OSET INSTITUTE

Position Paper

Released 04.July 2019

Rebutting Recent Congressional Member Commentary

House Administration Committee Markup Session for HR 2722

Prepared for:
U.S. Election Administration & Public Policy Leadership

Prepared By:
E. John Sebes, Co-Founder & CTO
Gregory A. Miller, Co-Founder & COO

Overview

Recently, the OSET Institute monitored the June 21, 2019 Committee on House Administration Markup meeting on HR 2722, the SAFE Act. That markup session, in its entirety, can be viewed at this URL: https://youtu.be/QCiD5VPrOGU. Several assertions by one of the Committee members, Congressman Barry Loudermilk of Georgia, ran considerably counter to the facts and evidence on the topics of HR 2722—so much so, the Institute's Chief Technology Officer, E. John Sebes, reviewed every one of Congressman Loudermilk's comments. This Paper is a result of Mr. Sebes' review, which was motivated by the fact that at the outset of his remarks, Rep. Loudermilk asserted a background, and impliedly subject matter expertise, in cybersecurity.

Specifically, at the 41:19 time-mark, Congressman Loudermilk makes the following assertion of his particular subject-matter expertise: "*I have a background in information technology, cybersecurity, and in the intelligence community*." However, OSET Institute researchers have been *unable* to verify the Congressman acquired such skills or credentials in cybersecurity, or election technology digital security.

Regardless of whether or not the Congressman possesses the knowledge he asserts, the fact that a member of Congress is on the record asserting that he is qualified and then proceeds to offer the comments reviewed in this Paper should be of serious concern to all. The comments' correctness are implied by his representations of his subject matter expertise, which makes his comments all the more important to examine.

During this time of growing distrust in the processes and technology of election administration, mired in confusion, disinformation, and mischaracterization of many aspects and elements, the OSET Institute believes it is imperative to maintain clear intellectual honesty about all matters of election and voting administration systems characteristics including, but not limited to, their integrity and security.

Accordingly, in a rare public rebuttal, the OSET Institute's Chief Technology Officer, sets forth in this Paper a comment-by-comment review of each of Congressman Loudermilk's assertions through the one hour and 30 minute Markup Session held on the 21st of June, the record of which was video compiled and recorded and is available at the URL provide above.

The OSET Institute takes no pleasure whatsoever in producing this rebuttal to the Congressman's contributions in his capacity as an important and valued member of the House Administration Committee. This paper is without any partisan agenda. Any Congressional members' comments, regardless of political affiliation, that clearly run counter to the facts and evidence on the very serious matter of election security need to be called out, clarified, or corrected.

The OSET Institute Chief Technology Officer begins the remainder of this Paper with a review of six topical assertions (*paraphrased as close as possible, but which can be verified against the audio at the URL provided above*). Following that, Mr. Sebes provides comments in Part II on each comment made by the Honorable Congressman Loudermilk at the timestamp marks as they occurred.

I. Topical Review of Congressman Loudermilk's Assertions

1. Russia attacked voter registration systems systems, not voting machines; we are focusing on a non-problem at the expense of a problem.

- It's not a zero sum game between securing databases and having auditable voting—Federal funds can apply to both, and in fact, did in the case of the $380M HAVA allocation in 2018. Congressman Loudermilk's assertion that the legislation is forcing States to spend scarce funds on the wrong problem is contradicted by the main goal of providing Federal funds.
- It is factually incorrect to assert that there is a lack of verified Russian attacks on ballot casting and counting infrastructure. DHS, FBI, and other investigative sources asserting that there is a lack of evidence of such does not equal a proof of absence. Any cyber security specialist or expert understands this ***vital*** distinction. And such is the very catalyst for performing post election deep forensic analyses of machinery. This observation suggests argumentation in bad faith at worst, and not actually understanding the DHS or DNI assessments at best.
- Cyber-attacks on voting machinery are ***not*** the main point, but rather a distraction. The reason for paper and audits is that 1] ***any*** kind of computing equipment can malfunction in the future (whether from operator error, software bugs, or nation state adversaries) regardless of what happened or didn't in the past, and 2] we need the ability for humans to detect and correct malfunctions.
- Russian attacks, or the lack thereof, are ***not*** the defining principle of whether people should cross check the work of computers.

2. Fraud vulnerabilities of paper ballots

- While the Congressman refers multiple times to “ballot harvesting” and signature match or lack thereof, as the types of voter fraud that paper ballots are vulnerable to, but that DREs are not, he fails to recognize that ballot harvesting and signatures are part of the absentee voting process. Any risks in those cases are not affected by decisions about how people vote in person with or without paper.
- Turning to electoral fraud, all voting methods have fraud risks. Paperless electronic voting has greater risks due to technical attacks to alter digital vote totals. I am not convinced that Rep. Loudermilk understands the *difference* between risk of fraud and technological risk.

3. DREs and Paper Ballots

- The Congressman refers at times to paper backups and paper trails, and eventually a paper ballot that is printed by a DRE (i.e., "Paper ballot generated after the DRE"). That's properly called a Ballot Marking Device, and it is the current standard recommendation to replace DREs, which “directly record” votes *without* a durable paper ballot of record.
- Rep. Loudermilk refers to *voter verification* of paper ballots after printing as the “*best way to determine if a machine isn't working right*.” No, that is putting the requirement for error detection on to voters, who cannot and should not be relied on to make an accurate assessment in every case.
- Voter *verifiability* is important, but voter *verification* is *no* substitute for a statistical sample of all ballots, and not just the ballots that a few diligent voters might check.

4. Anonymous voting

- The Congressman refers to DREs as "verifying to the person that is present and pressing the button" and a "voter signs" after checking. DREs do not do anything with the identity of the voter, and voters do not sign ballots.
- For a Congressman who is concerned about voter fraud, it is unclear if Rep. Loudermilk understands the concept of ballot anonymity to prevent bribery and coercion.

5. Automation benefits

- The Congressman asserts that DREs are faster and better. Some usability studies have found that in some cases paper/pen voting is actually faster. Regardless, rapidity of voting is not the issue, but rather whether DRE voting can be trusted to accurately capture and store voters' intent 100% accurately and reliably, and the facts are numerous that they cannot.
- Furthermore, while the many historical reasons why we shifted to electronic voting might have included efficiency for some stakeholders, a historical reason of efficiency does not change the fact that paper records and audits remain necessary.

6. Audits

- There are far more than four (4) types of audits—there are many more in various state's election code and practices.
- Risk Limiting Audit (RLA) is the least effort and cost method, so there's little value in asking States to re-invent wheels.
- Asking or expecting States to define *their own standards* might enable States to decide not to ensure that true paper ballots are required, and not to require meaningful audits. The majority of States today have *already* decided not to require binding audits that are statistically sound. So we know that the status quo in much of the country is to *not* have the ability for people to detect when voting machinery has malfunctions. Flexibility might lead to no effective method of detection of machine malfunction in some States.

II. Specific Comments Made Throughout the Hearing

Turning to the Congressman's comments at specific timestamps in the recorded Hearing, OSET Institute CTO, John Sebes offers the following observations.

41:00-42:50: Agree: Russia attacked Voter Registration systems. Disagree: that Russia did *not* attack voting systems—this is "unknowable." DHS has been very careful to state that there is no (*unclassified*) evidence of the latter, and the OSET Institute knows from its work with elements of the national security apparatus that this distinction was purposefully made.

Disagree: with the assertion that the fact Voter Registration systems were attacked *suggests* that voting system technology is *not* worthy of improvement.

42:50-43:20: Regarding paper ballots as more susceptible to fraud, Congressman Loudermilk refers to "*ballot harvesting*," which is a form of voter fraud that recently was notable in North Carolina. But the point is relevant *only to absentee voting*. Risks of voter fraud in absentee voting are *not* mitigated in the slightest by the use of DREs ("Direct Recording Electronics") for in-person voting. Congressman Loudermilk also complains that some minority doesn't like signature verification, which is also an issue with voter fraud in absentee voting, and isn't mitigated by any practices for in-person voting.

The key issue, regardless of fraud risks to paper-based absentee voting, is how to improve in-person voting to reduce technological risk. We should be concerned that Congressman Loudermilk appears to not understand the difference between *risk of fraud* and *technological risk*—a basic cybersecurity principle.

However, if we consider the matter of electoral fraud, all voting methods are at risk, and DREs enable technical attacks to create wholesale fraud.

43:24 "All for paper verification" is an assertion good to hear, but this assertion is *not* consistent with Congressman Loudermilk's subsequent remarks about DREs.

43:34 Disagree: “DREs verify the person that is pressing the button.” Incorrect. In fact, DREs do *not* verify anything about the person pressing the button. We should be concerned that Congressman Loudermilk does not understand the role of DREs in enforcing the requirement of anonymous ballots.

43:18 Disagree: “Automation allows more rapid voting.” Some usability studies have found that in some cases paper/pen voting is faster. Regardless, rapidity of voting is not the issue, but rather whether DRE voting can be trusted to accurately capture and store voters' intent 100% accurately and reliably.

43:48 Agree: “Paper backup is required when a voter uses a voting machine.” Disagree: “The paper backup *is* an audit.” Incorrect. An audit is a process by an independent party comparing the paper record to the digital record. Disagree: “The voter signs the paper backup.” Incorrect, that violates ballot anonymity. We should be concerned that Congressman Loudermilk seems unclear on the concept of private voting to produce ballots that are *not* tied to a specific person.

44:16 Disagree: “Problem with paper being the primary record, we got away from that to get automation that is more secure.” Congressman Loudermilk still hasn't explained what the security problem is that DREs are intended to solve. But we *do* know that DREs are simply computers, with inherent security problems of their own.

45:12 Agree: “Russian goal is discord and distrust. However, Congressman Loudermilk advocates for use of voting machines where attacks cannot be detected, which by itself is a great opportunity for propaganda about election technology cyber attacks because there is no way to refute claims that such occurred.

45:50 Disagree: Congressman Loudermilk returns to the notion that “ballot harvesting” is the threat, but without apparently understanding that polling place automation does nothing about ballot harvesting. Accordingly, the Congressman still has not stated any cyber security benefit of DREs.

49:50 Disagree: Again, Congressman Loudermilk claims without evidence that voting machines were not hacked, and concludes that voting systems need no security help. *One ordinarily skilled in the science and process of I.T. Security would never make such an assertion*. This assertion also ignores the fact that voting machines can malfunction (*whether from operator error, software bugs, or nation state adversaries intervention*) in the future, regardless of what happened or didn't in the past, and that we need the ability for humans to detect and correct malfunctions. Russian attacks or the lack thereof are not the defining principle of whether people should crosscheck the work of computers.

57:12 "Paper ballot generated after the DRE." That is properly called a “Ballot Marking Device,” and it is the current standard recommendation to replace DREs, which (as the acronym name suggests) “directly record” votes *without* a durable paper ballot of record (“DRE” is “Direct Recording Electronics”).

57:18 Disagree: “The best way to determine if a voting machine is not working right is for the voter to examine a BMD's paper ballot.” Incorrect. That is putting the requirement for error detection onto voters, who can cannot (and should not) be relied on to make an accurate assessment in every case. Moreover, today there is no provision for a voter to repudiate a ballot that (s)he believes or perceives was produced in error.

Congressman Loudermilk goes on to assert there is the opportunity the change what's on the paper ballot. However, if the voter is going mark a paper ballot, what's the value of the voting machine? "Efficiency" is the Congressman Loudermilk’s assertion, but that's not what's at issue, security is the issue at hand.

57:44 Disagree: (paraphrasing) “Force States to spend limited funds changing their voting machines.” This is patently incorrect. The objective is to provide Federal funding to mitigate the limitations of State funds availability.

58:01 Disagree: “4 types of audits.” In fact, there are many more types of audits in various State's election code and practices. Letting States define their own standards will enable some States to decide not to require meaningful audits. The majority of States, so far, have already decided *not* to require binding audits. So, we know that the status quo in much of the country is to *not* have the ability for people to detect when voting machinery has malfunctions. Flexibility might lead to no effective method of detection of machine malfunction in some States.

1:12:07 Agree: “Superior to have a machine that prints a ballot that the voter could check right there.” However, it is no substitute for a statistical sample of all ballots, not just the ballots that a few diligent voters might check.

1:12:52 Disagree: “The reason we went to electronic voting is efficiency.” This is incorrect. There were many reasons for the shift to digital means, most notably to address accessibility issues. However, this accrued a side effect of paperless voting machines for which there is no malfunction detection ability. The lack of ability to detect errors is unacceptable, regardless of historical reasons for adoption.

In Summary

The OSET Institute monitored the June 21, 2019 Committee on House Administration Markup meeting on HR 2722, the SAFE Act. Several assertions by one of the Committee members, Congressman Barry Loudermilk of Georgia, ran considerably counter to the facts and evidence on the topics of HR 2722—so much so, the Institute’s Chief Technology Officer, E. John Sebes, reviewed every one of Congressman Loudermilk’s comments.

At the 41:19 time-mark of the Session, Congressman Loudermilk asserts, “*I have a background in information technology, cybersecurity, and in the intelligence community*.” OSET Institute researchers have been *unable* to verify his acquired skills or credentials in cybersecurity, or election technology digital security.

The critical concern is Congressman Loudermilk is claiming information technology security expertise for which there is little to no public record of such, and nothing in this Congressional record of his comments supports such knowledge; unfortunately, it supports the opposite.

Regardless of whether or not the Congressman possesses the knowledge he asserted, the fact that a member of Congress is on the record asserting that he is qualified and then proceeds to offer the comments reviewed in this Paper should be of serious concern to all. The comments' correctness are implied by his assertion of subject matter expertise, which makes them all the more important to examine.

During this time of growing distrust in the processes and technology of election administration, mired in confusion, disinformation, and mischaracterization of many aspects and elements, the OSET Institute believes it is imperative to maintain clear intellectual honesty about all matters of election and voting administration systems characteristics including, but not limited to, their integrity and security.

There were six topical areas of comments by Congressman Loudermilk in which, unfortunately, he exhibited a significant lack of understanding about voting technology and the current processes of election administration. Those topics included:

1. Russia attacks on our electoral infrastructure in 2016
2. Fraud vulnerabilities of paper ballots
3. Direct Recording Electronics and the relationship to paper ballots
4. Anonymous voting
5. Automation benefits
6. Audits

The OSET Institute sincerely appreciates the civility and substantive debate presented in the Markup Session held on the 21st of June. We further appreciate that there are members on both sides of the political aisle interested in advancing responsible election security initiatives. However, in so doing, intellectual honesty remains imperative.

End Note

The OSET Institute believes it is imperative for Congress to have members who are information technology adept in this digital age. Thus, when a member asserts such domain expertise this raises our attention, and leads us to want to learn more. In the case of the Honorable Congressman Loudermilk, here is what we were able to determine:

- In the 114th Congress, Rep. Loudermilk served as a member of two important U.S. House Committees: (1) Homeland Security, and (2) Space, Science and Technology.
- Rep. Loudermilk also has served as Chairman of the SST Subcommittee on Oversight, and was a member of the Homeland Security Committee's Special Task Force on Combating Terrorist and Foreign Fighter Travel.

- Rep. Loudermilk holds an Associate Degree in Telecommunications Technology (1987), and a Bachelor of Science in Occupational Education and Information Systems Technology (1992).
- The Congressman also served in the U.S. Air Force for eight years (1984-1992; during which time he apparently completed his education) serving as a "Communications Computer Supervisor." [1] He was discharged at the rank of Staff Sargent.

Research suggests that the Congressman's trajectory was from college and the Air Force and into politics. It is possible that he acquired cybersecurity skills along the way; however, given his IT education at the undergraduate level was in the mid-to-late 1980s, any information technology security knowledge he acquired would be pre-commercial Internet era, and significantly dated 30+ years later.

In any event, Congressman Loudermilk's education, experience, or training could *not* have included anything about election technology specific security, because topically such did not become a seriously contemplated technical issue until at best, 2005. During that time, the Congressman was beginning his public office career in the Georgia State House of Representatives representing the 14th District, having succeeded Tom Knox. And prior to that he had been in political party administration from 2001 onward.

Accordingly, while the OSET Institute appreciates any and every member of Congress aspiring to be technically adept or at least competent in issues of the digital age such as cybersecurity, great care must be taken in making such representations. Even unintentional misrepresentation can induce misleading presumptions that assertions, commentary, or opinions carry a greater weight of credibility or correctness than is intellectually honest.

This Paper has gone to careful lengths to clarify (*and agree where possible with*) the remarks of Congressman Loudermilk during the 21st June Markup Session for HR 2722 because the OSET Institute believes it is imperative that everyone clearly understand the challenges, issues, and opportunities before America in defense of democracy—particularly as it applies to critical election infrastructure.

1 https://trustthevote.org/wp-content/uploads/2019/07/LoudermilkDischargeRecord.pdf