory set of [regulations], it's not a federal takeover, it's not binding operational directives. And here are the advantages: priority in terms of our services and the benefit of the protection of the international cyber norm."[328] Secretary Johnson continued: "I stressed at the time that this is all voluntary and it prioritizes assistance if they seek it."[329]

(U) Some states were vocal in objecting to the idea. In evaluating the states' response, DHS came to the conclusion that it should put the designation on hold, deciding it would earn more state trust and cooperation if it held off on the designation as critical infrastructure and perhaps sought more buy-in from the states at a later date.[330]

---

[325] **(U)** SSCI Transcript of the Interview with Lisa Monaco, Former Homeland Security Advisor, held on Thursday, August 10, 2017, SSCI interview of Lisa Monaco, August 10, 2017, p. 25.
[326] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with State 17, January 25, 2018.
[327] **(U)** SSCI Transcript of the Interview with Jeh Johnson, Former Secretary of Homeland Security, held on Monday, June 12, 2017, p. 10.
[328] **(U)** *Ibid.*, p. 14. For additional information on the definition of critical infrastructure in a cybersecurity context, *see* Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013.
[329] **(U)** SSCI Transcript of the Open Hearing on Election Security, March 21, 2018, p. 34.
[330] **(U)** *Ibid.*, p. 115.

(U) After the election, Secretary Johnson decided the time had come to make the designation. He held a follow-up call with NASS on the critical infrastructure designation in January 2017: "I didn't tell them I'm doing this the next day, but I told them I was close to making a decision. I didn't hear anything further [along the lines of additional, articulated objections], so the same day we went public with the [unclassified] version of the report,[331] I also made the designation."[332]

(U) Mr. Daniel summed up the rationale for proceeding this way: "I do believe that we should think of the electoral infrastructure as critical infrastructure, and to me it's just as critical for democracy as communications, electricity, water. If that doesn't function, then your democracy doesn't function. . . . To me that is the definition of 'critical.'"[333]

(U) In interviews with the Committee in late 2017 and early 2018, several states were supportive of the designation and saw the benefits of, for example, the creation of the Government Coordinating Council. Others were lukewarm, saying they had seen limited benefits for all the consternation officials said it had caused. Still others remained suspicious that the designation is a first step toward a federal takeover of elections.

B. (U) The View From the States

(U) For most states, the story of Russian attempts to hack state infrastructure was one of confusion and a lack of information. It began with what states interpreted as an insignificant event: an FBI FLASH notification on August 18, 2016, [redacted][334] Then, in mid-October, the MS-ISAC reached out to state IT directors with an additional alert about specific IP addresses scanning websites.[335] At no time did MS-ISAC or DHS identify the IP addresses as associated with a nation-state actor. Given the lack of context, state staff who received the notification did not ascribe any additional urgency to the warning; to them, it was a few more suspect IP addresses among the thousands that were constantly pinging state systems. Very few state IT directors informed state election officials about the alert.

---

[331] **(U)** Secretary Johnson was referring to the declassified version of the Intelligence Community Assessment, *Assessing Russian Activities and Intentions in Recent U.S. Elections,* January 6, 2017.
[332] **(U)** *Ibid.*, p. 46.
[333] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 98.
[334] **(U)** FBI FLASH, Alert Number T-LD1004-TT, TLP-AMBER, [redacted]
[335] **(U)** FBI FLASH, Alert Number T-LD1005-TT, TLP-AMBER, [redacted]; DHS/FBI JAR-16-20223, *Threats to Federal, State, and Local Government Systems,* October 14, 2016.

- **(U)** State 11 had a meeting with DHS officials, including the regional DHS cyber advisor, in August 2016, but according to State 11 officials, DHS did not mention any specific threat against election systems from a nation-state actor.[336]

- **(U)** State 13 reported that DHS contacted an affected county at one point, but never contacted the state-level officials.[337]

- **(U)** When they saw an IP address identified in the alerts had scanned their systems, State 6 and State 16 sent their logs to the MS-ISAC for analysis.[338] State 16 said it never received a response.[339]

(U) DHS, conversely, saw its efforts as far more extensive and effective. Ms. Manfra testified to SSCI that DHS "held a conference call where all 50 secretaries of state or an election director if the secretary of state didn't have that responsibility [participated], in August, in September, and again in October [of 2016], both high-level engagement and network defense products [sic]."[340] Mr. Daniel reported that "by the time Election Day rolls around, all but one state has taken us up on the offer to at least do scanning [,] so I want to give people credit for not necessarily sticking to initial partisan reactions and . . . taking steps to protect their electoral infrastructure."[341]

(U) States reported to the Committee that Election Day went off smoothly. For most state election officials, concerns about a possible threat against election systems dropped off the radar until the summer or fall of 2017. Many state election officials reported hearing for the first time that Russian actors were responsible for scanning election infrastructure in an estimated 21 states from the press or from the Committee's open hearing on June 21, 2017. During that hearing, in response to a question from Vice Chairman Warner inquiring whether all affected states were aware they were attacked, Ms. Manfra responded that "[a]ll of the system owners within those states are aware of the targeting, yes, sir."[342] However, when pressed as to whether election officials in each state were aware, the answer was less clear.[343]

- **(U)** In that hearing, Dr. Liles said DHS had "worked hand-in-hand with the state and local partners to share threat information related to their networks."[344]

---

[336] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 11], December 8, 2017.
[337] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[338] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 16], December 1, 2017.
[339] **(U)** *Ibid.* State 6 did not indicate whether they received feedback from DHS.
[340] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, June 21, 2017, p. 74.
[341] **(U)** SSCI Transcript of the Interview with Michael Daniel, Former Special Assistant to the President and Cybersecurity Coordinator, National Security Council, held on Wednesday, August 31, 2017, p. 49.
[342] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 28.
[343] **(U)** *Ibid.*, pp. 62-63.
[344] **(U)** *Ibid.*, p. 12.

- **(U)** Ms. Manfra said, "The owners of the systems within those 21 states have been notified." Senator King then asked, "How about the election officials in those states?" Ms. Manfra responded, "We are working to ensure that election officials as well understand. I'll have to get back to you on whether all 21 states ....[crosstalk]."[345]

- **(U)** Given Ms. Manfra's testimony and the fact that some election officials did not get a notification directly to their offices, election officials in many states assumed they were not one of the 21; some even issued press releases to that effect.[346]

(U) The disconnect between DHS and state election officials became clear during Committee interactions with the states throughout 2017. In many cases, DHS had notified state officials responsible for network security, but not election officials, of the threat. Further, the IT professionals contacted did not have the context to know that this threat was any different than any other scanning or hacking attempt, and they had not thought it necessary to elevate the warning to election officials.

(U) After the hearing, and in part to respond to confusion in the states, DHS held a conference call with representatives from 50 states in September 2017. In that call, DHS said they would contact affected states directly. State 8 state election officials noted that the call became "somewhat antagonistic."[347] State 17 officials reported that the phone call "just showed how little DHS knew about elections."[348] Several officials argued that all 50 states should be notified of who had been hacked. DHS followed up with one-to-one phone calls to states over the next several days.

- **(U)** Officials from some states reported being shocked that they were in fact one of the states, and further surprised that their states had supposedly been notified.

- **(U)** Most state officials found the conference calls lacking in information and were left wondering exactly what the threat might be. Several states said the DHS representatives could not answer any specific questions effectively.

(U) Following this series of difficult engagements, DHS set about trying to build relationships with the states, but it faced a significant trust deficit. Early follow-up interactions between state election officials and DHS were rocky. States reported that DHS seemed to have little to no familiarity with elections. For example, State 6 said that the DHS representatives they were assigned seemed to know nothing about State 6, and, when pressed, they admitted they were "just reading the spreadsheet in front of [them]."[349] State 8 reported that "we are spending

---

[345] **(U)** *Ibid.*, pp. 62-63.
[346] **(U)** State 8 said they put out a press release because DHS had said publicly that they had notified the 21 states, and "if you were one of the 21, you would know."
[347] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[348] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.
[349] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017.

a ton of time educating outside groups on how elections are run."[350] State 3 officials said, "DHS didn't recognize that securing an election process is not the same as securing a power grid."[351]

(U) By early 2018, State officials gave DHS credit for making significant progress over the next six months. States began to sign up for many of the resources that DHS had to offer, and DHS hosted the first meeting of the Government Coordinating Council required under the critical infrastructure designation. Those interactions often increased trust and communication between the federal and state entities. For example, DHS has identified a list of contacts to notify if they see a threat; that list includes both IT officials and election officials. State 9 described it as "quite a turnaround for DHS," and further stated that the Secretaries of State had been disappointed with how slowly DHS got up to speed on election administration and how slowly the notifications happened, but DHS was "quick with the *mea culpas* and are getting much better."[352]

(U) Not all of the engagements were positive, however. State 13 in early December 2017 still reported continued frustration with DHS, indicating to the Committee that it had not seen much change in terms of outreach and constructive engagement. As of summer 2017, according to State 13, "the lack of urgency [at DHS] was beyond frustrating."[353]

C. (U) Taking Advantage of DHS Resources

(U) As DHS has pursued outreach to the states, more and more have opened their doors to DHS assistance. DHS told the Committee that its goal has been relationship building and:

> *In the partnerships with the states and secretaries of states, state election directors, and at the local level, we're trying to shift them to a culture of more information security management, where they can now account for the integrity of their system, or, if something did happen . . . they know the full extent of what happened on their system. . . . We're providing vulnerability assessments and trend analysis, in addition to connecting them to the threat intelligence that we can, in order to evolve their . . . cyber culture.*[354]

(U) DHS's assistance can be highly tailored to need, and falls into roughly two buckets: remote cyber hygiene scans, which provide up to weekly reports, and on-site risk and vulnerability assessments. DHS also offers a suite of other services, including phishing campaign assessments. All these efforts seek to provide the states with actionable information to improve cyber hygiene, but DHS has been keen to avoid what could be perceived by the states as

---

[350] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[351] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 3], December 8, 2017.
[352] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[353] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 13], December 1, 2017.
[354] **(U)** SSCI interview with DHS and CTIIC, February 27, 2018, pp. 54-55.

unfunded mandates.[355] Some states requesting more intensive services have also experienced significant delays before DHS could send a team to assist.

- **(U)** By October 2018, DHS said 35 states, 91 local jurisdictions, and eight election system vendors had signed up for remote persistent scans.[356] All the requests for these scans have been fulfilled. "They can be turned on basically within the week," according to DHS.[357]

- **(U)** DHS said that as of October 2018, it had completed 35 in-depth, on the ground vulnerability assessments: 21 states, 13 localities, and one election system vendor. These assessments are one week off-site remote scans followed by a second week on site.[358]

- **(U)** Two states who completed the in-depth assessments reported in late 2017 they had had a good experience. State 12 officials said the team was "extremely helpful and professional."[359] State 10 said the review was a good experience, although DHS was somewhat limited in what it could do.[360] For example, DHS did a phishing email test that showed the training for employees had worked.[361] DHS gave "good and actionable recommendations." Although DHS "didn't really understand election systems when they came," they learned a lot.[362]

- **(U)** As of November 2017, State 6 and State 9 requested an on-site scan, but those scans were on track to be delayed past the August 2018 primaries.[363] State 7 was expecting a four-to-six month delay.[364] State 8 signed up for a checkup in October 2017 and was due to get service the following February.[365] As of January 2018, State 17 also had requested an on-site scan.[366]

(U) In a sign of improving relations between the states and DHS, two states that had elections in 2017 attempted to include DHS in the process more extensively than in the past. In State 17, a two-person DHS team sat with election officials during the 2017 special election and monitored the networks. Even though "their presence was comforting," they "really didn't do much." State 17 signed DHS's normal MOU, but also added its own clause to underscore the state's independence: a formal sunset on DHS's access to state systems, one week after the

---

[355] **(U)** *Ibid.*, p. 60.
[356] **(U)** *Ibid.*, p. 57.
[357] **(U)** DHS phone call with SSCI; October 16, 2018.
[358] **(U)** *Ibid.*
[359] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 12], December 1, 2017.
[360] **(U)** *Ibid.*
[361] **(U)** *Ibid.*
[362] **(U)** *Ibid.*
[363] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 6], November 17, 2017; Memorandum for the Record, SSCI Staff, Conference Call with [State 9], November 17, 2017.
[364] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[365] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 8], February 2, 2018.
[366] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 17], January 25, 2018.

election. State 7 reported their experience with DHS during the 2017 statewide election was quite good. DHS sat with election officials all day, which meant State 7 could pass messages quickly to NCCIC.

(U) In March 2018, Congress appropriated $380 million in funding for election security improvements. The funding was distributed under the formula laid out in the Help American Vote Act (HAVA) and was intended to aid in replacing vulnerable voting machines and improving cybersecurity. As of July 2018, 13 states said they intended to use the funds to buy new voting machines, and 22 said they have "no plans to replace their machines before the election—including all five states that rely solely on paperless electronic voting devices," according to a survey by Politico.[367]

IX. (U) RECOMMENDATIONS

1. (U) Reinforce States' Primacy in Running Elections*

(U) States should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information.

2. (U) Build a Stronger Defense, Part I: Create Effective Deterrence

(U) The United States should communicate to adversaries that it will view an attack on its election infrastructure as a hostile act, and we will respond accordingly. The U.S. Government should not limit its response to cyber activity; rather, it should create a menu of potential responses that will send a clear message and create significant costs for the perpetrator.

[redacted] **Ideally, this principle of deterrence should be included in an overarching cyber doctrine for the U.S. Government**. That doctrine should clearly delineate cyberespionage, cybercrime, and cyber attacks. Further, a classified portion of the doctrine should establish what the U.S. Government believes to be its escalation ladder in the cyber realm—what tools does it have, what tools should it pursue, and what should the limits of cyber war be. The U.S. strategic approach tends to overmatch adversaries with superior technology, and policymakers should consider what steps the U.S. will need to take to outstrip the capabilities of Russia, China, Iran, North Korea, and other emerging hostile actors in the cyber domain.

(U) U.S. cyber doctrine should serve as the basis for a discussion with U.S. allies and others about new cyber norms. Just as the international community has established norms and treaties about the use of technologies and weapons systems, the U.S. should lead a conversation about cyber norms and the limits of cyber activity with allies and others.

*The Committee's recommendation to "reinforce states' primacy in running elections" should be understood in reference to states' responsibility for election security, and not as pertaining to broader election issues, such as campaign finance laws or voting rights laws.

[367] **(U)** States Slow to Prepare for Hacking Threats, Eric Geller, Politico, July 18, 2018.

3. (U) Build a Stronger Defense, Part II: Improve Information Gathering and Sharing on Threats

The U.S. government needs to build the cyber expertise and capacity of its domestic agencies, such as DHS and FBI, and reevaluate the current authorities that govern efforts to defend against foreign cyber threats. NSA and CIA collection is, by law, directed outside the United States.

The U.S. government should invest in capabilities for rapid attribution of cyber attacks, without sacrificing accuracy. However, the IC needs to improve its ability to provide timely and actionable warning. Timely and accurate attribution is not only important to defensive information sharing, but will also underpin a credible deterrence and response strategy.

(U) The federal government and state governments need to create clear channels of communication two ways—down from the federal government to the state and local level, and up from the state and local officials on the front lines to federal entities. In 2016, DHS and FBI did not provide enough information or context to election officials about the threat they were facing, but states and DHS have made significant progress in this area in the last two years. For example, Secretary of Homeland Security Nielsen testified to the Committee in March 2018 that "today I can say with confidence that we know whom to contact in every state to share threat information. That capability did not exist in 2016."[369]

(U) A key component of information sharing about elections is security clearances for appropriate officials at the state and local level. DHS and its partners can effectively strip classified information off of cyber indicators, which can then be passed to technical staff at the state level, but in order for those indicators to not get lost in the multitude of cyber threats those professionals see on a daily basis, senior officials at the state and local levels need to know the

---

[368]

[369] (U) SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p. 16.

context surrounding the indicators. State officials need to know why a particular threat is of significant concern, and should be prioritized. That context could come from classified information, or states could come to understand that threat information DHS passes them is more serious than that received through other sources. DHS's goal is to obtain clearances for up to three officials per state.[370] As of August 2018, DHS had provided a clearance to 92 officials[371]; as of late 2017 all state election officials had received interim secret clearances or one-day read-ins for secret-level briefings.[372] DHS, along with ODNI and FBI, also hosted state and local election officials for a SECRET-level briefing on the sidelines of the biannual NASS and NASS-ED conferences in Washington, DC in February 2018. In March, Amy Cohen, Executive Director of NASS-ED testified in front of the Committee that, "It would be naïve to say that we received answers to all our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community as well as to our concerns."[373] The Committee recommends DHS continue providing such briefings and improve the quality of information shared.

(U) Fundamental to meaningful information sharing, however, is that state officials understand what they are getting. New inductees to the world of classified information are often disappointed—they expected to see everything laid out in black and white, when intelligence is often very gray, with a pattern discernable only to those who know where to look and what conclusions to draw. Those sharing the intelligence should manage expectations—at the SECRET level, officials are likely to see limited context about conclusions, but not much more.

(U) Federal officials should work to declassify information, for the purpose of providing warning to appropriate state and local officials, to the greatest extent possible. If key pieces of context could be provided at a lower classification level while still protecting classified information, DHS and its partners should strive to do so.

4. (U) Build a Stronger Defense, Part III: Secure Election-Related Cyber Systems

(U) Despite the expense, cybersecurity needs to become a higher priority for election-related infrastructure. The Committee found a wide range of cybersecurity practices across the states. Some states were highly focused on building a culture of cybersecurity; others were severely under-resourced and relying on part-time help.

(U) The Committee recommends State officials work with DHS to evaluate the security of their election systems end-to-end and prioritize implementing the following steps to secure voter registration systems, state records, and other pre-election activities. The Committee additionally recommends that State officials:

---

[370] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.15.
[371] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[372] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p 15, 26.
[373] **(U)** SSCI Transcript of the Open Hearing on Election Security, held on March 21, 2018, p.113.

- **(U)** Identify the weak points in their networks, like under-resourced localities. State 7 said they are not worried about locations like larger counties when it comes to network security, but they are worried about "the part-time registrar who is also the town attorney and the town accountant and is working out of a 17th century jail." [374]

- **(U)** Undertake security audits of state and local voter registration systems, ideally utilizing private sector entities capable of providing such assistance. State and local officials should pay particular attention to the presence of high severity vulnerabilities in relevant web applications, as well as highly exploitable vulnerabilities such as cross-site scripting and SQL injection.

- **(U)** Institute two-factor authentication for user access to state databases.

- **(U)** Install monitoring sensors on state systems. As of mid-2018, DHS's ALBERT sensors covered up to 98% of voting infrastructure nationwide, according to Undersecretary Krebs.[375]

- **(U)** Include voter registration database recovery in state continuity of operations plans.

- **(U)** Update software in voter registration systems. One state mentioned that its voter registration system is more than ten years old, and its employees will "start to look for shortcuts" as it gets older and slower, further imperiling cybersecurity.

- **(U)** Create backups, including paper copies, of state voter registration databases.

- **(U)** Consider a voter education program to ensure voters check registration information well prior to an election.

(U) DHS in the past year has stepped up its ability to assist the states with some of these activities, but DHS needs to continue its focus on election infrastructure and pushing resources to the states.

(U) The Committee recommends DHS take the following steps:

- **(U)** Create an advisory panel to give DHS expert-level advice on how states and localities run elections. The Government Coordinating Council, created as part of the critical infrastructure designation, could serve as a venue for educating DHS on what states do and what they need.

---

[374] **(U)** Memorandum for the Record, SSCI Staff, Conference Call with [State 7], January 25, 2018.
[375] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

- **(U)** Create guidelines on cybersecurity best practices for elections and a public awareness campaign to promote election security awareness, working through EAC, NASS, and NASED, and with the advisory panel.

- **(U)** Develop procedures and processes to evaluate and routinely provide guidance on relevant vulnerabilities associated with voting systems in conjunction with election experts.

- **(U)** DHS has already created a catalog of services they can provide to states to help secure states' systems. DHS should maintain the catalog and continue to update it as it refines its understanding of what states need.

- **(U)** Expand capacity so wait times for services, like voluntary vulnerability assessments, are manageable and so that DHS can maintain coverage on other critical infrastructure sectors. Robbing resources from other critical infrastructure sectors will eventually create unacceptable new vulnerabilities.

- **(U)** Work with GSA to establish a list of approved private-sector vendors who can provide services similar to those DHS provides. States report being concerned about "vultures" —companies who show up selling dubious cyber solutions. That being said, some states will be more comfortable having a private sector entity evaluate their state systems than a federal agency.

- **(U)** Continue to build the resources of the newly established EI-ISAC. States have already found this information sharing service useful, and it could serve as a clearinghouse for urgent threat information. As of August 2018, the EI-ISAC had over 1,000 members with participants in all 50 states.[376]

- **(U)** Continue training for state and local officials, like the table-top exercise conducted in August of 2018 that brought together representatives from 44 states, localities, and the federal government to work through an election security crisis.[377] The complexity of the scenario encouraged state and local officials to identify serious gaps in their preparations for Election Day.

5. (U) Build a Stronger Defense, Part IV: Take Steps to Secure the Vote Itself

(U) Given Russian intentions to undermine the credibility of the election process, states should take urgent steps to replace outdated and vulnerable voting systems. When safeguarding the integrity of U.S. elections, all relevant elements of the government—including at the federal, state, and local level—need to be forward looking and work to address vulnerabilities before they are exploited.

---

[376] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.
[377] **(U)** DHS, Press release: DHS Hosts National Exercise on Election Security, August 15, 2018.

- **(U)** As states look to replace HAVA-era machines that are now out of date, they should purchase more secure voting machines. Paper ballots and optical scanners are the least vulnerable to cyber attack; at minimum, any machine purchased going forward should have a voter-verified paper trail and remove (or render inert) any wireless networking capability.

- **(U)** States should require that machines purchased from this point forward are either EAC certified or comply with the VVSG standards. State purchasers should write contracts with vendors to ensure adherence to the highest security standards and to demand guarantees the supply chains for machines are secure.

- **(U)** In concert with the need for paper ballots comes the need to secure the chain of custody for those ballots. States should reexamine their safeguards against insertion of fraudulent paper ballots at the local level, for example time stamping when ballots are scanned.

- **(U)** Statistically sound audits may be the simplest and most direct way to ensure confidence in the integrity of the vote.[378] States should begin to implement audits of election results. Logic and accuracy tests of machines are a common step, but do not speak to the integrity of the actual vote counting. Risk-limiting audits, or some similarly rigorous alternative, are the future of ensuring that votes cast are votes counted. State 8, State 12, State 21, State 9, State 2, State 16, and others already audit their results, and others are exploring additional pilot programs.[379] However, as of August 2018, five states conducted no post-election audit and 14 states do not do a complete post-election audit.[380] The Committee recognizes states' concern about the potential cost of such audits and the necessary changes to state laws and procedures; however, the Committee believes the benefit of having a provably accurate vote is worth the cost.

- **(U)** States should resist pushes for online voting. One main argument for voting online is to allow members of the military easier access to their fundamental right to vote while deployed. While the Committee agrees states should take great pains to ensure members

---

[378] **(U)** Election experts point out, however, that audits could create a new vector for election-related lawsuits. Complainants could allege that the audit was done improperly, or that the audit process reflected bias.

[379] **(U)** State 8 passed a law to audit starting in 2018, with random precinct sampling. State 12 does state-wide audits. State 21 audits 2% of ballots, randomly selected. State 9 picks 210 of 4100 precincts at random for an audit. State 2 hand-counts ballots in randomly selected precincts and uses automated software to test. A States law on ballot storage can't accommodate risk-limiting audits. Instead, they use ClearBallot software. They upload images of ballots to an external hard drive and send it to ClearBallot. ClearBallot is blind to who won and independently evaluates the results. In addition, the company can identify problems with scanners; for example, when a fold in absentee ballots recorded as a vote. Cybersecurity experts still doubt, however, that this type of procedure is secure.

[380] **(U)** DTS 2018-3275, Summary of 8/22/2018 All Senators Election Security Briefing, August 28, 2018.

of the military get to vote for their elected officials, no system of online voting has yet established itself as secure.[381]

- **(U)** DHS should work with vendors of election equipment to educate them about the vulnerabilities in both the machines and the supply chains for the components of their machines. Idaho National Lab is already doing some independent work on the security of a select set of voting machines, developing a repeatable methodology for independently testing the security of such systems.

- **(U)** The Department of State should work with FBI and DHS to warn states about foreign efforts to access polling places outside normal channels in the future and remain vigilant about rejecting aberrant attempts.

- **(U)** The Associated Press is responsible for reporting unofficial, initial election results on election night and is a critical part of public confidence in the voting tally. States and DHS should work with the AP and other reporting entities to ensure they are both secure and reporting accurate results.

- **(U)** The Committee found that, often, election experts, national security experts, and cybersecurity experts are speaking different languages. Election officials focus on transparent processes and open access and are concerned about introducing uncertainty into the system; national security professionals tend to see the threat first. Both sides need to listen to each other better and to use more precise language.

6. (U) Assistance for the States

(U) State officials told the Committee the main obstacle to improving cybersecurity and purchasing more secure voting machines is cost. State budgets are stretched thin by priorities that seem more urgent on a daily basis and are far more visible to constituents.

(U) In March 2018, Congress appropriated $380 million in funds under the HAVA formula for the states. As of August 2018, states had begun to allocate and spend that money for items such as cybersecurity improvements.

(U) The Committee recommends the EAC, which administers the grants, regularly report to Congress on how the states are using those funds, whether more funds are needed, and whether states have both replaced outdated voting equipment and improved

---

[381] **(U)** Dr. Halderman in his testimony before the Committee said, "I think that online voting, unfortunately, would be painting a bullseye on our election system. Today's technology just does not provide the level of security assurance for an online election that you would need in order for voters to have high confidence. And I say that having myself . . . hacked an online voting system that was about to be used in real elections, having found vulnerabilities in online voting systems that are used in other countries. The technology just isn't ready for use." *See* SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 152.

cybersecurity. More funds may be needed, as the allocation under the HAVA formula did not prioritize replacing vulnerable electronic-only machines.

- **(U)** States should be able to use grant funds to improve cybersecurity in a variety of ways, including hiring additional IT staff, updating software, and contracting with vendors to provide cybersecurity services. "Security training funded and provided by a federal entity such as the EAC or DHS would also be beneficial in our view,"[382] an official from Illinois testified.

- **(U)** Funds should also be available to defray the cost of instituting audits.

- **(U)** States with vulnerable DRE machines with no paper backup should receive urgent access to funding. Dr. Halderman testified that replacing insecure paperless voting machines nationwide would cost $130 to $400 million dollars. Risk-limiting audits would cost less than $20 million a year.[383]

7. [redacted] **Build a Credible** [redacted]

[redacted]

[redacted]

[382] **(U)** SSCI Transcript of the Open Hearing on Russian Interference in the 2016 U.S. Elections, held on Wednesday, June 21, 2017, p. 114.
[383] **(U)** *Ibid.*, p. 119.

MINORITY VIEWS OF SENATOR WYDEN

(U) The role of the federal government

(U) The Committee report describes Russian attacks on U.S. election infrastructure in 2016 and lays out many of the serious vulnerabilities that exist to this day. These vulnerabilities pose a direct and urgent threat to American democracy which demands immediate congressional action. The defense of U.S. national security against a highly sophisticated foreign government cannot be left to state and county officials. For that reason, I cannot support a report whose top recommendation is to "reinforce[ ] state's primacy in running elections."

(U) Congress's constitutional role in regulating federal elections is well-established. In response to an inquiry from the bipartisan leadership of the U.S. Senate, the General Accounting Office (GAO) wrote that "[w]ith regard to the administration of federal elections, Congress has constitutional authority over both congressional and presidential elections."[1] Indeed, pursuant to the Elections Clause of the U.S. Constitution,[2] Congress's authority over congressional elections is "paramount to that of the states." As the GAO report details, Congress has repeatedly passed legislation related to the administration of elections on topics such as the timing of federal elections, voter registration, absentee voting requirements, disability access, and voting rights.

(U) If there was ever a moment when Congress needed to exercise its clear constitutional authorities to regulate elections, this is it. America is facing a direct assault on the heart of our democracy by a determined adversary. We would not ask a local sheriff to go to war against the missiles, planes and tanks of the Russian Army. We shouldn't ask a county election IT employee to fight a war against the full capabilities and vast resources of Russia's cyber army. That approach failed in 2016 and it will fail again. The federal government's response to this ongoing crisis cannot be limited offers to provide resources and information, the acceptance of which is voluntary. If the country's elections are to be defended, Congress must also establish mandatory, nation-wide cybersecurity requirements.

(U) Security of voting machines

(U) Experts are clear about the measures necessary to protect U.S. elections from cyber manipulation.[3] Absent an accessibility need, most voters should hand-mark paper ballots. For voters with some kind of need, ballot marking devices that print paper ballots should be available. Risk-limiting audits must be also be required. Currently, however, only Virginia, Colorado and Rhode Island meet these requirements.[4] These critical reforms must be adopted

---

[1] "Elections. The Scope of Congressional Authority in Election Administration," General Accounting Office, March 2001, prepared in response to a joint inquiry from Senator Trent Lott, Republican Leader; Senator Tom Daschle, Democratic Leader; Senator Mitch McConnell, Chairman, and Senator Christopher Dodd, Ranking Member, of the Senate Committee on Rules and Administration.

[2] Article I, Section 4, Clause 1

[3] Securing the Vote; Protecting American Democracy; National Academy of Sciences, Engineering and Medicine, September 2018

[4] National Conference of State Legislatures, Post-Election Audits, January 3, 2019. Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018. Oregon requires paper ballots and the Oregon State Senate has passed a bill requiring risk-limiting audits.

throughout the country, which is why, on June 27, 2019, the House of Representatives passed H.R. 2722, the Securing America's Federal Elections (SAFE) Act. The security of the country's voting machines depends on this legislation being signed into law.

(U) The Committee, in recommending basic security measures like paper ballots and audits, notes that there is currently "a wide range of cybersecurity practices across the states." Indeed, the data is deeply concerning and highlights the need for mandatory, nation-wide standards. For example, the Committee rightly highlights the vulnerabilities of Direct-Recording Electronic (DRE) Voting Machines, noting that, without a paper trail, there would be no way to conduct a meaningful "recount" and compromises would remain undetected. As of November 2018, however, there were still four states in which every single county relied on DREs without voter verified paper audit trail printers (VVPAT) and, in an additional eight states, there were multiple counties that relied on DREs without a VVPAT.[5] Gaps in the deployment of VVPATs, which are far less secure than hand-marked paper ballots, demonstrate that even bare minimum security best practices are not being met in many parts of the country.

(U) In addition, 16 states have no post-election audits of any kind, while many others have insufficient or perfunctory audits. Only four states have a statutory requirement for risk-limiting audits, while two states provide options for counties to run different kinds of audits, one of which is a risk-limiting audit.[6] Next year, a third state will provide that option. In other words, the vast majority of states have made no moves whatsoever toward implementing minimum standards that experts agree are necessary to guarantee the integrity of elections.

(U) The Committee rightly identifies problems with vendors of voting machines, noting vulnerabilities in both the machines and the supply chains for machine components. Currently, however, the federal government has no regulatory authority that would require these vendors to adhere to basic security practices.[7] Only general federal requirements that states and localities use paper ballots and conduct audits will ensure that the risk posed by voting machines provided by private vendors to states and localities can be contained. The stakes could not be more clear. As Homeland Secretary Kirstjen Nielsen testified to the Committee, "If there is no way to audit the election, that is absolutely a national security concern."[8]

(U) Registration databases and election night reporting websites

(U) Two additional components of the U.S. election infrastructure require immediate, mandatory cybersecurity fixes. The first are voter registration databases. The Committee received testimony about successful Russian exfiltration of databases of tens of thousands of voters.[9] Expert witnesses also described the chaos that manipulated voter registration data could cause should voters arrive at the polls and find that their names had been removed from the rolls.

---

[5] Verifiedvoter.org. The Verifier – Polling Place Equipment – November 2018.

[6] The four states are Colorado, Nevada, Rhode Island, and Virginia. National Conference of State Legislatures, Post-Election Audits, January 3, 2019.

[7] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.

[8] Testimony of Homeland Security Secretary Kirstjen Nielsen, March 21, 2018.

[9] Testimony of Connie Lawson, President-elect, National Association of Secretaries of State, and Secretary of State, State of Indiana; testimony of Steve Sandvoss, Executive Director of Illinois State Board of Elections, June 21, 2017; Illinois Voter Registration System Database Breach Report.

As one expert testified, this form of interference "could be used to sabotage the election process on Election Day."[10]

(U) The Committee report describes a range of cybersecurity measures needed to protect voter registration databases, yet there are currently no mandatory rules that require states to implement even minimum cybersecurity measures. There are not even any voluntary federal standards.

(U) An additional component of the U.S. election infrastructure that requires immediate, mandatory cybersecurity measures are the election night reporting websites run by the states. The Committee heard testimony about a Russian attack on Ukraine's web page for announcing results. That attacked allowed the Russians to use misinformation that left Ukraine in chaos for days after the election. As the Committee's expert witness warned, "[w]e need to look at that playbook. They will do it to us."[11] Like voter registration databases, election results websites are not subject to any mandatory standards. Both of these critical vulnerabilities, as well as vulnerabilities of voting machines, must be addressed by the U.S. Congress through the passage of S. 2238, the Senate version of the SAFE Act.

(U) Given the inconsistent, and at times non-existent adherence to basic cybersecurity among states and localities, I cannot agree with the Committee's conclusion that "the country's decentralized election system can be a strength from a cybersecurity perspective." Until election security measures are required of every state and locality, there will be vulnerabilities to be exploited by our adversaries. The persistence of those vulnerabilities has national consequences. The manipulation of votes or voter registration databases in any county in the country can change the result of a national election. The security of the U.S. election system thus hinges on its weakest links – the least capable, least resourced local election offices in the country, many of which do not have a single full-time employee focused on cybersecurity.

(U) Every American has a direct stake in the cybersecurity of elections throughout the country. Congress has an obligation to protect the country's election system everywhere. If there were gaps in the defense of our coastline or air space, members would ensure that the federal government close them. Vulnerabilities in the country's election cybersecurity require the same level of national commitment.

(U) Cybersecurity vulnerabilities and influence campaigns

(U) The cybersecurity vulnerabilities of the U.S. election system cannot be separated from Russia's efforts to influence American voters. As the January 2017 Intelligence Community Assessment (ICA) concluded, and as the Committee report notes, the Russians were "prepared to publicly call into question the validity of the results" and "pro-Kremlin bloggers had prepared a Twitter campaign, #DemocracyRIP, on election night in anticipation of Secretary Clinton's victory." This plan highlights an additional reason why nation-wide election cybersecurity standards are so critical. If Russia's preferred candidate does not prevail in the 2020 election, the

---

[10] Testimony of Alex J. Halderman, Professor of Computer Science and Engineering, University of Michigan, June 21, 2017.

[11] Testimony of Eric Rosenbach, Co-Director of the Belfer Center for Science and International Affairs, Harvard Kennedy School, March 21, 2018.

Russians may seek to delegitimize the election. The absence of any successful cyber intrusions, exfiltrations or manipulations would greatly benefit the U.S. public in resisting such a campaign.

(U) While not formally part of the U.S. election infrastructure, the devices and accounts of candidates and political parties represent an alarming vulnerability in the country's overall election system. Russia's campaign of hacking the emails of prominent political figures and releasing them through Wikileaks, Gucifer 2.0, and DCLeaks was probably its most effective means of influencing the 2016 election. The Committee has received extensive testimony about these operations, the vulnerabilities that allowed them to occur, and the threat those vulnerabilities pose to the integrity of American democracy.[12] Yet little has been done to prevent it from happening all over again. S. 1569, the Federal Campaign Cybersecurity Assistance Act of 2019, addresses these vulnerabilities head on by authorizing political committees to provide cybersecurity assistance to candidates, campaigns and state parties.

(U) These vulnerabilities extend to the U.S. Senate, most of whose members are or will be candidates for reelection or for other positions. As a November 2018 Senate report noted, there is "mounting evidence that Senators are being targeted for hacking, which could include exposure of personal data."[13] Private communications and information reside on personal accounts and devices. Passage of S. 890, the Senate Cybersecurity Protection Act, will authorize the Senate Sergeant at Arms to protect the personal devices and accounts of Senators and their staff and help prevent the weaponization of their data in campaigns to influence elections.

(U) Assessments related to the 2016 election

(U) I have also submitted these Minority Views to address assessments related to Russian activities during the 2016 election. According to the January 2017 ICA, DHS assessed that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." An assessment based on observations is only as good as those observations and this assessment, in which DHS had only moderate confidence,[14] suffered from a lack of observable data. As Acting Deputy Undersecretary of Homeland Security for National Protection and Programs Directorate, Jeannette Manfra, testified at the Committee's June 21, 2017, hearing, DHS did not conduct any forensic analysis of voting machines.

(U) DHS's prepared testimony at that hearing included the statement that it is "likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected." The language of this assessment raises questions, however, about DHS's ability to identify cyber manipulation that could have affected a very close national election, particularly given DHS's acknowledgment of the "possibility that individual or isolated cyber

---

[12] See, for example, Committee hearing, March 30, 2017.

[13] Senators' Personal Cybersecurity Working Group Report, submitted by the Senators' Personal Cybersecurity Working Group, November 2018.

[14] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following Committee hearing, June 21, 2017.

intrusions into U.S. election infrastructure could go undetected, especially at local levels."[15] Moreover, DHS has acknowledged that its assessment with regard to the detection of outcome-changing cyber manipulation did not apply to state-wide or local elections.[16]

(U) Assessments about manipulations of voter registration databases are equally hampered by the absence of data. As the Committee acknowledges, it "has limited information on the extent to which state and local election authorities carried out forensic evaluation of registration databases." Assessments about Russian attacks on the administration of elections are also complicated by newly public information about the infiltration of an election technology company. Moreover, as the Special Counsel reported, the GRU sent spear phishing emails to "Florida county officials responsible for administering the 2016 election" which "enabled the GRU to gain access to the network of at least one Florida county government."[17]

(U) The Committee, in stating that it had found no evidence that vote tallies were altered or that voter registry files were deleted or modified, rightly noted that the Committee's and the IC's insight into this aspect of the 2016 election was limited. I believe that the lack of relevant data precludes attributing any significant weight to the Committee's finding in this area.

(U) The Committee's investigation into other aspects of Russia's interference in the 2016 election will be included in subsequent chapters. I look forward to reviewing those chapters and hope that outstanding concerns about members' Committee staff access to investigative material, including non-compartmented and unclassified information, will be resolved.

---

[15] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[16] Responses to Questions for the Record from Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis; and Jeanette Manfra, Acting Deputy Undersecretary, National Protection and Programs Directorate, following.Committee hearing, June 21, 2017.

[17] Report on the Investigation Into Russian Interference In The 2016 Presidential Election, Special Counsel Robert S. Mueller III, March 2019

ADDITIONAL VIEWS OF SENATORS HARRIS, BENNET, AND HEINRICH

(U) The Russian government's attack on the 2016 election was the product of a deliberate, sustained, and sophisticated campaign to undermine American democracy. Russian military intelligence carried out a hacking operation targeting American political figures and institutions. The Internet Research Agency—an entity with ties to Russian President Vladimir Putin—used social media to sow disinformation and discord among the American electorate. And, as this report makes clear, individuals affiliated with the Russian government launched cyber operations that attempted to access our nation's election infrastructure, in some cases succeeding.

(U) The Russian objectives were clear: deepen distrust in our political leaders; exploit and widen divisions within American society; undermine confidence in the integrity of our elections; and, ultimately, weaken America's democratic institutions and damage our nation's standing in the world. The Committee did not discover evidence that Russia changed or manipulated vote tallies or voter registration information, however Russian operatives undoubtedly gained familiarity with our election systems and voter registration infrastructure—valuable intelligence that it may seek to exploit in the future.

(U) The Committee's report does not merely document the wide reach of the Russian operation; the report reveals vulnerabilities in our election infrastructure that we must collectively address. We do not endorse every recommendation in the Committee's report, and we share some of our colleagues' concerns about the vulnerability that we face, particularly at the state level, where counties with limited resources must defend themselves against sophisticated nation-state adversaries. Nevertheless, the report as a whole makes an important contribution to the public's understanding of how Russia interfered in 2016, and underscores the importance of working together to defend against the threat going forward.

(U) It is critical that state and local policymakers study the report's findings and work to secure election systems by prioritizing cybersecurity, replacing outdated systems and machines, and implementing audits to identify and limit risk. The Intelligence Community and other federal agencies must improve efforts to detect cyberattacks, enhance coordination with state and local officials, and develop strategies to mitigate threats. And, critically, Congress must take up and pass legislation to secure our elections. We must provide states the funding necessary to modernize and maintain election infrastructure, and we must take commonsense steps to safeguard the integrity of the vote, such as requiring paper ballots in all federal elections.

(U) Our adversaries will persist in their efforts to undermine our shared democratic values. In order to ensure that our democracy endures, it is imperative that we recognize the threat and make the investments necessary to withstand the next attack.