House State Government Committee
April 15, 2021

Written Testimony of Lt. Colonel (ret) Anthony Shaffer
President, London Center for Policy Research

Thank you, members of the House State Government Committee, for allowing me to submit written testimony in connection with this Joint Meeting to discuss the integrity of Pennsylvania's election system from the national security perspective.

I write to address the national security implications of Pennsylvania's the perception and observed reality of the vulnerabilities presented in the tabulation, amalgamation and transmission of voting results. Because of these urgent concerns, it is imperative for the Pennsylvania General Assembly to assess, audit, evaluate and act to address the material weaknesses, and perceptions of election integrity failures before the 2022 election cycle.

I have worked the election integrity issue for the past decade. I have testified on the election security issue in multiple of states and three times in Pennsylvania.
I am a cyber operations expert, having worked as a Senior Intelligence Operations Office with the FBI, NSA and CIA to develop both offensive and defensive cyber capabilities. I created and directed Task Force STRATUS IVY, the first undercover offensive Cyber Unit at the Department of Defense. I continue to advise the Pentagon, the Army War College and multiple members of the current Cabinet on cyber threat and intervention issues. Frequently I am interviewed on this and related threat issues throughout the spectrum media - electronic and print. Because of my 40 years of experience in national security, cyber security, and cyber defense my purpose here today is twofold: First, I am here to warn the Pennsylvania General Assembly that the Keystone State's elections are an open target for foreign interference. We cannot afford to have the results of elections questioned, especially in an important swing state like Pennsylvania, which is certainly a target of opportunity for anyone wanting to undermine the validity of U.S. elections. Pennsylvanians deserve to be confident that their votes will be cast as intended and counted as cast.

I last testified before the House Committee on Veterans Affairs & Emergency Preparedness Senate Committee on Veterans Affairs & Emergency Preparedness Joint Informational Meeting on February 11, 2019 - and had private consultations with members of both parties just after the hearing where I provided detailed assessments and answered questions. I have included my previous testimony as part of this submission.

As someone who has spent a career in the trenches of information operations, perception management and weaponization of technology, I understand the threat and I am here to urge you to examine the issues that have been identified and work to answer and resolve them factually and efficiently.

By way of background, I have supported Pennsylvania adopting optical scan systems that incorporates a voter-marked paper ballot, marked either with a pen or pencil or with a ballot marking device and where that ballot is retained for recounts or audits. Optical scan systems leverage the speed of the computer to report unofficial results quickly. The paper ballots provide a way to check that the computer reported the results accurately either by sampling them in an audit or hand counting the paper ballots if necessary.

Today, my concern is not only about the domestic election integrity but the obvious vulnerability this presents to foreign actors and adversaries.

And this leads to the main point I wish to make: Failure to establish election integrity will likely enable hostile actors to learn from our mistakes and work to establish the capability to severely disrupt and create doubt in the results of our elections. I ask - What could be more critical to the USA than the integrity of our entire political system?   And hostile opponents of our democratic republic know that this is the key feature of our free and fair election system – and our adversaries are working to establish ways to undermine confidence and sew discontent.

Adversaries will examine the results and target them – they have seen the chaos that can come from even the perception of fraud.

Most vital to our election system is accuracy and integrity - and this is the main topic I wish to cover. It is a truism that any system devised by man can be corrupted by man. This is particularly true of technological innovation. Digitization of some aspects of voting have improved processing of results and timely reporting. But our addiction to "rapid gratification" of results has now opened the door for vulnerabilities. The moving and reporting of voting data, even when hand marked paper ballots are used, has created points of potential weakness in the integrity of the vote. There is still points of access of even the most secure voting system to the threat of insiders who abuse the technology or bypass the security protocols necessary to prevent intrusion or the perception of compromise.

The real problem is that we cannot see electrons, nor can we know for sure that data sent by electronic means is always totally accurate – especially if there are questions as to the honesty of election officials and their method of counting ballots. This creates space and opportunity for foreign adversaries to develop offensive capabilities to disrupt and potentially modify results.

Technology is a tool for the user - it is only as good as the people who use the technology.

It is for this reason I continue to believe hand-marked ballots are the best solution if there is a viable auditing the paper ballots used in our elections.

There are vulnerabilities we know a foreign adversary may target – these things are hard drives, USB Drives, access to voting machine certification and operations. There are other 'human in the loop' issues such as Chain of custody and manual counting. While it would be a significant challenge for a foreign adversary or outside actor to directly impact on a chain of custody, they

can and do conduct "information operations" that can create, enhance and amplify the perception of compromise or corruption of a vote count.

So, a basic question must be that if we are going to continue to use paper ballots, with markings visible to the human eye, why are we bothering with converting them to a digital format, and thus rendering those marks invisible?

The tabulation of ballots – hand marked and mailed, have become a contested issue in multiple states. The digitized record created during the counting/tabulation process appears to be a vulnerability that was observed by credible election observers and is now the subject of several lawsuits.

Time does not permit me to recount the observed instance of anomalies, potential fraud that has been stipulated by election observers such as Greg Stenstrom and other poll observers– but I have reviewed their affidavits and spoken to him and other witnesses who persist in their belief that the integrity of the vote counting was compromised in the 2020 election.

The observations (or in this case the failure to permit observations in the case of some election observers) has created space for the perception of election irregularity and potential fraud. Greg Stenstrom documented specific observations of the misuse and breaking of security protocols regarding hardware- the actual vote tabulation machines, the hard drives and the USB VDrives.

Not only does this create a perception of weakness of the Pennsylvania voting system, this presents a whole target set for foreign and international threats to examine, develop access to, and use for their own purpose to potentially change, modify or otherwise modify voting results to create chaos or change outcomes.

We, the London Center, did a preliminary review of election anomalies – the report of this I will make available to the Pennsylvania legislature as an addendum to my testimony.

My own investigations of anomalies from the November-December 2020 period remain unresolved – one of them resulted in a conversation with Attorney General William Barr over my preliminary results of the investigation into the potential bypassing of Pennsylvania's election integrity system. We are hoping to continue this investigation with Pennsylvania's support at some point.

It is my judgement that Pennsylvania must undertake a non-partisan effort to Investigate, resolve and fix, if necessary, all material weaknesses in the election process.
The legislature must establish, and remain firm in their resolve, the controls and oversight system, no matter what happens – this IS the Constitutional responsibility. Neither the Judiciary or the Executive branch in your state has the authority to override or weaken the protections that you all in the legislature establish.

One thing is certain. The vulnerabilities observed in the Pennsylvania voting system WILL be exploited by foreign adversaries in the future.

Conclusion/recommendation:

1. Enforcement of State Laws and Regulations MUST be foremost – legal observers must be granted and ensured access to all aspects of vote counting and aggregation.

2. Tabulation and consolidation of results must be publicly visible. To this end, electronic systems, including the internet, have a likely role, but only if the public can monitor, audit and view the entire system, live and in real time.

3. Even with hand marked paper ballots the tabulation, and transmission remains vulnerable – the perception, as is what I believe to be the observed reality, is the voting system in Pennsylvania is NOT secure, and with the state of current technology, cannot be secured until a full audit and "red team" evaluation is done to validate the process and audits of problematic counties/precincts completed.

4. Bad actors spend billions of dollars and man-years of effort developing software to hack electronic voting systems or conduct "information operations" to cause doubt in the results. We can spend far less in defense against such hostile acts, but we must do so now.

5. The Primary and Official ballot of record should only be the paper ballot and it must be 100% human readable.

    1. Each paper ballot should have a human readable and unique serial number…like money, so it can be tracked from issuance to final disposition.

    2. Each voter should have the option to retain a physical copy of their completed ballot.

6. Recognize that, despite best efforts, some degree of fraud will occur AND any such fraud is most likely to target population centers, because that's where it can be more easily hidden among the larger numbers. Therefore, the legislature should consider a system to apportion the electors across the state. With the current "winner takes all" system, fraud in any one geographical area [especially population centers] can more easily disenfranchise legitimate voters outside of those population centers. It's a method to encapsulate or isolate the effect of fraud, incompetence, or otherwise to the geography where it occurs.

7. Mathematical validations (tests) as part of the voting equipment certification must be included to ensure that the software being used is the same as that publicly disclosed in combination with hard copy "risk limiting audits" within key precincts to further bolster confidence in the counting/tabulation process.

It is my judgment that Pennsylvania must act PRUDENLY to conduct audits, review process and procedures of the 2020 election, standardize the best practices and create enforcement mechanisms to ensure oversight and access for election observers to monitor the tabulation process so that the sacred right to vote for all citizens of Pennsylvania is protected.

****DRAFT****

House Committee on Veterans Affairs & Emergency Preparedness
Senate Committee on Veterans Affairs & Emergency Preparedness
Joint Informational Meeting
February 11, 2019
1 p.m. G-50 Irvis Office Building
Commonwealth Avenue, Harrisburg, PA

Written Testimony of
Lt. Colonel Anthony Shaffer
February 8, 2019

Thank you Chairmen Barrar, Regan, Sainato and Williams, and members of the Committee for allowing me to submit written testimony in connection with this Joint Meeting to discuss national security interests and voting machines. I write to address the national security implications of Pennsylvania's continued use of insecure and vulnerable paperless voting systems. Because of these urgent concerns, it is imperative for the Pennsylvania General Assembly to appropriate adequate funding to assist counties in replacing their systems before the 2020 election.

I am a cyber operations expert, having worked as a Senior Intelligence Operations Office with the FBI, NSA and CIA to develop both offensive and defensive cyber capabilities. I created and directed Task Force STRATUS IVY, the first undercover offensive Cyber Unit at the Department of Defense. I continue to advise the Pentagon, the Army War College and multiple members of the current Cabinet on cyber threat and intervention issues. Frequently I am interviewed on this and related threat issues throughout the spectrum media - electronic and print because of my 40 years of experience in national security, cyber security, and cyber defense.

My purpose here today is twofold: First, I am here to warn the Pennsylvania General Assembly that the Keystone State's elections are an open target for foreign interference. We cannot afford to have the results of elections questioned, especially in an important swing state like Pennsylvania, which is certainly a target of opportunity for anyone wanting to undermine the validity of U.S. elections. Pennsylvanians deserve to be confident their votes will be cast as intended and counted as cast. That's why Pennsylvania should support the Trump Administration's endorsement of paper ballots and answer Homeland Security Secretary Kirstjen Nielsen's call for "all state and local election officials to make certain that by the 2020 presidential election, every American votes on a verifiable and auditable ballot."

Second, in light of Governor's Wolf budget presented this past Tuesday, I write to urge the General Assembly to include adequate funding in the budget for counties to move forward as expeditiously as possible to replace their current aging and vulnerable voting systems. Local election officials, and national advocacy groups believe the cost to replace the existing equipment, including training, voter outreach and logistical needs for deployment is $150 million. The Governor's budget asks for only $15 million this year, 10% of the actual estimated cost, and would include an additional $15 million each year over the next 4 years. Even as a fiscal conservative, I see this proposal as insufficient, and too vague to allow counties to adequately plan their budgets and replace vulnerable equipment ahead of the 2020 election. Because we count our votes on computers, it is vitally important, now more than ever, to invest

in protecting our national security. As someone who has spent a career in the trenches of cyber warfare, I understand the threat and I'm here to urge you to stand strong in our national defense.

By way of background, Pennsylvania uses two basic kinds of electronic voting systems: 1) Direct recording electronic (DRE) or 2) optical scan systems. Both types of systems are computers but with a significant difference: optical scan systems incorporate a voter-marked paper ballot, marked either with a pen or pencil or with a ballot marking device and that ballot is retained for recounts or audits. Optical scan systems leverage the speed of the computer to report unofficial results quickly. The paper ballots provide a way to check that the computer reported the results accurately either by sampling them in an audit or hand counting the paper ballots if necessary. ***Seventeen counties in Pennsylvania already benefit from the security protection of paper ballots.***

It is my judgment that Pennsylvania must act PRUDENLY to both standardize the best practices and select best technology to protect the sacred right to vote for all citizens of Pennsylvania.

Unfortunately, a majority of Pennsylvania voters use computers that record their vote choices directly to computer memory with no other record of their choice. These kinds of computers cannot be audited, or recounted. And, because they are programmed by other computers, they may be indirectly connected to a network even if they themselves are not connected to the internet.

It's these paperless electronic voting systems that must be replaced as soon as possible. A computer voting system that incorporates a paper ballot provides a way to check on the results of the computer. That check is also a critically important step in the process of shoring up the legitimacy of our elections. Pennsylvania should institute mandatory routine post-election audits that use statistical methods to verify the accuracy of the reported results. Without these steps, our elections will continually be dogged by legitimacy questions at a time when our local election officials do not need to be hampered by such questions.

Pennsylvania will be the only swing state without paper records of the intent of voters for the 2020 election unless we act soon. Election security experts and cyber experts like me support electronic voting systems only if they incorporate voter-marked paper ballots (whether marked by hand or device) and those paper ballots are retained for recounts and ballots. Integrity in process and reliable audit process are paramount.

As I have done in Washington, I am here to warn the Pennsylvania General Assembly that paperless DREs are an open target for foreign interference in our elections; whether the threat emanates from the Chinese trying to undermine President Trump or the Russians doing the opposite. It could as well be the Iranians or the North Koreans that try to intervene. We cannot afford to have the results of elections questioned, especially in an important swing state like Pennsylvania. Because of its vulnerable technology, Pennsylvania is certainly a prime target and presents opportunity for anyone wanting to undermine the validity of US elections. It is critical that paperless DRE machines be replaced in time for the 2020 election.

As has been its history, Pennsylvania is truly the keystone state. In 2020, the election could be decided by Pennsylvania and its electoral votes. If you remember the Florida election

disaster of 2000, with the infamous hanging chads technology and the negative reputation Florida had following that election, you might want to consider making this investment for Pennsylvania, so that Pennsylvania does not suffer the same fate as Florida in 2020. This is the appropriate time and the geopolitical climate to recognize that the most secure technology mix in all new voting systems will be a ***technology to count votes rapidly***, but that is still safe in that it is able to provide paper backups if necessary.

The solution to this problem is known and achievable. The threats to the existing process are known and real.   It is not a political issue or a partisan issue. Rather, it is an issue of national security and acting to protect a sacred right. Even though election administration discussion sometimes veers off into the political realm, election security is not one of those issues. Election security is national security and these committees, which are charged with emergency preparedness, should do everything necessary to ensure that Pennsylvania is ready to meet this threat, mitigate the risk, and protect our democracy from outside interference. I ask you to stand with me in calling for adequate funding in the amount of $150 million to make sure that paper ballots are everywhere in Pennsylvania in 2020.