UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF KENTUCKY
DIVISION OF FRANKFORT

[redacted] Plaintiff, V. MICHAEL ADAMS, ALBERT B. CHANDLER III, SHERRY WHITEHOUSE, JERRY D. JOHNSON, LYNN LANE, DEANNA BRANGERS, CORY SKOLNICK, DWIGHT SEARS, AND JAMES LEWIS Defendants.	Civil Action No. 3:22-CV-45-REW **COMPLAINT AND REQUEST FOR EMERGENCY INJUNCTION**

[redacted]
Plaintiff,

V.

SOS OF KENTUCKY:
MIKE ADAMS
Serve: Mike Adams
700 Capitol Avenue, Suite 152
Frankfort, Kentucky 40601

and

KENTUCKY STATE BOARD OF ELECTIONS:
ALBERT B. CHANDLER, III
Serve: Albert B. Chandler, III
140 Walnut Street
Frankfort, Kentucky 40601

and
SHERRY WHITEHOUSE
Serve: Sherry Whitehouse

140 Walnut Street
Frankfort, Kentucky 40601

and

JERRY D. JOHNSON
Serve: Jerry D. Johnson
140 Walnut Street
Frankfort, Kentucky 40601

and

LYNN LANE
Serve: Lynn Lane
140 Walnut Street
Frankfort, Kentucky 40601

and

DEANNA BRANGERS
Serve: DeAnna Brangers
140 Walnut Street
Frankfort, Kentucky 40601

and

CORY SKOLNICK
Serve: Cory Skolnick
140 Walnut Street
Frankfort, Kentucky 40601

and

DWIGHT SEARS
Serve: Dwight Sears
140 Walnut Street
Frankfort, Kentucky 40601

and

JAMES LEWIS
Serve: James Lewis
140 Walnut Street
Frankfort, Kentucky 40601
Defendants

TABLE OF CONTENTS

INDEX OF AUTHORITIES

CASES **PAGE**

STATE CONSTITUTION AND STATUTES

OTHER AUTHORITIES

RULES

US CONSTITUTION

COMPLAINT AND REQUEST FOR EMERGENCY INJUNCTION

NOW COMES pro se Plaintiff[redacted], and hereby files this Complaint and request for injunction against Defendants KENTUCKY SECRETARY OF STATE (SOS) Michael Adams in his individual capacity and in his official capacity as STATE BOARD OF ELECTIONS Chief Election Official; Albert B. Chandler in his individual and official capacities as member of the STATE BOARD OF ELECTIONS; Sherry Whitehouse in her individual and official capacities as member of the STATE BOARD OF ELECTIONS; Jerry D. Johnson in his individual and official capacities as member of the STATE BOARD OF ELECTIONS; Lynn Lane in her individual and official capacities as member of the STATE BOARD OF ELECTIONS; DeAnna Brangers in her individual and official capacities as member of the STATE BOARD OF ELECTIONS; Cory Skolnick in his individual and official capacities as member of the STATE BOARD OF ELECTIONS; Dwight Sears in his individual and official capacities as member of the STATE BOARD OF ELECTIONS; and James Lewis in his individual and official capacities as member of the STATE BOARD OF ELECTIONS sued in their individual capacity and in their official capacity, (collectively, "Defendants"). In support of the claims set forth herein, Plaintiff alleges as follows:

PARTIES

1. Plaintiff,[redacted] is an adult individual who is a resident, a taxpayer, and a registered voter in the Commonwealth of Kentucky.

2. Defendant, Mike Adams, as the acting Secretary of State and chief election official of the Commonwealth of Kentucky, has a duty to ensure free and equal elections across the Commonwealth. He is sued in his official and individual capacities.

3. Defendant, Albert B. Chandler III, as an appointed member of the State Board of Elections is responsible for elections across the Commonwealth. He is sued in his official and individual capacities.

4. Defendant, Sherry Whitehouse, as an appointed member of the State Board of Elections is responsible for elections across the Commonwealth. She is sued in her official and individual capacities.

5. Defendant, Jerry D. Johnson, as an appointed member of the State Board of Elections is responsible for elections across the Commonwealth. He is sued in his official and individual capacities.

6. Defendant, Lynn Lane, as an appointed member of the State Board of Elections is responsible for elections across the Commonwealth. She is sued in her official and individual capacities.

7. Defendant, DeAnna Brangers, as an appointed member of the State Board of Elections, is responsible for elections across the Commonwealth. She is sued in her official and individual capacities.

8. Defendant, Cory Skolnick, as an appointed member of the State Board of Elections, is responsible for elections across the Commonwealth. He is sued in his official and individual capacities.

9. Defendant, Dwight Sears, as an appointed member of the State Board of Elections, is responsible for elections across the Commonwealth. He is sued in his official and individual capacities.

10. Defendant, James Lewis, as an appointed member of the State Board of Elections, is responsible for elections across the Commonwealth. He is sued in his official and individual capacities.

JURISDICTION AND VENUE

3. This Court has proper jurisdiction, pursuant 28 U.S. Code 1331, as this action seeks to protect civil rights under 14th and 10th amendments of US Constitution:

> "The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States."

4. This Court has jurisdiction to grant injunctive relief based on 28 U.S.C. § 1343(a)(3) authority to do so under Federal Rule of Civil Procedure 65.

5. This Court has authority to grant declaratory relief based on 28 U.S.C. §§ 2201, 2202, and Rule 57 of the FRCP.

6. This Court has jurisdiction to award nominal and compensatory damages under 28 U.S.C. § 1343(a)(4).

7. There exists an actual and justifiable controversy between Plaintiff(s) and Defendant(s) requiring resolution by this Court.

8. Plaintiff(s) have no adequate remedy at law.

9. Venue is proper before the United States Eastern District Court of Kentucky, Frankfort Division under 28 U.S.C. §1391(b)(2) as a substantial part of the events or omissions giving rise to the claim occurred here.

INTRODUCTION

Plaintiff seeks redress for the abuse and devastation of his Constitutional rights and protections from our elected officials. Both houses of the Kentucky State Legislatures, State Board of Elections, County Clerks, Kentucky Sheriffs, Attorney General Daniel Cameron, and the

Kentucky Secretary of State Office have been notified but have found no relief (Exhibit 1). Plaintiff has been called a conspiracy theorist and labeled a domestic terrorist by the U.S. D.O.J. Yet, Plaintiff remains undaunted to seek redress for the violation of his rights and all the People of Kentucky. Plaintiff comes before this court with the acquired knowledge that we are still free on paper. The Constitution affords us the right to elect the state or federal officials we want but due to the actions of those elected, our rights have been deprived.

> *"No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined*." *Wesberry v. Sanders, 376 U.S. 1, 10 (1964).*

Lawful elections are the backbone of our local, state, and national government. The right to vote is protected by U.S. CONST. amend. XIV, § 1, cl. 3-4.

> *"the right to vote is personal," Reynolds, 377 U.S. at 561-62* and *"[e]very voter in a federal … election, whether he votes for a candidate with little chance of winning or for one with little chance of losing, has a right under the Constitution to have his vote fairly counted." Anderson v. United States, 417 U.S. 211, 227 (1974); Baker v. Carr, 369 U.S. 186, 208 (1962).* Invalid or fraudulent votes debase or dilute the weight of each validly cast vote. *Bush II, 531 U.S. at 105*.

The unequal treatment of votes within a state, and unequal standards for processing votes raise equal protection concerns. Justice Thomas wrote in his Dissent regarding *The State of Texas v. Pennsylvania*:

> "*Here, we have the opportunity to do so almost two years before the next federal election cycle. Our refusal to do so by hearing these cases is befuddling. One wonders what this Court waits for. We failed to settle this dispute before the election, and thus provide clear rules. Now we again fail to provide clear rules for future elections. The decision to leave election law hidden beneath a shroud of doubt is baffling. By doing nothing, we invite further confusion and erosion of voter confidence. Our fellow citizens deserve better and expect more of us. I respectfully dissent" State of Texas vs. Commonwealth of Pennsylvania, State of Georgia, State of Michigan, and State of Wisconsin (2020)*. Justice Thomas went on to say; *"the court was thought to be the least dangerous branch and we may have become the most dangerous."* He furthered warned against, *"destroying our institutions because they don't give us what we want, when we want it."*

STANDING

Plaintiff has standing under; *Lujan v. Defenders of Wildlife, U.S. 112 s.Ct. 2130, 2136, 119 L. Ed.2d 351 (1992)* and *Elmore v. McCammon (1986) 640 F. Supp. 905*:

> *"….the right to file a lawsuit pro se is one of the most important rights under the constitution and laws." "Allegations such as those asserted by the petitioner, however in artfully pleaded, are sufficient"*, *"which we hold to less stringent standards than formal pleading drafted by a lawyer."*

Jenkins v. McKeithen, 395 U.S. 411, 411, 421 (1959); Picking v. Pennsylvania R. Co., 151 Fed 2nd; Pucket v. Cox, 456 2nd 233

> *"Pro se pleadings are to be considered without regard to technicality; pro se litigants' pleadings are not to be held to the same standards of perfection as lawyers."* The plaintiff's civil rights pleadings were 150 pages and described by a federal judge as *"inept"*. Nevertheless, it was held *"Where a plaintiff pleads pro se in a suit for protection of civil rights, the Court should endeavor to construe Plaintiff's Pleadings without regard to technicalities."*
>
> (a) (1) Plaintiff has suffered injury as protected interest are actual or imminent, concrete and particularized. (2) The 14th amendment protects our right to vote. (3) The 10th amendment protects states from federal intrusion. (4) Plaintiff was a registered voter during the national election of 2020 and (5) Defendants failed to meet required legally established laws to ensure a free and equal election injuring Plaintiff and all Kentuckians.

STATEMENT OF FACTS

10. The Secretary of State, as Chief Election Official of Kentucky, and the appointed members of the State Board of Elections, deprived our right to vote in free and equal elections, violating 18 U.S. Code § 242, by ignoring state and federal election laws and allowing the use of illegally certified electronic voting machine systems for the November 2020 and subsequent elections. The right to vote is protected under U.S. CONST. amend. XIV, § 1 which states:

> "All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make

> or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

SOS and members of the board allowed the federal government in our local and state elections violating U.S. CONST. amend. X which states:

> "The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people."

We as Citizens have the right to choose those representing us and can only do so if our elections are secure and free of manipulation and federal intrusion. The above-mentioned violations by the SOS and Board of Elections gave rise to the use of insecure electronic voting machines and CISA involvement in our elections across the Commonwealth of Kentucky.

11. A person elected or appointed to office pursuant to Section 228 and KRS 62.010 shall take and subscribe to the following oath of office:

> "I do solemnly swear (or affirm, as the case may be) that I will support the Constitution of the United States and the Constitution of this Commonwealth, and be faithful and true to the Commonwealth of Kentucky so long as I continue a citizen thereof, and that I will faithfully execute, to the best of my ability...according to law; and I do further solemnly swear (or affirm) that since the adoption of the present Constitution, I, being a citizen of this State, have not fought a duel with deadly weapons within this State nor out of it, nor have I sent or accepted a challenge to fight a duel with deadly weapons, nor have I acted as second in carrying a challenge, nor aided or assisted any person thus offending, so help me God." (Exhibit 2)

Secretary of State Mike Adams has broken his oath to uphold Kentucky Constitution § 6 by allowing insecure voting machines in Kentucky elections, thereby depriving our rights to liberty under section 1 of 14th amendment of US Constitution.

12. The Help America Vote (HAVA) Act of 2002 established the Election Assistance Commission (EAC), and according to their Voting System Certification Program[1], Kentucky's

[1]https://www.eac.gov/sites/default/files/eac_assets/1/1/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf

machines are to be tested to federal guidelines. The SOS and board failed to uphold the election laws of our state pursuant to KRS § 117.015(1) which states the Board of Elections shall

> "administer the election laws of the state and supervise registration and purgation of voters within the state."

Kentucky state election law, KRS § 117.125(26-27) states voting equipment must

> "(26) Meet or exceed the standards for a voting system established by the Election Assistance Commission, as amended from time to time, and those approved under KRS 117.379; and
>
> (27) Meet such other requirements as may be established by the State Board of Elections in administrative regulations promulgated under KRS Chapter 13A to reflect changes in technology to ensure the integrity and security of voting systems."

If the EAC breaks federal law by not following their own guidelines, then responsibility falls to our Chief Election Official and Board of Elections to ensure Kentucky remains compliant. There is no excuse for allowing the use of insecure, illegally certified voting machines in our elections.

13. The EAC, pursuant to 52 U.S. Code § 20971(b)(2)(a), are responsible for accrediting the Voting System Testing Laboratories (VSTL). Pro V&V and SLI Compliance, formerly SLI Global, are 2 of the 3 federally accredited labs[2] and are used by voting equipment manufacturers such as Hart Intercivic and ES&S. According to Guideline 3.8 of the VSTL manual, "a grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation." [3] Evidence shows both labs were not accredited for the 2020 November election which means all 120 counties in our state (Exhibit 3) used either Hart or ES&S and were illegally certified.

[2] https://www.eac.gov/voting-equipment/accredited-laboratories
[3]https://www.eac.gov/sites/default/files/eac_assets/1/28/EAC%20VSTL%20Program%20Manual%20Version%202.0.FORCOMMENT.4.4.13.pdf

14. VSTL accreditations must be renewed every 2 years and at the time of the 2020 election, Pro V&V had received their last certificate of accreditation on 2/25/2015 and SLI Compliance on 2/28/2007. In a letter to Pro V&V labs, Senator Wyden warned of the importance of accreditation prompting the EAC to release a series of memos explaining the reason why neither lab had received their new certificates of accreditation.[4] On 1/27/2021, EAC released a memo stating "Due to the outstanding circumstances posed by Covid-19, the renewal process for EAC laboratories has been delayed for an extended period. While this process continues, Pro V&V retains its EAC VSTL accreditation" (Exhibit 4). EAC released their last memo on 7/22/2021, stating SLI Compliance has yet to receive their new accreditation but that the "accreditation remains effective until revoked by a vote of the EAC pursuant to 52 U.S. Code § 20971(c)(2)" (Exhibit 5). Revocation has nothing to do with the above-mentioned guidelines of the EAC VSTL Program Manual which state VSTL accreditations are not to exceed 2 years. In the very same memo, they claim an administrative error for the certification of accreditation during 2017-2019 but admit that the accreditation process is essential, and that it is the primary means to make sure election voting systems meet the requirements. It appears the EAC, once again, failed to uphold their own VSTL Manual, specifically Guideline 3.6.1, that states "The certificate shall be signed by the Chair of the Commission." The only valid Certificate of Accreditation for SLI Compliance[5] (formerly SLI

[4] https://www.wyden.senate.gov/imo/media/doc/wyden-pro-vandv-election-cybersecurity-letter.pdf
[5] https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/sli-compliance-division-gaming-laboratories

Global Solutions) [6], signed by the EAC chair was in 2009.[7] Pro V&V[8] does not have a current accreditation as original accreditation in 2015[9] was not signed by the chair.

15. The lapsed accreditations and security vulnerabilities of the voting machines is detailed in the affidavit of whistleblower Terpsehore Maras (Exhibit 6). According to Maras, accreditation of VSTL's is very important and the purpose being to ensure no foreign or domestic bad actors access the tally data via backdoors in the equipment software. The role VSTL's play is vital because equipment vulnerabilities allow for deployment of algorithms (FROGs-encryption plus decryption)[10] and scripts that intercept, alter, and adjust voting tallies (Exhibit 7). One of the vulnerabilities the VSTL's examine is the use of COTS (Commercial Off–The-Shelf). COTS are the most important component of the election machine and are preferred by many because they have been tried and tested in the open market, with most being readily available and economical. COTS are a source of vulnerability because their components can be used by voting system machine manufacturers as a "Black Box" which means changes to their specs and hardware can happen continuously. Some changes can be simple upgrades to make them more efficient in operation, cost efficient for production, end of life (EOL), or even complete reworks to meet new standards. The key issue is the manufacturing of the COTS, which are used by election machine vendors like Dominion, ES&S, Hart Intercivic, Smartmatic and others, has been outsourced to China. If such components are implemented in our election machines, we become vulnerable to

[6] https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/sli-global-solutions-formerly-systest-labs
[7]https://www.eac.gov/sites/default/files/voting_system_test_lab/files/SysTest%202009%20Certificate%20of%20Accreditation.pdf
[8] https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/pro-vv
[9]https://www.eac.gov/sites/default/files/voting_system_test_lab/files/Pro_VandV_accreditation_certificate_2015.pdf
[10] https://toresays.com/2021/02/11/dominions-own-frog-destroys-their-claim/

black box antics/backdoors due to hardware changes that go undetected proving why VSTL's and their accreditation are so important.

16. C-span's Washington Journal interviewed Dr. Alex J. Halderman, a professor of engineering and computer science at the University of Michigan, on electronic voting machine security. Dr. Halderman was asked about a recent headline, "Hackers can easily break into voting machines used across the U.S."[11] He agreed and further stated that "Election infrastructure across the United States remains weakly protected and vulnerable against sophisticated foreign hackers."[12] He then warned that "we have a lot of work to do as a country before 2020 and elections to come." Dr. Halderman during his security research, rigorously tested every single kind of voting machine. Vulnerabilities were discovered "where someone could hack in, put malicious software on the voting machine, cause it to be sabotaged or even silently steal votes."[13] Dr. Halderman submitted a sworn declaration[14] in *Curling v. Raffensperger*[15] detailing the security vulnerabilities of the election machines in general. He also filed a motion in support of a preliminary injunction because the vulnerabilities of the machines were so great. (Exhibit 8).

17. Kentucky elections have been riddled with security vulnerabilities for a long time. In 2007, then SOS Greg Stumbo requested the EAC do an expert report on "Improving Kentucky's Electronic Voting Systems Certifications."[16] A few of the key findings of this report stated that public confidence in elections were at an all-time low, studies[17] showed the electronic voting

[11] https://www.salon.com/2019/08/14/hackers-can-easily-break-into-voting-machines-used-across-the-u-s-play-doom-nirvana/
[12] https://www.c-span.org/video/?463480-4/washington-journal-j-alex-halderman-discusses-election-security
[13] https://www.c-span.org/video/?463480-4/washington-journal-j-alex-halderman-discusses-election-security
[14] https://www.courtlistener.com/docket/6139924/260/2/curling-v-raffensperger/
[15] https://www.courtlistener.com/docket/6139924/curling-v-raffensperger/
[16]https://www.eac.gov/sites/default/files/eac_assets/1/1/Kentuckys%20Election%20Voting%20Systems%20and%20Certification%20Process%20Report.pdf
[17] http://web.archive.org/web/20080403154728/https://www.sos.state.oh.us/sos/info/EVEREST/14-AcademicFinalEVERESTReport.pdf

systems employed in Kentucky were not secure, and the use of a non-certified electronic voting system should have been detected and corrected during normal State oversight procedures. Security vulnerabilities existed in 2007 and it has only worsened with the continued disregard of violations and fraud. In 2019, the State Board of Elections removed 175,000 ineligible voters from our voter rolls[18], but Andy Beshear, who was AG at the time, sued to have all reinstated.[19] The Court ruled in October of 2019 to reinstate the 175,000 ineligible voters and just in time for the Governor's race with Andy Beshear as the democrat candidate. The Governor's race between Bevin and Beshear was decided by only 5,000 votes leaving speculation about the 175,000 ineligible voters and the effects of Beshear's suit. The Beshear/Bevin race was a clear trial run on stealing elections by switching votes in real time, which were caught live on air.[20] The blatant fraud has continued with current SOS Michael Adams claiming on his rumor page that "voting systems used in the Commonwealth of Kentucky are designed to protect against tampering, including during system storage, transport and voting. Each machine uses physical and system access controls, including lockable doors, tamper-evident seals and access codes."[21] Voting tabulators, pursuant to KRS § 117.125(25), are not to be connected to the internet. Our SOS says "No Kentucky voting equipment is ever connected to the Internet. Votes are tabulated by the County Board of Elections using a calculator. No Kentucky voting machine contains a modem -- it is not allowed by Kentucky law or certification rules." Voters in the May 17, 2022 primary elections witnessed new available Wi-Fi networks on their phones when their vote was tabulated (See Affidavits). Poll workers are trained to know that tabulators must be connected to the internet

[18] https://toresays.com/2019/11/22/breaking-voter-fraud-confirmed-in-kentucky-electoral-office-confirms-175k-voters-were-added-back-to-voter-rolls-in-2019/
[19] https://americanindependent.com/kentucky-inactive-voters-lawsuit-2019-election-november-5-matt-bevin/
[20] https://www.youtube.com/watch?v=VQvLZ0aGYRs (vote switching explained and shown at 1:35mm)
[21] https://www.sos.ky.gov/elections/Pages/Rumor-Control.aspx

so they can communicate with each other (See Affidavits). There is a patent on the Smart Device Network Application (SDNA's) technology which allows devices such as voting machines to "talk" to one another (Exhibit 9). Connection to networks opens the door for online hacking and manipulation of votes which is a security vulnerability our SOS and election board have ignored and allowed to occur. The evidence of election fraud during the 2020 election is starting to come out in Arizona[22], Wisconsin[23], and Colorado.[24] [25]

18. Cybersecurity and Infrastructure Security Agency (CISA) focuses on the cybersecurity of all critical infrastructure, including election offices) within the United States. The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) is federally funded by CISA and a division of the Center for Internet Security (CIS).[26] EI-ISAC members include 30 Kentucky county clerks as well as the State Board of Elections and Office of the Secretary of State.[27] CIS also has partnerships with Kentucky state local governments proving CISA is here and involved in making decisions for our state.[28] The US Department of Homeland Security (DHS) has been subdelegated as the Sector-Specific Agency (SSA) for the Election Infrastructure Subsector and coordinates closely with EAC to provide guidance.[29] DHS provides cybersecurity tools and protections of Kentucky's infrastructure and is a key partner in election security.[30] The US government took over elections in our state through the HAVA Act, this act

[22] https://www.azag.gov/sites/default/files/2022-04/2022-04-06%20Fann%20letter.pdf
[23] https://yournews.com/2022/03/04/2308797/wisconsin-special-counsel-finds-widespread-election-fraud-in-2020-nursing/
[24] https://thecorporateasylum.com/colorado-dominion-voting-machine-issues-forensic-examination-proves-vote-manipulation-and-illegal-destruction-of-records/
[25]https://www.ksal.com/wp-content/uploads/2022/03/Mesa-County-Forensic-Report-No.-3-signed1.pdf
[26] https://www.cisecurity.org/ei-isac
[27] https://www.cisecurity.org/ei-isac/partners-ei-isac/
[28] http://www.cisecurity.org/partners-local-government
[29] https://www.cisa.gov/sites/default/files/publications/gov-facilities-EIS-scc-charter-2020-508.pdf
[30] https://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=177

of congress and the actions of our SOS and State Board of Elections are direct violations of the 10th amendment of the US Constitution.

CONCLUSION

19. The Secretary of State and the State Board of Elections have deprived the People of Kentucky our right to liberty by allowing the use of illegally certified machines in the November 2020 General Election, thereby rendering the results null and void. The right of the People to vote in free and equal elections was and continues to be violated by our Local, State, and Federal governments. The current usurping of rights has had dire consequences for the People of our country, resulting in pain and suffering. The policies of this administration have caused wide-ranging, pervasive financial and physical hardships for Kentuckians (See Affidavits). To redress our grievances and seek remedy for these hardships, the People of Kentucky have been notifying our elected officials. We sent all election fraud evidence that was gathered and presented in this complaint, but no response to date by any elected official even though ample time was given to rectify. The Secretary of State and Attorney General of Kentucky were served a complaint in November of 2021, regarding the 2020 election, with over 200 pages of election fraud evidence (See Exhibit 1). Both received a sworn declaration about the security vulnerabilities of the election machines and how the EAC failed to renew accreditation for the labs responsible with certifying this equipment. To date, both have continued to ignore this and all attempts to redress our grievances.

20. We the People are losing more rights each day due to the policies of those voted into office on these same machines. It is time the People pick their candidates and run their own elections. There was a time in our history when the People were happy with their voting equipment and 60% of the country used mechanical lever machines with ease and free of manipulation, hacking, and

human error. In fact, all of New York City in 1929 used these lever machines in their elections. Cheating occurred in cities that used paper ballots since it was impossible with the lever machines[31]. Two highly contested Presidential elections happened, destroying any public confidence in our elections. These events gave rise to the HAVA Act which is responsible for the shift away from the mechanical lever machines to efficient, not so accurate, electronic machines[32]. The growing, irrelevant demand for efficient elections gave rise to other forms of voting such as mail-in voting, electronic tabulators, drop boxes, absentee voting, etc which are all susceptible to fraud. Efficient elections are conducted to "perform or function in the best possible manner with the least waste of time."[33] Time is not a factor when elections are conducted accurately, freely, and equally. The People want transparency and accuracy with each vote being counted correctly, not quickly. Continuing to conduct elections on illegally certified machines with security vulnerabilities is a violation of our 1st and 14th amendment rights and the People will hold our elected public servants accountable.

PRAYER FOR RELIEF

A. For these reasons, Plaintiff respectfully requests the Court to grant an emergency injunction preventing the use of electronic voting machines in the state and in the interim, replace with paper ballots.

B. GRANTS an emergency injunction prohibiting Defendants from destruction/deletion of any election records created under KRS 117.027(4), to include all paper ballots created by voting systems, USB devices, memory cards, electronic storage devices, mail in

[31] https://www.opednews.com/articles/Machining-the-Vote--A-brie-by-Rady-Ananda-080628-791.html
[32] https://nyvv.org/newdoc/2009/LeverMachinesAndHAVA020909.pdf
[33] https://www.dictionary.com/browse/efficient

ballots, tabulation tapes, USB final counts from precincts and all other election records not specifically stated from the 2020, 2021, and 2022 elections.

C. Compel the Secretary of State office and State Board of Elections to halt the use of any electronic voting machine in the Commonwealth of Kentucky.

D. Request the Court to compel the Secretary of State office to issue a referral of a complaint under 52 U.S. Code §20511(2) to Attorney General Daniel Cameron and the Civil Rights Department of the Department of Justice to open an investigation of criminal and fraudulent election violations and allegations henceforth provided in this complaint with the full authority of 52 U.S. Code §20511(2) including but not limited to the impounding of election materials and electronic voting system.

E. Plaintiff requests the Court order that the Defendants be cited to appear herein and, upon final hearing, that this Court sustain these elections and enter a final judgment directing Governor Beshear to render elections void no later than 10 days after the date of judgment becomes final as "fraud vitiates everything,". *United States v. Thorckmorton*, *98 U. S. 61*.

F. Respectively requests this Court to strike down the HAVA Act and declare it unconstitutional for limiting our forms of voting. Court has jurisdiction to declare legislation inconsistent with the U.S. Constitution ("unconstitutional") and therefore null and void, *Marbury v. Madison (1803)*.

G. Plaintiff asks that this Court enter an order requiring Defendants to provide to Plaintiff all correspondence relating to the certification of the electronic voting machines.

H. For an award of attorney's fees and costs incurred because of this action.

I. That this Honorable Court grant this injunction pursuant to Fed. R. Civ. P. 65(b)(1).

J. That this Honorable Court "order a speedy hearing" of this declaratory judgment action as permitted by Fed. R. Civ. P. 57.

K. For all other relief to which the Plaintiff is entitled.

RESPECTFULLY submitted this ___ day of _____, 2022.

EXHIBIT TABLE OF CONTENTS

EXHIBIT 1

DIVISION OF FRANKFORT

[redacted] MEKUS, **Plaintiff,** **V.** **MICHAEL ADAMS, ALBERT B. CHANDLER III, SHERRY WHITEHOUSE, JERRY D. JOHNSON, LYNN LANE, DEANNA BRANGERS, CORY SKOLNICK, DWIGHT SEARS. AND JAMES LEWIS** **Defendants.**	**Civil Action No. _____** **AFFIDAVIT OF** [redacted]

I, [redacted] having been first duly sworn, do depose and state, under 28 U.S. Code § 1746, as follows:

1. I voted in the 2020 Presidential Election in person and early because of Covid-19 measures. Voting in elections should not be on multiple days but done so on one day and only in person.
2. I am a part of a group, Kentucky Stands United, who has been tirelessly working to notify our elected officials of our grievances, only to be ignored every time.
3. In October of 2021, I joined 49 other litigants in a writ filed with SCOTUS regarding the 2020 election. Before the filing, Kentucky Stands United group members tried to get a meeting with AG Cameron to share election fraud evidence detailing how the election machines were not even properly certified leaving them vulnerable to attacks and manipulation, but we were denied. Apparently, AG Cameron does not meet personally, only his constituent liaison. The evidence we were going to share with Cameron's office was the whistleblower affidavit cited in this complaint. The writ, the whistleblower affidavit, and other election fraud evidence was sent certified mail to both Attorney General Daniel Cameron and Secretary of State Michael G. Adams on November 1, 2021. Each have had ample time to address the situation yet no response to date.
4. There is more than enough evidence to prove fraud in the 2020 election and time is running out to preserve any election data, machines, documents, etc. After September 3rd, the materials pertaining to the 2020 election can legally be destroyed resulting in evidence lost. The Citizens of Kentucky and America cannot endure any more injury as a result of a stolen election.

Further the Affiant sayeth naught.

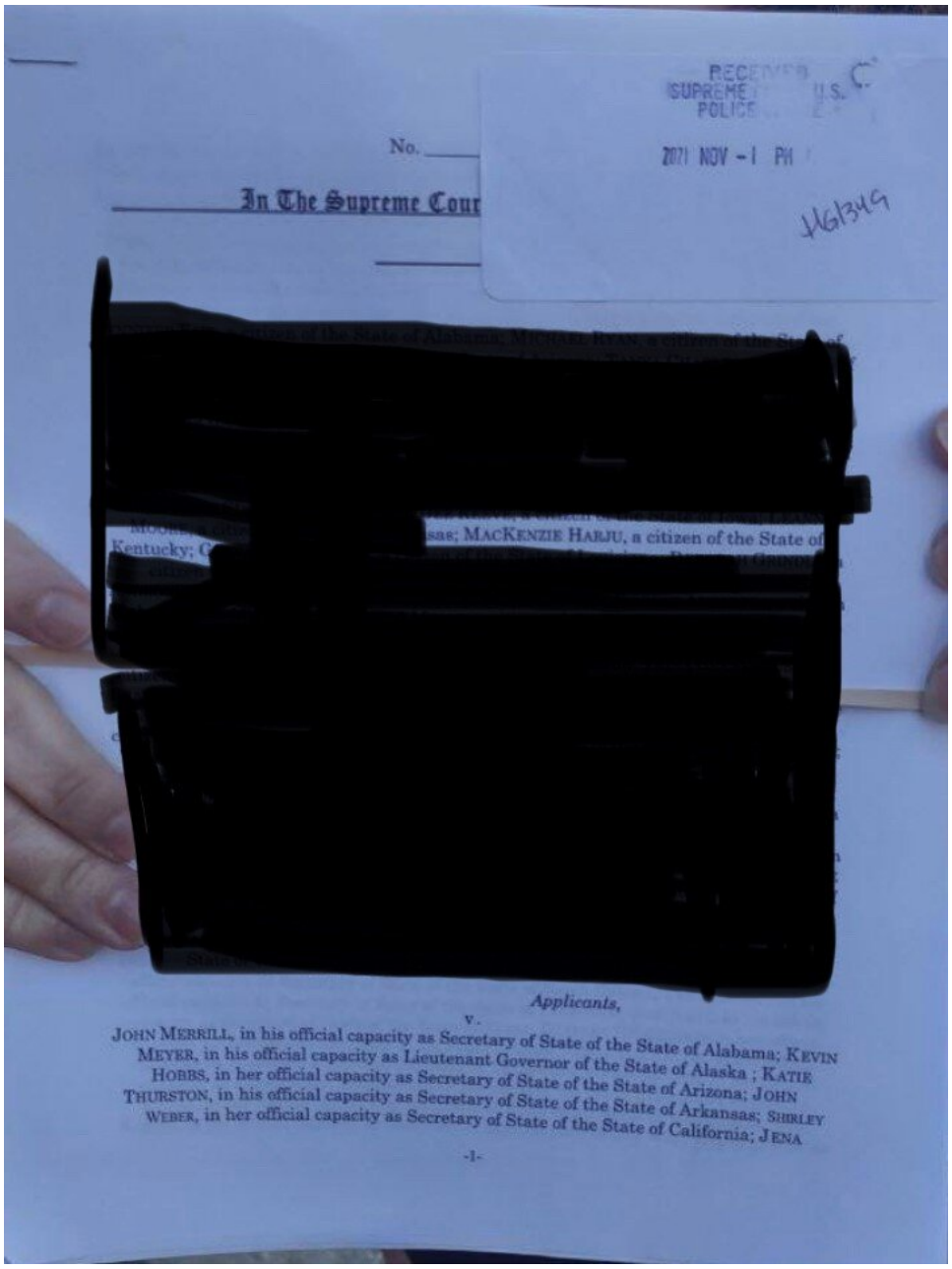

RECEIVED
SUPREME COURT U.S.
POLICE
2021 NOV -1 PM
No.
In The Supreme Cour
sas; MACKENZIE HARJU, a citizen of the State of
Kentucky;
Applicants,
v.
JOHN MERRILL, in his official capacity as Secretary of State of the State of Alabama; KEVIN MEYER, in his official capacity as Lieutenant Governor of the State of Alaska ; KATIE HOBBS, in her official capacity as Secretary of State of the State of Arizona; JOHN THURSTON, in his official capacity as Secretary of State of the State of Arkansas; SHIRLEY WEBER, in her official capacity as Secretary of State of the State of California; JENA
-1-

EXHIBIT 2

OFFICE OF THE
CLERK OF THE COURT OF APPEALS
360 DEMOCRAT DRIVE
FRANKFORT, KENTUCKY 40601-8209

Rebecca Combs Lyon
CLERK

(502) 573-7920
Phone

(502) 573-6795
Fax

ORDER OF CERTIFICATION

I, Rebecca Combs Lyon, Clerk of the Court of Appeal of Kentucky, do hereby certify that the attached Oath of Office Order for Michael G. Adams, Kentucky Secretary of State, entered January 6, 2020, is a true and correct copy of the original Order as it appears on file in this office.

The certification of Oath of Office was served on the Governor in accordance with KRS 62.020(2)(c).

Done this the 6th day of January, 2020, at Frankfort, Kentucky.

Rebecca Combs Lyon
REBECCA COMBS LYON, CLERK

Commonwealth of Kentucky

Court of Appeals

MICHAEL G. ADAMS

OATH OF OFFICE

To All Whom These Presents Shall Come, Greetings:

The Honorable Michael G. Adams, having been elected Kentucky Secretary of State, by the citizens of the Commonwealth of Kentucky;

Whereupon, the Honorable Michael G. Adams, Kentucky Secretary of State, appeared the 6th day of January, 2020, in Frankfort, Kentucky before the Honorable Allison E. Jones, Judge, Court of Appeals of Kentucky, and took the oath as required by Section 228 of the Kentucky Constitution.

IT IS ORDERED that the Honorable Michael G. Adams, having taken the oath as required by law, enter upon the discharge of his duties.

The Clerk of the Court of Appeals of Kentucky is requested to certify this Order to the Governor in accordance with KRS 62.020(2)(c) with a copy to the Secretary of State.

This the 6th day of January, 2020.

HON. ALLISON E. JONES, JUDGE
COURT OF APPEALS OF KENTUCKY

EXHIBIT **3**

Voting Systems

2020

Kentucky State Board of Elections						
Type of Voting Equipment used in each KY County						
County Code No.	**County Name**	**Number of Precincts**	**Number of Voting Machines**	**Equipment Type**		
1	Adair	16	17	Hart InterCivic eScan™		
			17	Hart InterCivic eSlate™		
2	Allen	13	16	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
3	Anderson	14	17	Hart InterCivic eScan™		
			17	Hart InterCivic eSlate™		
4	Ballard	13	16	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
5	Barren	25	27	Hart InterCivic eScan™		
			25	Hart InterCivic eSlate™		
6	Bath	12	1	Hart InterCivic eScan™		
			13	Hart InterCivic eSlate™		
7	Bell	30	35	Hart InterCivic eScan™		
			31	Hart InterCivic eSlate™		
8	Boone	63	67	Hart InterCivic eScan™		
			62	Hart InterCivic eSlate™		
9	Bourbon	16	20	Hart InterCivic eScan™		
			21	Hart InterCivic eSlate™		
10	Boyd	48	52	Hart InterCivic eScan™		
			49	Hart InterCivic eSlate™		
11	Boyle	25	28	Hart InterCivic eScan™		
			28	Hart InterCivic eSlate™		
12	Bracken	8	1	Hart InterCivic eScan™		
			9	Hart InterCivic eSlate™		
13	Breathitt	21	44	ES&S Ivotronic		
			1	ES&S M-100 Scan		
14	Breckinridge	16	19	Hart InterCivic eScan™		
			16	Hart InterCivic eSlate™		
15	Bullitt	47	53	Hart InterCivic eScan™		
			43	Hart InterCivic eSlate™		
16	Butler	12	15	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
17	Caldwell	13	16	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
18	Calloway	23	34	Hart InterCivic eScan™		
			29	Hart InterCivic eSlate™		
19	Campbell	67	72	Hart InterCivic eScan™		
			66	Hart InterCivic eSlate™		
20	Carlise	6	9	Hart InterCivic eScan™		
			8	Hart InterCivic eSlate™		
21	Carroll	11	13	Hart InterCivic eScan™		
			13	Hart InterCivic eSlate™		
22	Carter	26	2	Hart InterCivic eScan™		
			26	Hart InterCivic eSlate™		
23	Casey	15	17	Hart InterCivic eScan™		
			16	Hart InterCivic eSlate™		
24	Christian	41	50	Hart InterCivic eScan™		
			47	Hart InterCivic eSlate™		
25	Clark	26	28	Hart InterCivic eScan™		
			26	Hart InterCivic eSlate™		
26	Clay	20	41	ES&S Ivotronic		
			1	ES&S M-100 Scan		

Kentucky State Board of Elections						
Type of Voting Equipment used in each KY County						
County Code No.	County Name	Number of Precincts	Number of Voting Machines	Equipment Type		
27	Clinton	13	26	ES&S Ivotronic		
			1	ES&S M-100 Scan		
28	Crittenden	12	18	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
29	Cumberland	10	11	Hart InterCivic eSlate™		
			11	Hart InterCivic eScan™		
30	Daviess	57	86	Hart InterCivic eScan™		
			87	Hart InterCivic eSlate™		
31	Edmonson	8	11	Hart InterCivic eScan™		
			11	Hart InterCivic eSlate™		
32	Elliott	7	14	ES&S Ivotronic		
			1	ES&S M-100 Scan		
33	Estill	15	1	Hart InterCivic eScan™		
			15	Hart InterCivic eSlate™		
34	Fayette	286	4	Hart InterCivic eScan™		
			719	Hart InterCivic eSlate™		
35	Fleming	18	20	Hart InterCivic eScan™		
			19	Hart InterCivic eSlate™		
36	Floyd	42	42	ES&S Ivotronic		
			1	ES&S M-100 Scan		
37	Franklin	44	47	Hart InterCivic eScan™		
			45	Hart InterCivic eSlate™		
38	Fulton	11	15	Hart InterCivic eScan™		
			16	Hart InterCivic eSlate™		
39	Gallatin	8	10	Hart InterCivic eScan™		
			10	Hart InterCivic eSlate™		
40	Garrard	14	15	Hart InterCivic eScan™		
			15	Hart InterCivic eSlate™		
41	Grant	22	23	Hart InterCivic eScan™		
			24	Hart InterCivic eSlate™		
42	Graves	30	36	Hart InterCivic eScan™		
			32	Hart InterCivic eSlate™		
43	Grayson	22	23	Hart InterCivic eScan™		
			24	Hart InterCivic eSlate™		
44	Green	10	13	Hart InterCivic eScan™		
			11	Hart InterCivic eSlate™		
45	Greenup	29	33	Hart InterCivic eScan™		
			33	Hart InterCivic eSlate™		
46	Hancock	10	12	Hart InterCivic eScan™		
			11	Hart InterCivic eSlate™		
47	Hardin	59	61	Hart InterCivic eScan™		
			59	Hart InterCivic eSlate™		
48	Harlan	32	2	Hart InterCivic eScan™		
			36	Hart InterCivic eSlate™		
49	Harrison	19	2	Hart InterCivic eScan™		
			20	Hart InterCivic eSlate™		
50	Hart	19	23	Hart InterCivic eScan™		
			18	Hart InterCivic eSlate™		
51	Henderson	45	47	Hart InterCivic eScan™		
			39	Hart InterCivic eSlate™		
52	Henry	20	21	Hart InterCivic eScan™		
			25	Hart InterCivic eSlate™		

Kentucky State Board of Elections						
Type of Voting Equipment used in each KY County						
County Code No.	County Name	Number of Precincts	Number of Voting Machines	Equipment Type		
53	Hickman	6	8	Hart InterCivic eScan™		
			7	Hart InterCivic eSlate™		
54	Hopkins	50	58	Hart InterCivic eScan™		
			41	Hart InterCivic eSlate™		
55	Jackson	14	29	ES&S Ivotronic		
			1	ES&S M-100 Scan		
56	Jefferson	623	350	ES&S DS200 Scanner		
			350	ES&S ExpressVote BMD Terminal		
57	Jessamine	36	46	Hart InterCivic eScan™		
			45	Hart InterCivic eSlate™		
58	Johnson	31	63	ES&S Ivotronic		
			1	ES&S M-100 Scan		
59	Kenton	106	114	Hart InterCivic eScan™		
			108	Hart InterCivic eSlate™		
60	Knott	30	60	ES&S Ivotronic		
			1	ES&S M-100 Scan		
61	Knox	30	66	ES&S Ivotronic		
			1	ES&S M-100 Scan		
62	Larue	12	16	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
63	Laurel	45	78	ES&S Ivotronic		
			1	ES&S M-100 Scan		
64	Lawrence	18	21	Hart InterCivic eScan™		
			20	Hart InterCivic eSlate™		
65	Lee	10	20	ES&S Ivotronic		
			1	ES&S M-100 Scan		
66	Leslie	17	36	MicroVote, Version		
			1	ES&S M-100 Scan		
67	Letcher	30	49	ES&S Ivotronic		
			1	ES&S M-100 Scan		
68	Lewis	14	17	Electronic 1242		
			17	Hart InterCivic eSlate™		
			1	Hart InterCivic eScan™		
69	Lincoln	17	38	ES&S Ivotronic		
			1	ES&S M-100 Scan		
70	Livingston	10	13	Hart InterCivic eScan™		
			12	Hart InterCivic eSlate™		
71	Logan	20	20	Hart InterCivic eScan™		
			21	Hart InterCivic eSlate™		
72	Lyon	6	6	Hart InterCivic eScan™		
			7	Hart InterCivic eSlate™		
73	McCracken	54	55	Hart InterCivic eScan™		
			55	Hart InterCivic eSlate™		
74	McCreary	18	19	Hart InterCivic eScan™		
			19	Hart InterCivic eSlate™		
75	McLean	8	38	Hart InterCivic eScan™		
			9	Hart InterCivic eSlate™		
76	Madison	47	50	ES&S DS200 Scanner		
			50	ES&S ExpressVote BMD Terminal		
77	Magoffin	14	29	ES&S Ivotronic		
			1	ES&S M-100 Scan		
78	Marion	17	18	Hart InterCivic eScan™		

Kentucky State Board of Elections						
Type of Voting Equipment used in each KY County						
County Code No.	County Name	Number of Precincts	Number of Voting Machines	Equipment Type		
			19	Hart InterCivic eSlate™		
79	Marshall	25	26	Hart InterCivic Verity 2.0		
80	Martin	14	21	ES&S Ivotronic		
			1	ES&S M-100 Scan		
81	Mason	13	20	Hart InterCivic eScan™		
			21	Hart InterCivic eSlate™		
82	Meade	19	21	Hart InterCivic eScan™		
			21	Hart InterCivic eSlate™		
83	Meniffee	6	12	ES&S Ivotronic		
			1	ES&S M-100 Scan		
84	Mercer	17	21	Hart InterCivic eScan™		
			18	Hart InterCivic eSlate™		
85	Metcalfe	12	13	Hart InterCivic eScan™		
			13	Hart InterCivic eSlate™		
86	Monroe	12	14	Hart InterCivic eScan™		
			13	Hart InterCivic eSlate™		
87	Montgomery	18	20	Hart InterCivic eScan™		
			20	Hart InterCivic eSlate™		
88	Morgan	12	27	ES&S Ivotronic		
			1	ES&S M-100 Scan		
89	Muhlenberg	25	27	Hart InterCivic eScan™		
			28	Hart InterCivic eSlate™		
90	Nelson	24	26	Hart InterCivic eScan™		
			28	Hart InterCivic eSlate™		
91	Nicholas	5	1	Hart InterCivic eScan™		
			6	Hart InterCivic eSlate™		
92	Ohio	19	28	Hart InterCivic eScan™		
			26	Hart InterCivic eSlate™		
93	Oldham	38	44	Hart InterCivic eScan™		
			39	Hart InterCivic eSlate™		
94	Owen	12	15	Hart InterCivic eScan™		
			15	Hart InterCivic eSlate™		
95	Owsley	8	9	Hart InterCivic eScan™		
			9	Hart InterCivic eSlate™		
96	Pendleton	12	13	ES&S Ivotronic		
			1	ES&S M-100 Scan		
97	Perry	37	2	Hart InterCivic eScan™		
			39	Hart InterCivic eSlate™		
98	Pike	57	232	Hart InterCivic eScan™		
			58	Hart InterCivic eSlate™		
99	Powell	11	23	ES&S Ivotronic		
			1	ES&S M-100 Scan		
100	Pulaski	56	64	Hart InterCivic eScan™		
			59	Hart InterCivic eSlate™		
101	Robertson	5	5	Hart InterCivic eScan™		
			6	Hart InterCivic eSlate™		
102	Rockcastle	15	37	ES&S Ivotronic		
			1	ES&S M-100 Scan		
103	Rowan	18	20	Hart InterCivic eScan™		
			21	Hart InterCivic eSlate™		
104	Russell	16	19	Hart InterCivic eScan™		
			17	Hart InterCivic eSlate™		

Kentucky State Board of Elections						
Type of Voting Equipment used in each KY County						
County Code No.	**County Name**	**Number of Precincts**	**Number of Voting Machines**	**Equipment Type**		
105	Scott	46	47	Hart InterCivic eScan™		
			48	Hart InterCivic eSlate™		
106	Shelby	34	35	Hart InterCivic eScan™		
			37	Hart InterCivic eSlate™		
107	Simpson	13	14	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
108	Spencer	14	14	Hart InterCivic eScan™		
			13	Hart InterCivic eSlate™		
109	Taylor	20	52	Hart InterCivic eScan™		
			22	Hart InterCivic eSlate™		
110	Todd	13	15	Hart InterCivic eScan™		
			14	Hart InterCivic eSlate™		
111	Trigg	15	17	Hart InterCivic eScan™		
			16	Hart InterCivic eSlate™		
112	Trimble	12	14	Hart InterCivic Verity 2.0		
113	Union	16	19	Hart InterCivic eScan™		
			17	Hart InterCivic eSlate™		
114	Warren	121	83	Hart InterCivic eScan™		
			88	Hart InterCivic eSlate™		
115	Washington	14	15	Hart InterCivic eScan™		
			15	Hart InterCivic eSlate™		
116	Wayne	19	20	Hart InterCivic eScan™		
			20	Hart InterCivic eSlate™		
117	Webster	14	16	Hart InterCivic eScan™		
			15	Hart InterCivic eSlate™		
118	Whitley	36	39	Hart InterCivic eScan™		
			37	Hart InterCivic eSlate™		
119	Wolfe	8	17	ES&S Ivotronic		
			1	ES&S M-100 Scan		
120	Woodford	19	19	Hart InterCivic eScan™		
			19	Hart InterCivic eSlate™		
	Total	**3,719**	**7,400**			

EXHIBIT 4

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

FROM: Jerome Lovato, Voting System Testing and Certification Director

SUBJECT: Pro V&V EAC VSTL Accreditation

DATE: 1/27/2021

Pro V&V has completed all requirements to remain in good standing with the EAC's Testing and Certification program per section 3.8 of the Voting System Test Laboratory Manual, version 2.0:

> ***Expiration and Renewal of Accreditation.*** *A grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation. VSTLs in good standing shall renew their accreditation by submitting an application package to the Program Director, consistent with the procedures of Section 3.4 of this Chapter, no earlier than 60 days before the accreditation expiration date and no later than 30 days before that date. Laboratories that timely file the renewal application package shall retain their accreditation while the review and processing of their application is pending. VSTLs in good standing shall also retain their accreditation should circumstances leave the EAC without a quorum to conduct the vote required under Section 3.5.5.*

Due to the outstanding circumstances posed by COVID-19, the renewal process for EAC laboratories has been delayed for an extended period. While this process continues, Pro V&V retains its EAC VSTL accreditation.

EXHIBIT **5**

U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

The Voting System Test Laboratory (VSTL) accreditation program is an essential component of the EAC's Voting System Testing and Certification Program. The EAC has made National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) accreditation a requirement as part of its VSTL accreditation program. NVLAP accreditation is **the primary means by which the EAC ensures that each VSTL meets and continues to meet the technical requirements** of the EAC program. It sets the standards for each VSTL's technical, physical and personnel resources, as well as its testing, management, and quality assurance policies and protocols. NVLAP reviews VSTLs one year after their initial accreditation and biennially thereafter.

The EAC takes additional steps to ensure that laboratory policies are in place regarding compliance management and issues like conflict of interest, record maintenance, and financial stability. It also ensures that the VSTL is willing and capable to work with EAC in its Testing and Certification Program. This is performed by regularly working closely with the labs and performing audits biannually and generating certificates. [1]The VSTL accreditation does not get revoked unless the commission votes to revoke accreditation; and by that same token, EAC generated certificates or lack thereof do not determine the validity of a VSTL's accreditation status.

Due to administrative error during 2017-2019, the EAC did not issue an updated certificate to Pro V&V causing confusion with some people concerning their good standing status. Even though the EAC failed to reissue the certificate, Pro V&V's audit was completed in 2018 and again in early 2021 as the scheduled audit of Pro V&V in 2020 was postponed due to COVID-19 travel restrictions. Despite the challenges outlined above, throughout this period, Pro V&V and SLI Compliance remained in good standing with the requirements of our program and retained their accreditation. **In addition, the EAC has placed appropriate procedures and qualified staff to oversee this aspect of the program ensuring the continued quality monitoring of the Testing and Certification program is robust and in place.**

The Testing and Certification program has been fully staffed since May 2019, and we are confident that the integrity of the labs and our voting system certification program has remained strong throughout. The lack of generating a new certificate does not indicate that the labs were out of compliance. All certifications during this period remain valid as does the lab accreditation. The quality of our labs' work is closely monitored during certification campaigns. Both Pro V&V and SLI Compliance are NAVLAP accredited laboratories that are assessed against the management and technical requirements published in the International Standard, ISO/IEC 17025:2017.

---

[1] Pro V&V was accredited by the EAC on February 24, 2015, and SLI Compliance was accredited by the EAC on February 28, 2007. Federal law provides that EAC accreditation of a voting system test **laboratory cannot be revoked unless the EAC Commissioners vote to revoke the accreditation**: "The accreditation of a laboratory for purposes of this section may not be revoked unless the revocation is approved by a vote of the Commission." 52 U.S. Code § 20971(c)(2). The EAC has never voted to revoke the accreditation of Pro V&V. Pro V&V has undergone continuing accreditation assessments and had new accreditation certificate issued on February 1, 2021.

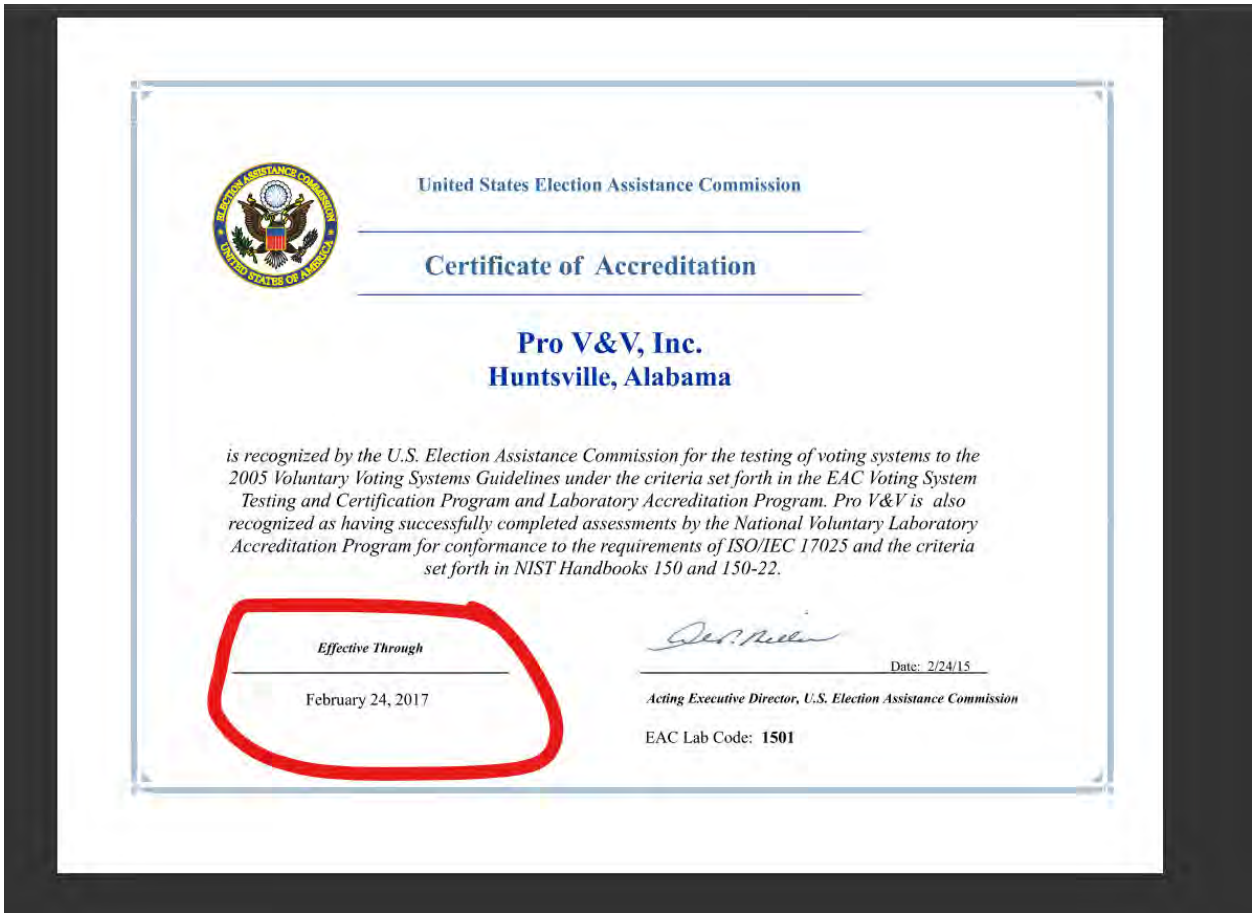
EXHIBIT **6**

Declaration of [redacted]

Pursuant to 28 U.S.C Section 1746, I, [redacted], make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I have been a private contractor with experience gathering and analyzing foreign intelligence and acted as a LOCALIZER during the deployment of projects and operations both OCONUS and CONUS. I am a trained Cryptolinguist, hold a completed degree in Molecular and Cellular Physiology and have FORMAL training in other sciences such as Computational Linguistics, Game Theory, Algorithmic Aspects of Machine Learning, Predictive Analytics among others.
3. I have operational experience in sources and methods of implementing operations during elections both CONUS and OCONUS
4. I am an amateur network tracer and cryptographer and have over two decades of mathematical modeling and pattern analysis.
5. In my position from 1999-2014 I was responsible for delegating implementation via other contractors sub-contracting with US or 9 EYES agencies identifying connectivity, networking and subcontractors that would manage the micro operations.
6. My information is my personal knowledge and ability to detect relationships between the companies and validate that with the cryptographic knowledge I know and attest to as well as evidence of these relationships.
7. In addition, I am WELL versed due to my assignments during my time as a private contractor of how elections OCONUS (for countries I have had an assignment at) and CONUS (well versed in HAVA ACT) and more.
8. On or about October 2017 I had reached out to the US Senate Majority Leader with an affidavit claiming that our elections in 2017 may be null and void due to lack of EAC certifications. In fact Sen. Wyden sent a letter to Jack Cobb on 31 OCT 2017 advising discreetly pointing out the importance of being CERTIFIED EAC had issued a certificate to

Pro V & V and that expired on Feb 24, 2017. No other certification has been located.



United States Election Assistance Commission

Certificate of Accreditation

Pro V&V, Inc.
Huntsville, Alabama

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the 2005 Voluntary Voting Systems Guidelines under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. Pro V&V is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Effective Through

February 24, 2017

Date: 2/24/15

Acting Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **1501**

9. Section 231(b) of the Help America Vote Act (HAVA) of 2002 (42 U.S.C. §15371(b)) requires that the EAC provide for the accreditation and revocation of accreditation of independent, non-federal laboratories qualified to test voting systems to Federal standards. Generally, the EAC considers for accreditation those laboratories evaluated and recommended by the National Institute of Standards and Technology (NIST) pursuant to HAVA Section 231(b)(1). However, consistent with HAVA Section 231(b)(2)(B), the Commission may also vote to accredit laboratories outside of those recommended by NIST upon publication of an explanation of the reason for any such accreditation.

10. 

United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200978-0

Pro V&V
Huntsville, AL

is accredited by the National Voluntary Laboratory Accreditation Program for specific services, listed on the Scope of Accreditation, for:

Voting System Testing

This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).

2020-03-26 through 2021-03-31
Effective Dates

For the National Voluntary Laboratory Accreditation Program

11. VSTL's are VERY important because equipment vulnerabilities allow for deployment of algorithms and scripts to intercept, alter and adjust voting tallies.
12. There are only TWO accredited VSTLs (VOTING SYSTEM TEST LABORATORIES). In order to meet its statutory requirements under HAVA §15371(b), the EAC has developed the EAC's Voting System Test Laboratory Accreditation Program. The procedural requirements of the program are established in the proposed information collection, the EAC **Voting System Test Laboratory Accreditation Program Manual**. Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants. The procedural requirements of this Manual will supersede any prior laboratory accreditation requirements issued by the EAC. This manual shall be read in conjunction with the EAC's **Voting System Testing and Certification Program Manual** (OMB 3265-0019).

U.S. Election Assistance Commission

MICHIGAN

State Participation:	**Requires Testing by an Independent Testing Authority.** MI requires that voting systems are certified by an independent testing authority accredited by NASED and the board of state canvassers.
Applicable Statute(s):	"An electronic voting system shall not be used in an election unless it is approved by the board of state canvassers … and unless it meets 1 of the following conditions: (a) Is certified by an independent testing authority accredited by the national association of state election directors and by the board of state canvassers. (b) In the absence of an accredited independent testing authority, is certified by the manufacturer of the voting system as meeting or exceeding the performance and test standards referenced in subdivision (a) in a manner prescribed by the board of state canvassers." MICH. COMP. LAWS ANN § 168.795a (2009).
Applicable Regulation(s):	MI does not have a regulation regarding the federal certification process.
State Certification Process:	The Secretary of State accepts requests from persons/corporations wishing to have their voting system examined. The requestor must pay the Secretary of State an application fee of $1,500.00, file a report listing all of the states in which the voting system has been approved and any reports that these states have made regarding the performance of the voting system. The Board of State Canvassers conducts a field test involving Michigan electors and election officials in simulated election day conditions. The Board of State Canvassers shall approve the voting system if it meets all of the state requirements. MICH. COMP. LAWS ANN § 168.795a (2009).
Fielded Voting Systems:	*[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].* http://www.michigan.gov/sos/0,1607,7-127-1633_8716_45458---,00.html

13.

WISCONSIN

State Participation:	**Requires Testing by a Federally Accredited Laboratory.** WI requires that its voting systems receive approval from an independent testing authority accredited by NASED verifying that the voting systems meet all of the recommended FEC standards.
Applicable Statute(s):	"No ballot, voting device, automatic tabulating equipment or relating equipment and materials to be used in an electronic voting system may be utilized in this state unless it is approved by the board [of election commissioners]." WIS. STAT.ANN. § 5.91 (West 2009).
Applicable Regulation(s):	"An application for approval of an electronic voting system shall be accompanied by all of the following … [r]eports from an independent testing authority accredited by the national association of state election directors (NASED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission." WIS. ADMIN. CODE GAB § 7.01 (2009).
State Certification Process:	The Board of Election Commissioners accepts applications for the approval of electronic voting systems. Once the application is completed, the vendor must set up the voting system for three mock elections using; (1) offices, (2) referenda questions and (3) candidates. A panel of local election officials can assist the Board in the review of the voting system. The Board conducts the test using a mock election for the partisan primary, general election, and nonpartisan election. The Board may also require that the voting system be used in an actual election as a condition of the approval. WIS. ADMIN. CODE GAB §§ 7.01, 7.02 (2009).
Fielded Voting Systems:	*[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].* http://elections.state.wi.us/section.asp?linkid=643&locid=47

14.

U.S. Election Assistance Commission

GEORGIA

State Participation:	**Requires Federal Certification.** GA requires that its voting systems are tested to EAC standards by EAC accredited labs and certified by the EAC.
Applicable Statute(s):	"Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any voting machine may request the Secretary of State to examine the machine. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any voting machine previously examined and approved by him or her. Before any such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination; provided, however, that in the case of a request by ten or more electors the examination fee shall be $ 250.00. The Secretary of State may, at any time, in his or her discretion, reexamine any voting machine." GA CODE ANN. § 21-2-324 (2008).
Applicable Regulation(s):	"Prior to submitting a voting system for certification by the State of Georgia, the proposed voting system's hardware, firmware, and software must have been issued Qualification Certificates from the EAC. These EAC Qualification Certificates must indicate that the proposed voting system has successfully completed the EAC Qualification testing administered by EAC approved ITAs. If for any reason, this level of testing is not available, the Qualification tests shall be conducted by an agency designated by the Secretary of State. In either event, the Qualification tests shall comply with the specifications of the *Voting Systems Standards* published by the EAC." GA. COMP. R. & RES. 590-8-1-.01 (2009).
State Certification Process:	After the voting system has passed EAC Qualification testing, the vendor of the voting system submits a letter to the Office of the Secretary of State requesting certification for the voting system along with a technical data package to the certification agent. An evaluation proposal is created by the certification agent after a preliminary view of the Technical Data Package and sent to the vendor. Any additional EAC ITA testing identified in the evaluation proposal is arranged by the vendor and the certification agent will perform all other tests identified in the evaluation proposal. The certification agent submits a report of their findings to the Secretary of State. Based on these findings the Secretary of State will make a final determination on whether to certify the voting system. GA. COMP. R. & RES. 590-8-1-.01 (2009).
Fielded Voting Systems:	*[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].* http://www.sos.georgia.gov/Elections/

15.

U.S. Election Assistance Commission

PENNSYVANIA

State Participation:	**Requires Testing by a Federally Accredited Laboratory.** PA requires that its voting systems are approved by a federally recognized independent testing laboratory as meeting federal voting system standards.
Applicable Statute(s):	"Any person or corporation owning, manufacturing or selling, or being interested in the manufacture or sale of, any electronic voting system, may request the Secretary of the Commonwealth to examine such system if the voting system has been examined and approved by a federally recognized independent testing authority and if it meets any voting system performance and test standards established by the Federal Government." 25 PA. CONS. STAT. ANN. Code § 3031.5 (West 2008).
Applicable Regulation(s):	PA does not have a regulation regarding the federal certification process.
State Certification Process:	The Secretary of State examines voting systems, upon request, once the voting systems have received approval by a federally recognized independent testing authority. The person(s) requesting the examination of the voting system are responsible for the cost of the examination. After the examination, the Secretary of State issues a report stating whether or not the voting systems are safe and compliant with state and federal requirements. If the voting systems are deemed safe and compliant by the Secretary of State then the systems may be adopted and approved for use in elections by each county through a majority vote of its qualified electors. 25 PA. CONS. STAT. ANN. Code §§ 3031.5, 3031.2 (West 2008).
Fielded Voting Systems:	*[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].* http://www.votespa.com/HowtoVote/tabid/74/language/en-US/Default.aspx

16.

U.S. Election Assistance Commission

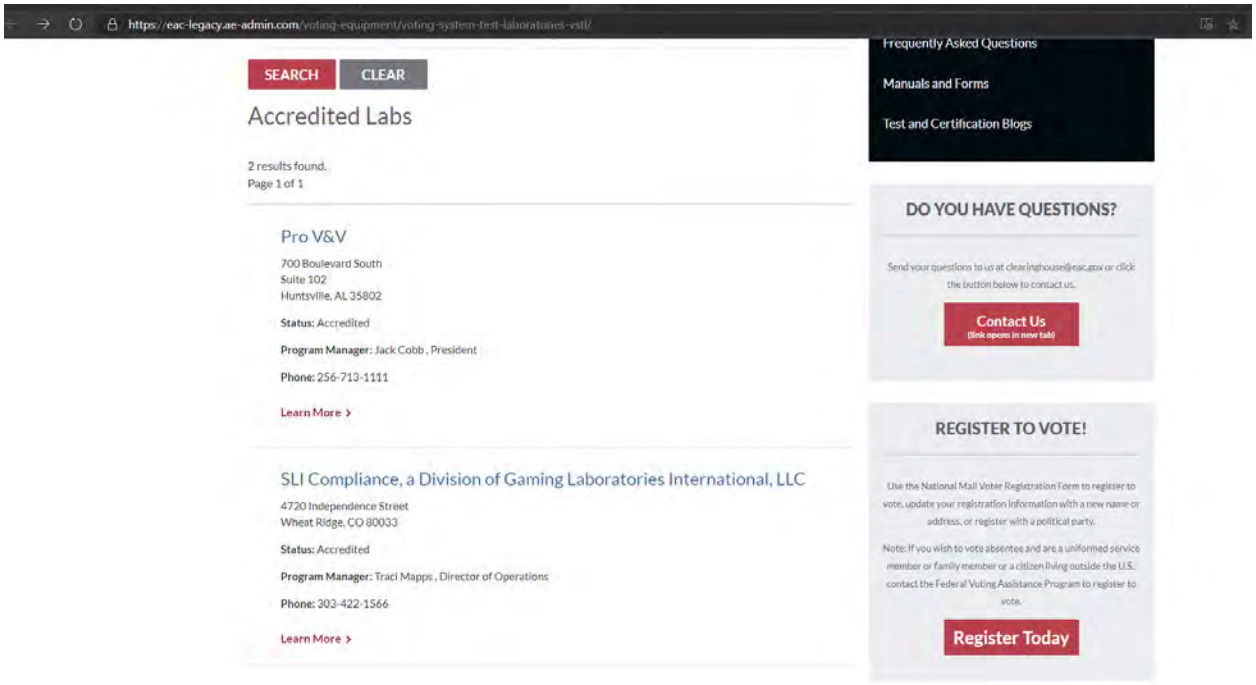
ARIZONA

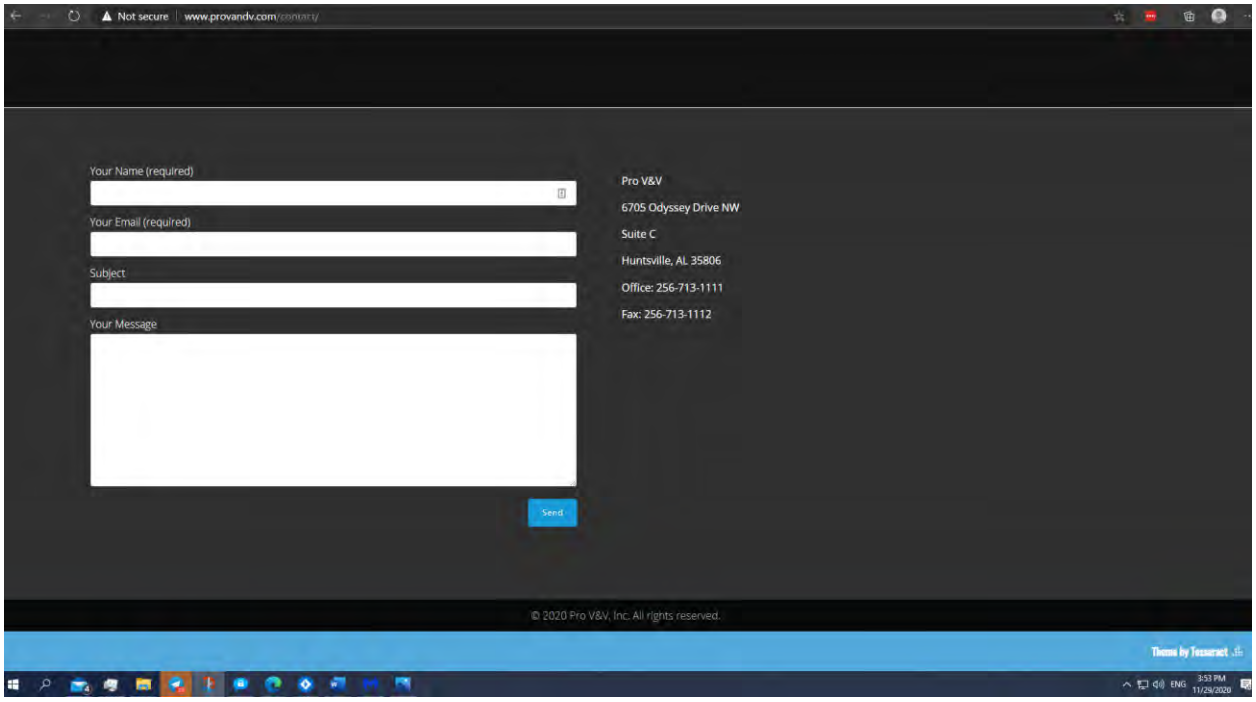
State Participation:	**Requires Testing by a Federally Accredited Laboratory.** AZ requires that its voting systems are HAVA compliant and approved by a laboratory that is accredited pursuant to HAVA.
Applicable Statute(s):	"On completion of acquisition of machines or devices that comply with HAVA, machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with HAVA and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to HAVA." ARIZ. REV. STAT. § 16-442(B) (2008).
Applicable Regulation(s):	AZ does not have a regulation regarding the federal certification process.
State Certification Process:	The Secretary of State appoints a committee of three people that test different voting systems. This committee is required to submit their recommendations to the Secretary of State who then makes the final decision on which voting system(s) to adopt. ARIZ. REV. STAT. § 16-442(A) and (C) (2008).
Fielded Voting Systems:	*[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].* http://www.azsos.gov/election/equipment/default.htm

17.

18. **Pro V& V** and **SLI Gaming** both lack evidence of EAC Accreditation as per the Voting System Testing and Certification Manual.

19. **Pro V& V** is owned and Operated by Jack Cobb. Real name is Ryan Jackson Cobb. The company ProV&V was founded and run by Jack Cobb who formerly worked under the entity of Wyle Laboratories which is an AEROSPACE DEFENSE CONTRACTING ENTITY. The address information on the EAC, NIST and other entities for Pro V& V are different than that of what is on ProV&V website. The EAC and NIST (ISO CERT) issuers all have another address.

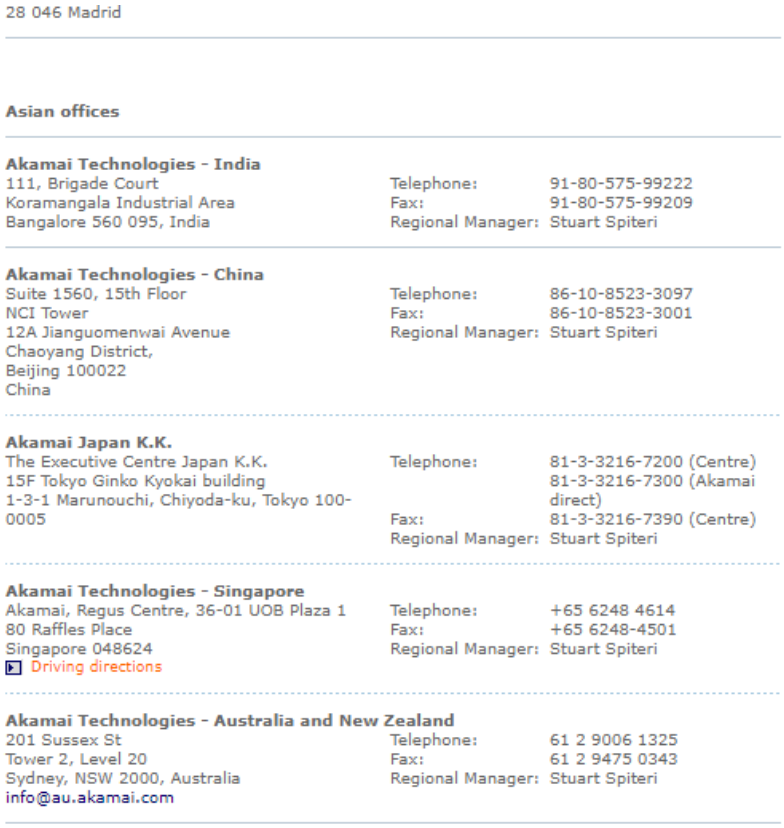




20. VSTLs are the most important component of the election machines as they examine the use of COTS (Commercial Off–The-Shelf)
21. "Wyle became involved with the testing of electronic voting systems in the early 1990's and has tested over 150 separate voting systems. Wyle was the first company to obtain accreditation by the National Association of State Election Directors (NASED). Wyle is accredited by the Election Assistance Commission (EAC) as a Voting System Testing Laboratory (VSTL). Our scope of accreditation as a VSTL encompasses all aspects of the hardware and software of a voting machine. Wyle also received NVLAP accreditation to ISO/IEC 17025:2005 from NIST." Testimony of Jack Cobb 2009
22. COTS are preferred by many because they have been tried and tested in the open market and are most economic and readily available. COTS are also the SOURCE of vulnerability therefore VSTLs are VERY important. COTS components by voting system machine manufacturers can be used as a "Black Box" and changes to their specs and hardware make up change continuously. Some changes can be simple upgrades to make them more efficient in operation, cost efficient for production, end of life (EOL) and even complete reworks to meet new standards. They key issue in this is that MOST of the COTS used by Election Machine Vendors like Dominion, ES&S, Hart Intercivic, Smartmatic and others is that such manufacturing for COTS have been outsourced to China which if implemented in our Election Machines make us vulnerable to BLACK BOX antics and backdoors due to hardware changes that can go undetected. This is why VSTL's are VERY important.
23. The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAILABLE and HOUSED on the HARDWARE. This is a vulnerability. Exporting system reporting using software like Crystal Reports, or PDF software allows for vulnerabilities with their constant updates.
24. As per the COTS hardware components that are fixed, and origin may be cloaked under proprietary information a major vulnerability exists since once again third-party support software is dynamic and requires FREQUENT updates. The hardware components of the computer components, and election machines that are COTS may have slight updates that can be overlooked as they may be like those designed that support the other third -party software. COTS origin is important and the US Intelligence Community report in 2018 verifies that.
25. The Trump Administration made it clear that there is an absence of a major U.S. alternative to foreign suppliers of networking equipment. This highlights the growing dominance of

Chinese manufacturers like Huawei that are the world's LARGEST supplier of telecom and other equipment that endangers national security.

26. China, is not the only nation involved in COTS provided to election machines or the networking but so is Germany via a LAOS founded Chinese linked cloud service company that works with SCYTL named Akamai Technologies that have offices in China and are linked to the server that Dominion Software.



28 046 Madrid

Asian offices

Akamai Technologies - India
111, Brigade Court
Koramangala Industrial Area
Bangalore 560 095, India

Telephone: 91-80-575-99222
Fax: 91-80-575-99209
Regional Manager: Stuart Spiteri

Akamai Technologies - China
Suite 1560, 15th Floor
NCI Tower
12A Jianguomenwai Avenue
Chaoyang District,
Beijing 100022
China

Telephone: 86-10-8523-3097
Fax: 86-10-8523-3001
Regional Manager: Stuart Spiteri

Akamai Japan K.K.
The Executive Centre Japan K.K.
15F Tokyo Ginko Kyokai building
1-3-1 Marunouchi, Chiyoda-ku, Tokyo 100-0005

Telephone: 81-3-3216-7200 (Centre)
81-3-3216-7300 (Akamai direct)
Fax: 81-3-3216-7390 (Centre)
Regional Manager: Stuart Spiteri

Akamai Technologies - Singapore
Akamai, Regus Centre, 36-01 UOB Plaza 1
80 Raffles Place
Singapore 048624
Driving directions

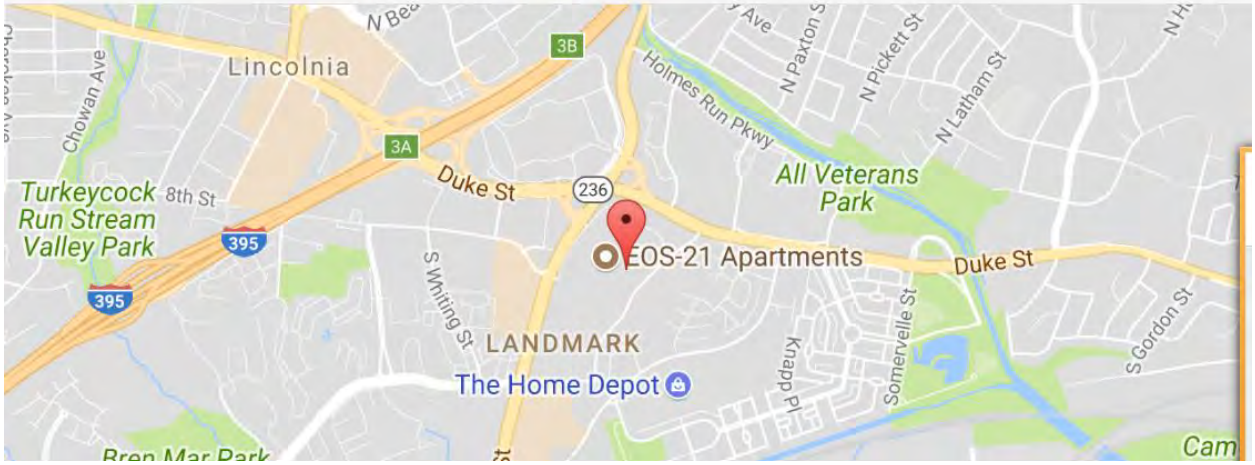
Telephone: +65 6248 4614
Fax: +65 6248-4501
Regional Manager: Stuart Spiteri

Akamai Technologies - Australia and New Zealand
201 Sussex St
Tower 2, Level 20
Sydney, NSW 2000, Australia
info@au.akamai.com

Telephone: 61 2 9006 1325
Fax: 61 2 9475 0343
Regional Manager: Stuart Spiteri

ptt.gov resolves to 4.30.228.74. According to our data this IP address belongs to *Level 3 Communications* and is located in *Alexandria, Virginia, United States*. Please have a look at the information provided below for further details.

4.30.228.74	
ISP/Organization	Level 3 Communications
Location	Alexandria 22304, Virginia (VA), United States (US)
Latitude	38.8115 / 38°48'41" N
Longitude	-77.1285 / 77°7'42" W
Timezone	America/New_York
Local Time	Thu, 12 Jul 2018 19:27:40 -0400

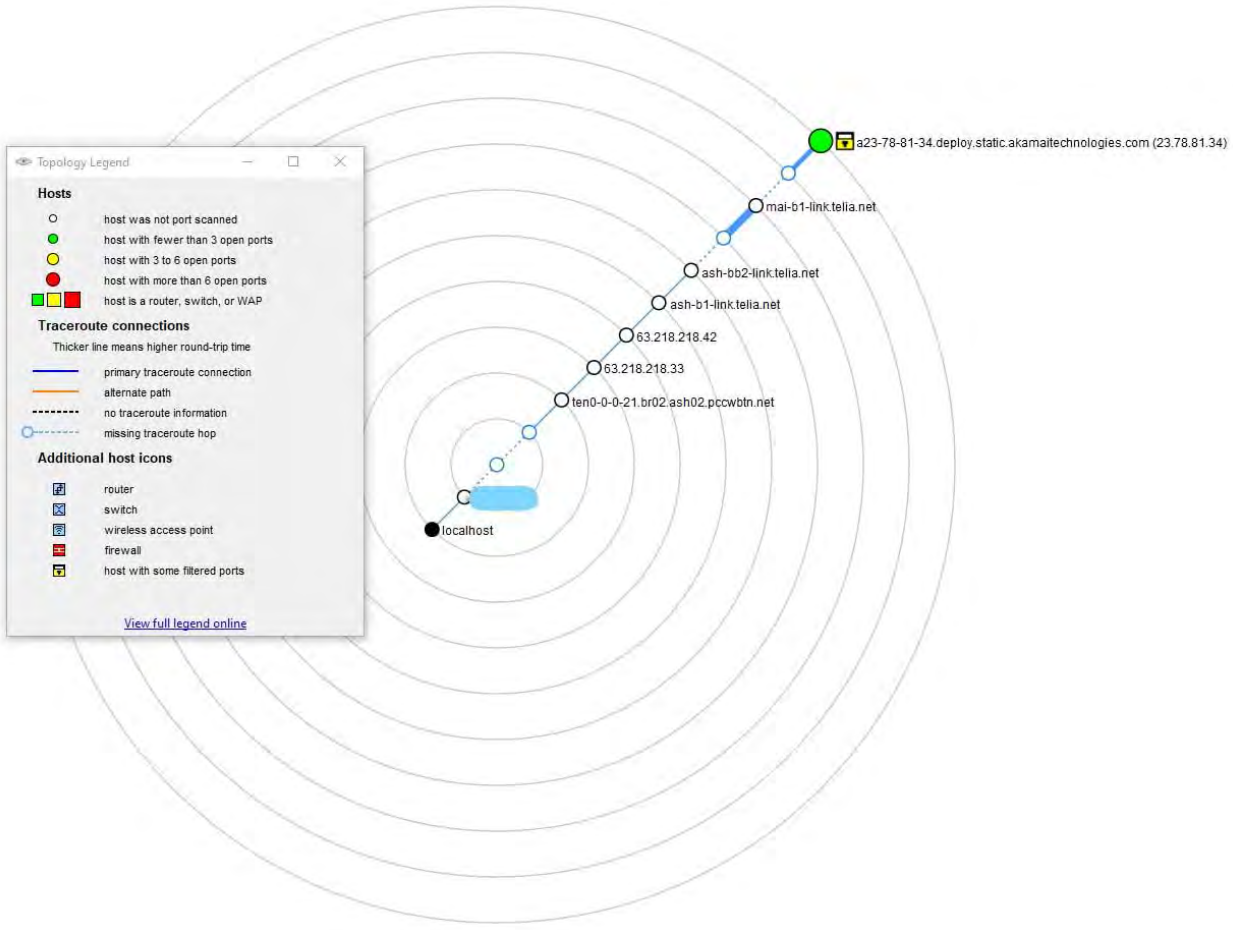


27.

28. L3 Level Communications is federal contractor that is partially owned by foreign lobbyist George Soros. An article that AP ran in 2010 – spoke out about the controversy of this that has been removed. (LINK) "As for the company's other political connections, it also appears that none other than George Soros, the billionaire funder of the country's liberal political infrastructure, owns 11,300 shares of OSI Systems Inc., the company that owns Rapiscan. Not surprisingly, OSI's stock has appreciated considerably over the course of the year. Soros certainly is a savvy investor." Washington Examiner re-write.

29.


a23-78-81-34.deploy.static.akamaitechnologies.com (23.78.81.34)
4.15.168.158
ae-11.edge2.Chicago10.Level3.net
cer-edge-20.inet.qwest.net
10.40.50.7
207.69.33.137
10.238.0.1
DeviceDHCP.Home
localhost
172.22.88.14
hu0-5-0-4.ccr21.cle04.atlas.cogentco.com
be2717.ccr41.ord01.atlas.cogentco.com
be2765.ccr41.ord03.atlas.cogentco.com
att.ord03.atlas.cogentco.com
cgcil22crs.ip.att.net
n54ny21crs.ip.att.net
12.122.115.105
12.244.79.30
michigan.gov (23.78.200.73)



30.

31. **L-3 Communication** Systems-East designs, develops, produces and integrates communication systems and support equipment for space, air, ground, and naval applications, including C4I systems and products; integrated Navy communication systems; integrated space communications and RF payloads; recording systems; secure communications, and information security systems. In addition, their site claims that MARCOM is an integrated communications system and The Marcom® is the foundation of the Navy's newest digital integrated voice / data switching system for affordable command and control equipment supporting communications and radio room automation. The MarCom® uses the latest **COTS** digital technology and open systems standards to offer the command and control user a low cost, user friendly, solution to the complex voice, video and data communications needs of present and future joint / allied missions. Built in reliability, rugged construction, and fail-safe circuits ensure your call and messages will go through. Evidently a HUGE vulnerability.

32. Michigan's government site is thumped off Akamai Technologies servers which are housed on **TELIA AB** a foreign server located in Germany.
33. Scytl, who is contracted with AP that receives the results tallied BY Scytl on behalf of Dominion – During the elections the AP reporting site had a disclaimer.
    AP – powered by SCYTL.

Advertisements

Geolocation on IP Map

Basic Tracking Info

Domain:	Michigan.gov [Whois Lookup - Domain Country - Domain To IP]
IP Address:	23.78.81.34 [IP Blacklist Check]
Reverse DNS:	34.81.78.23.in-addr.arpa
Hostname:	a23-78-81-34.deploy.static.akamaitechnologies.com
Nameservers:	a12-67.akam.net >> 184.26.160.67 a11-66.akam.net >> 84.53.139.66 a1-35.akam.net >> 193.108.91.35 a5-66.akam.net >> 95.100.168.66 a18-64.akam.net >> 95.101.36.64 a24-65.akam.net >> 2.16.130.65

Location For an IP: Michigan.gov

Continent:	North America (NA)
Country:	United States (US)
Capital:	Washington
State:	Unknown
City Location:	Unknown
ISP:	Akamai Technologies
Organization:	Akamai Technologies
AS Number:	AS1299 Telia Company AB
something went wrong!	something went wrong!
Time Zone:	America/North_Dakota/Center
Local Time:	13:48:46
Timezone GMT offset:	-21600
Sunrise / Sunset:	07:27 / 17:12

Extra Information for an IP: Michigan.gov

Continent Lat/Lon:	46.07305 / -100.546
Country Lat/Lon:	38 / -98
City Lat/Lon:	(37.751) / (-97.822)
IP Language:	English

34. “Scytl was selected by the Federal Voting Assistance Program of the U.S. Department of Defense to provide a secure online ballot delivery and onscreen marking systems under a program to support overseas military and civilian voters for the 2010 election cycle and beyond. Scytl was awarded 9 of the 20 States that agreed to participate in the program (New York, Washington, Missouri, Nebraska, Kansas, New Mexico, South Carolina, Mississippi and Indiana), making it the provider with the highest number of participating States.” PDF
35. According to DOMINION : 1.4.1Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-Aconsists of 2 types, custom and commercial off the shelf (COTS). COTS applications were verified to be pristine or were subjected to source code review for analysis of any modifications and verification of meeting the pertinent standards.
36. The concern is the HARDWARE and the NON – ACCREDITED VSTLs as by their own admittance use COTS.
37. The purpose of VSTL’s being accredited and their importance in ensuring that there is no foreign interference/ bad actors accessing the tally data via backdoors in equipment software. The core software used by ALL SCYTL related Election Machine/Software manufacturers ensures “anonymity” .
38. Algorithms within the area of this “shuffling” to maintain anonymity allows for setting values to achieve a desired goal under the guise of “encryption” in the trap-door.
39. The actual use of trapdoor commitments in Bayer-Groth proofs demonstrate the implications for the verifiability factor. This means that no one can SEE what is going on during the process of the “shuffling” therefore even if you deploy an algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : “The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system”
40. **Key Terms**
41. **UNIVERSAL VERIFIABILITY**: Votes cast are the votes counted and integrity of the vote is verifiable (the vote was tallied for the candidate selected) . **SCYTL FAILS UNIVERSAL VERIFIABILITY** because no mathematical proofs can determine if any votes have been manipulated.
42. **INDIVIDUAL VERIFIABILITY**: Voter cannot verify if their ballot got correctly counted. Like, if they cast a vote for ABC they want to verify it was ABC. That notion clearly discounts the need for anonymity in the first place.

43. To understand what I observed during the 2020 I will walk you through the process of one ballot cast by a voter.
44. STEP 1 |Config Data | All non e-voting data is sent to Scytl (offshore) for configuration of data. All e-voting is sent to CONFIGURATION OF DATA then back to the e-voting machine and then to the next phase called CLEANSING. **CONCERNS**: Here we see an "OR PROOF" as coined by mathematicians – an "or proof" is that votes that have been pre-tallied parked in the system and the algorithm then goes back to set the outcome it is set for and seeks to make adjustments if there is a partial pivot present causing it to fail demanding manual changes such as block allocation and narrowing of parameters or self-adjusts to ensure the predetermined outcome is achieved.
45. STEP 2|CLEANSING | The Process is when all the votes come in from the software run by Dominion and get "cleansed" and put into 2 categories: invalid votes and valid votes.
46. STEP 3|Shuffling /Mixing | This step is the most nefarious and exactly where the issues arise and carry over into the decryption phase. Simply put, the software takes all the votes, literally mixes them a and then re-encrypts them. This is where if ONE had the commitment key- TRAPDOOR KEY – one would be able to see the parameters of the algorithm deployed as the votes go into this mixing phase, and how algorithm redistributes the votes.
47. This published PAPER FROM University College London depicts how this shuffle works. In essence, when this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes when mixed.

48.

Background - ElGamal encryption

- Setup: Group $\mathcal{G}$ of prime order q with generator g
- Public key: $pk = y = g^x$
- Encryption: $\mathcal{E}_{pk}(m; r) = (g^r, y^r m)$
- Decryption: $\mathcal{D}_x(u, v) = vu^{-x}$
- Homomorphic:

$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(M; R) = \mathcal{E}_{pk}(mM; r + R)$$

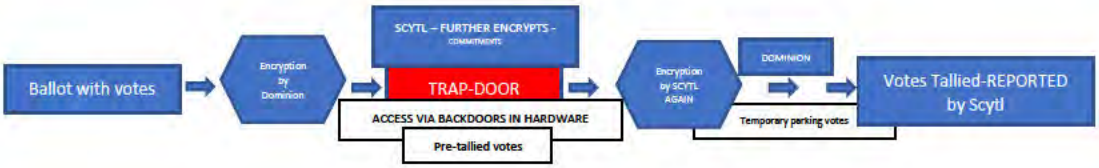
- Re-encryption:

$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(1; R) = \mathcal{E}_{pk}(m; r + R)$$

UCL

49. When this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes.
50. When the votes are sent to Scytl via Dominion Software EMS (Election Management System) the Trap Door is accessed by Scytl or TRAP DOOR keys (Commitment Parameters).

51.

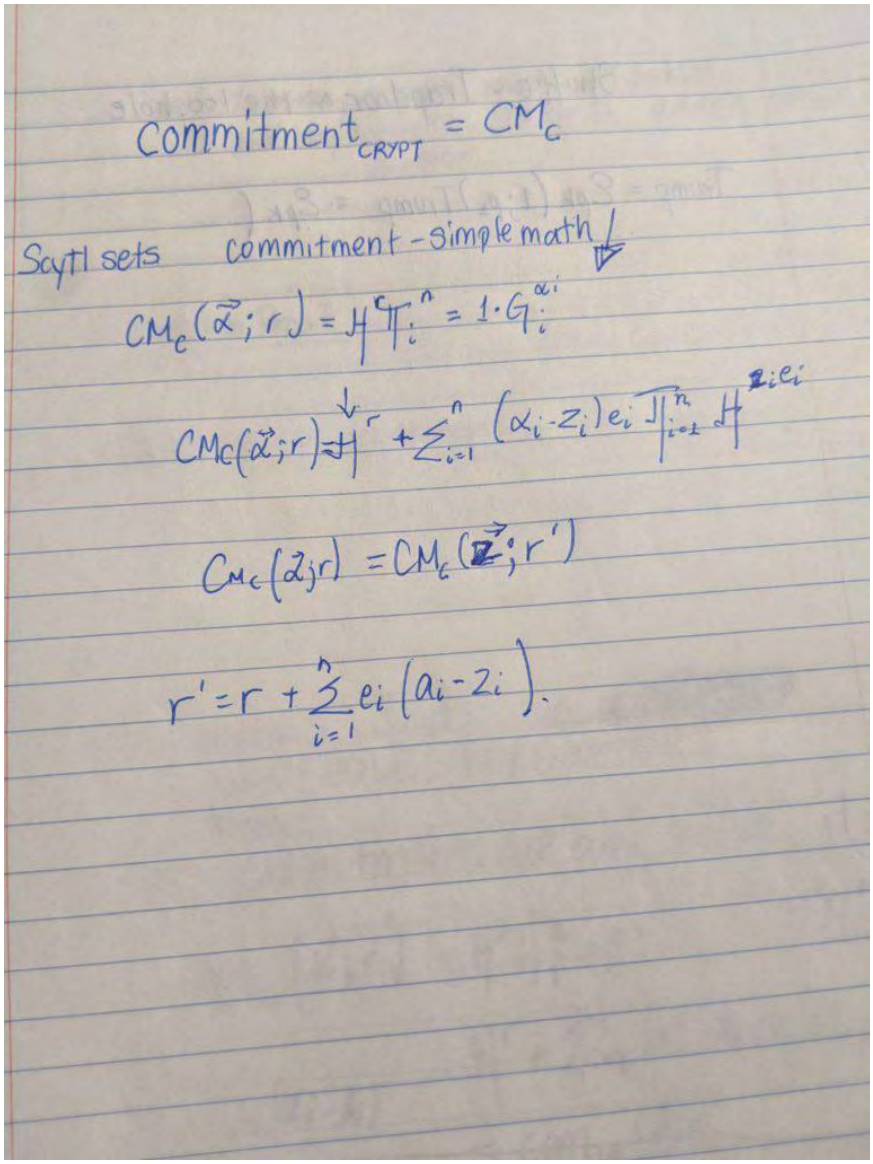


52. The encrypted data is shifted into Scytl's platform in the form of ciphertexts – this means it is encrypted and a key based on commitments is needed to read the data. The ballot data can only be read if the person has a key that is set on commitments.
53. A false sense of security is provided to both parties that votes are not being "REPLACED" during the mixing phase. Basically, Scytl re-encrypts the ballot data that comes in from Dominion (or any other voting software company) as ciphertexts. Scytl is supposed to prove that votes A, B, C are indeed X, Y, Z under their new re-encryption when sending back the votes that are tallied coding them respectively. This is done by Scytl and the Election Software company that agrees to certain

"Generators" and therefore together build "commitments."

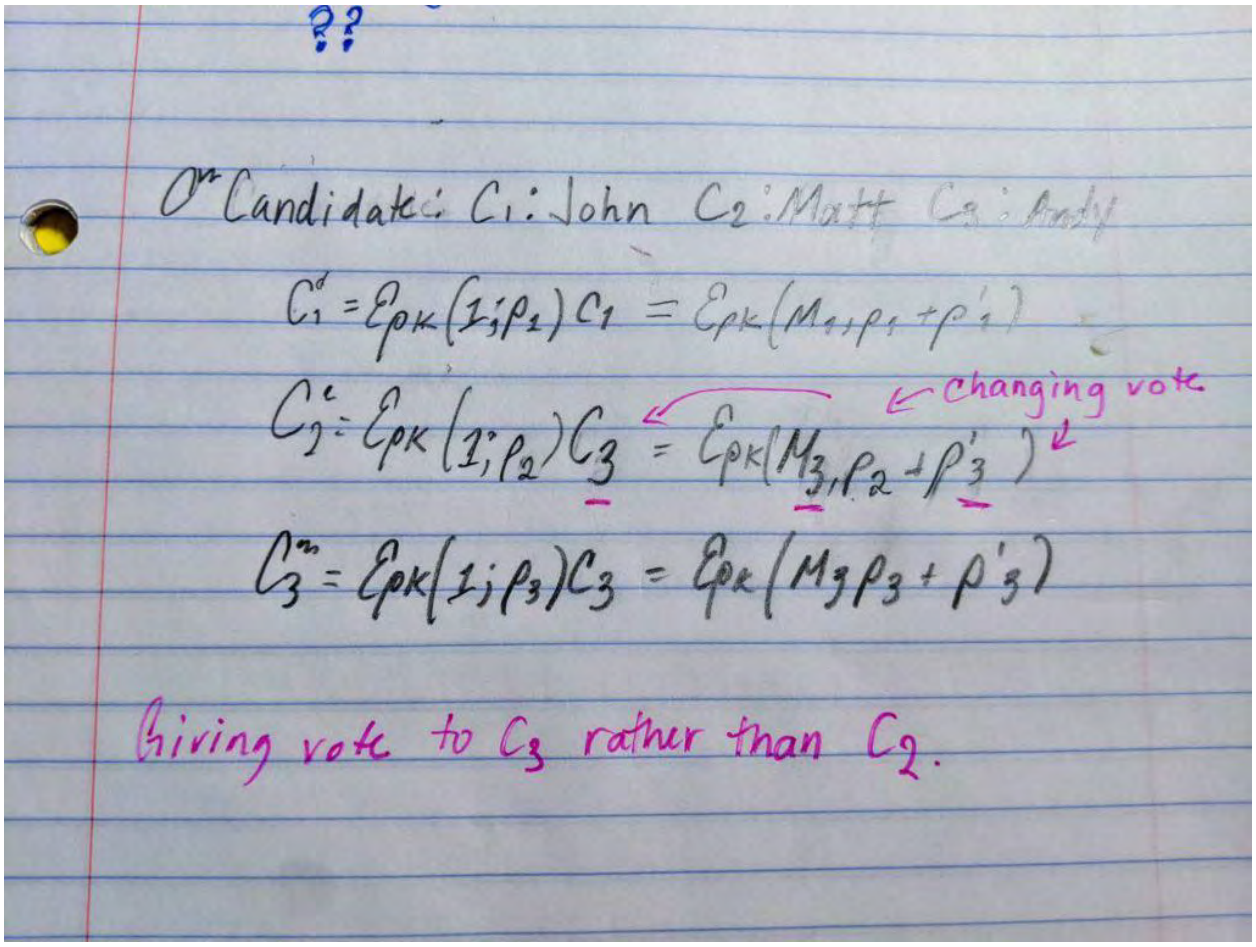
```
public CommitmentParams(final ZpSubgroup group, final int n) {
        group = group;
        h = GroupTools.getRandomElement(group);
        commitmentlength = n;
        g = GroupTools.getVectorRandomElement(group,
this.commitmentlength);
        }

        // from getRandomElement(group)
Exponent randomExponent = ExponentTools.getRandomExponent(group.getQ());
return group.getGenerator().exponentiate(randomExponent);
```

54. Scytl and Dominion have an agreement – only the two would know the parameters. This means that access is able to occur through backdoors in hardware if the parameters of the commitments are known in order to alter the range of the algorithm deployed to satisfy the outcome sought in the case of algorithm failure.
55. Trapdoor is a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able change the value of the commitments however it likes. In other words, Scytl or anyone that knows the commitment parameters can take all the votes and give them to any one they want. If they have a total of 1000 votes an algorithm can distribute them among all races as it deems necessary to achieve the goals it wants. (Case Study: Estonia)

56. 

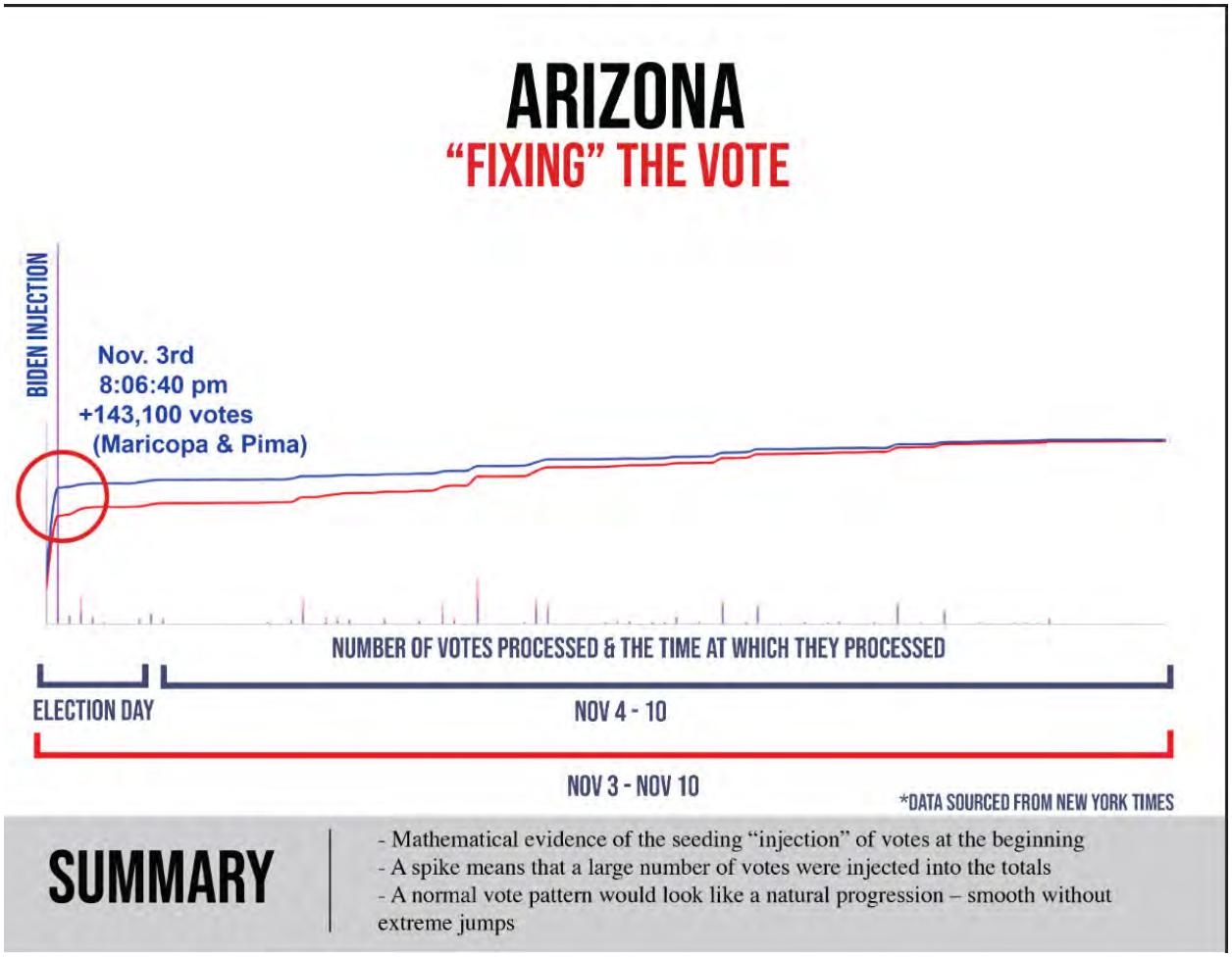
57. Within the trapdoor this is how the algorithm behaves to move the goal posts in elections without being detected by this proof . During the mixing phase this is the algorithm you would use to

"reallocate" votes via an algorithm to achieve the goal set.

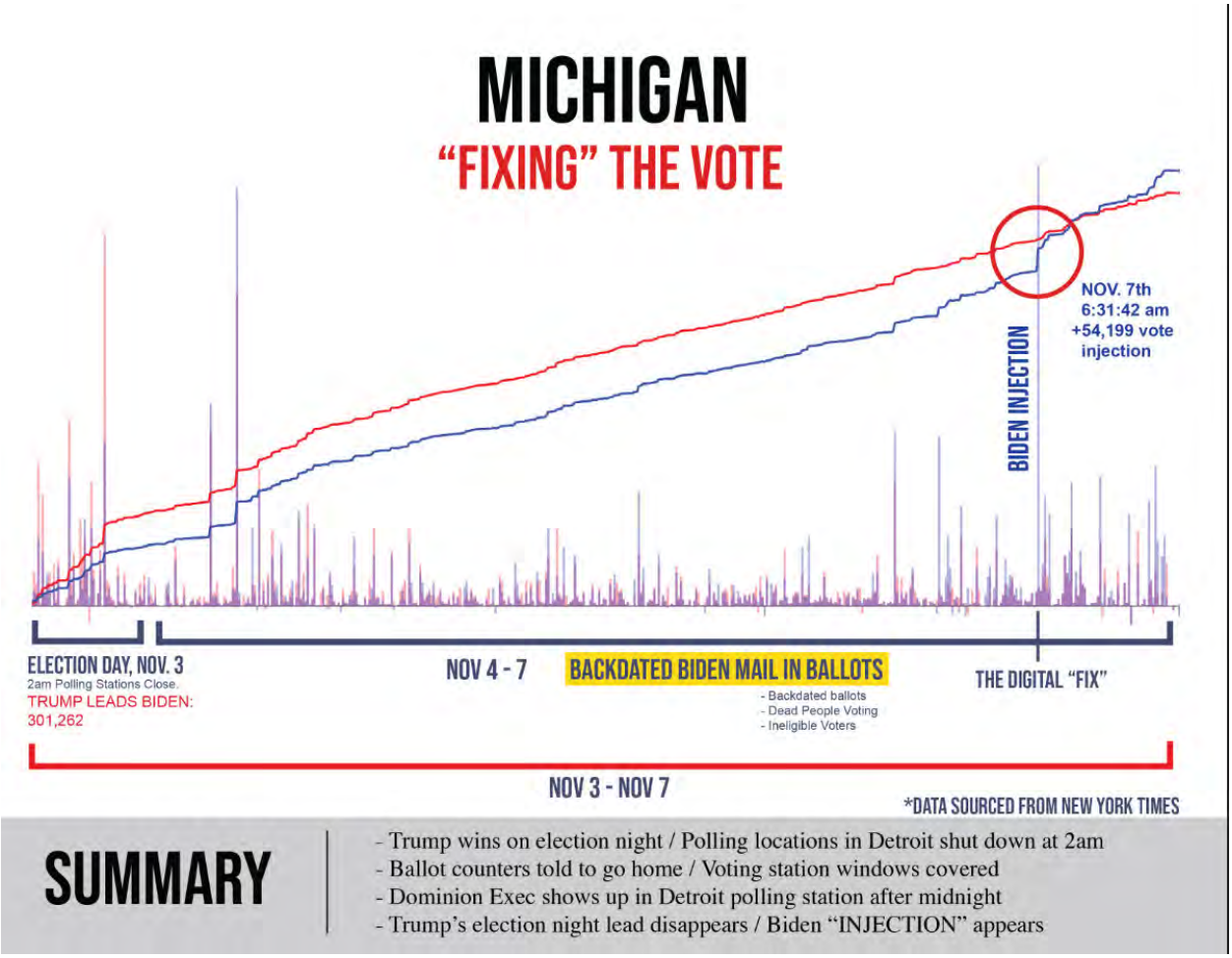


58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that the randomness is applied and used to generate the tally vote ciphertext. Thus in this case, Scytl who is the mixer can collude with their vote company clients or an agency (-------) to change votes and get away with it. This is because the receiver doesn't have the decryption key so they rely solely on Scytl to be ***honest*** or free from any foreign actors within their backdoor or the Election Company (like Dominion) that can have access to the key.
59. In fact, a study from the University of Bristol made claim that interference can be seen when there is a GREAT DELAY in reporting and finalizing numbers University of Bristol : How not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios
60. "Zero-knowledge proofs of knowledge allow a prover to convince a verifier that she holds information satisfying some desirable properties without revealing anything else." David Bernhard, Olivier Pereira,and Bogdan Warinschi.

61. Hence, you can't prove anyone manipulated anything. The TRAP DOOR KEY HOLDERS can offer you enough to verify to you what you need to see without revealing anything and once again indicating the inability to detect manipulation. **ZERO PROOF of INTEGRITY OF THE VOTE.**
62. Therefore, if decryption is challenged, the administrator or software company that knows the trap door key can provide you proof that would be able to pass verification (blind). This was proven to be factually true in the case study by The University of Melbourne in March. White Hat Hackers purposely altered votes by knowing the parameters set in the commitments and there was no way to prove they did it – or any way to prove they didn't.
63. IT'S THE PERFECT THREE CARD MONTY. That's just how perfect it is. They fake a proof of ciphertexts with KNOWN "RANDOMNESS" .This rolls back to the integrity of the VOTE. The vote is not safe using these machines not only because of the method used for ballot "cleansing" to maintain anonymity but the EXPOSURE to foreign interference and possible domestic bad actors.
64. In many circumstances, manipulation of the algorithm is NOT possible in an undetectable fashion. This is because it is one point heavy. Observing the elections in 2020 confirm the deployment of an algorithm due to the BEHAVIOR which is indicative of an algorithm in play that had no pivoting parameters applied.
65. The behavior of the algorithm is that one point (B) is the greatest point within the allocated set. It is the greatest number within the A B points given. Point A would be the smallest. Any points outside the A B points are not necessarily factored in yet can still be applied.
66. The points outside the parameters can be utilized to a certain to degree such as in block allocation.
67. The algorithm geographically changed the parameters of the algorithm to force blue votes and ostracize red.
68. Post block allocation of votes the two points of the algorithm were narrowed ensuring a BIDEN win hence the observation of NO Trump Votes and some BIDEN votes for a period of time.

69. 
ARIZONA
"FIXING" THE VOTE
BIDEN INJECTION
Nov. 3rd
8:06:40 pm
+143,100 votes
(Maricopa & Pima)
NUMBER OF VOTES PROCESSED & THE TIME AT WHICH THEY PROCESSED
ELECTION DAY
NOV 4 - 10
NOV 3 - NOV 10
*DATA SOURCED FROM NEW YORK TIMES
SUMMARY
- Mathematical evidence of the seeding "injection" of votes at the beginning
- A spike means that a large number of votes were injected into the totals
- A normal vote pattern would look like a natural progression – smooth without extreme jumps

70. Gaussian Elimination without pivoting explains how the algorithm would behave and the election results and data from Michigan confirm FAILURE of algorithm.



71. The "Digital Fix" observed with an increased spike in VOTES for Joe Biden can be determined as evidence of a pivot. Normally it would be assumed that the algorithm had a Complete Pivot. Wilkinson's demonstrated the guarantee as :

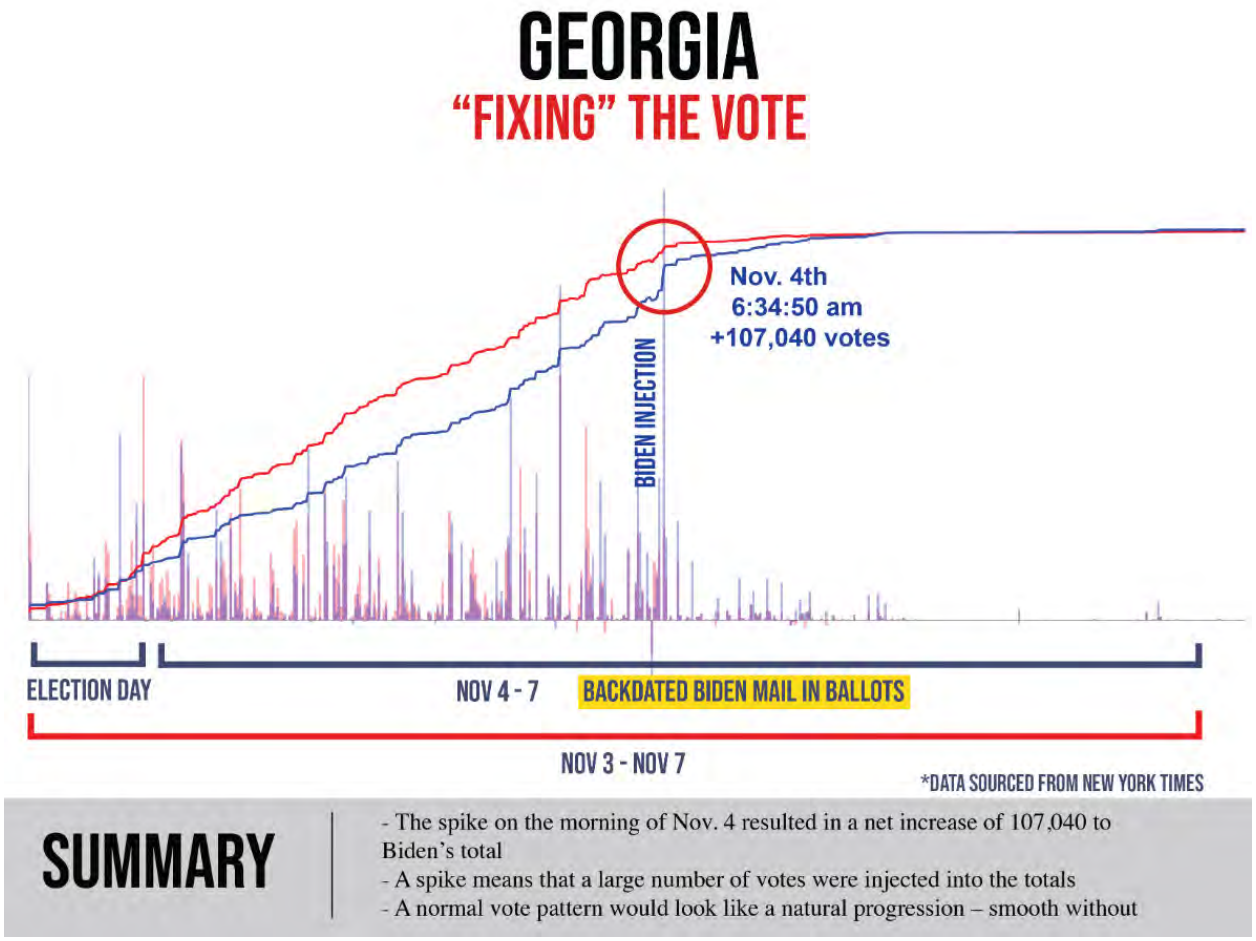
$$\frac{\|U\|_\infty}{\|A\|_\infty} \leq n^{\frac{1}{2}\log(n)}$$

72.

73. Such a conjecture allows the growth factor the ability to be upper bound by values closer to n. Therefore, complete pivoting can't be observed because there would be too many floating points. Nor can partial as the partial pivoting would overwhelm after the "injection" of votes. Therefore, external factors were used which is evident from the "DIGITAL FIX"

74. Observing the elections, after a review of Michigan's data a spike of 54,199 votes to Biden. Because it is pushing and pulling and keeping a short distance between the 2 candidates; but then a spike, which is how an algorithm presents; - and this spike means there was a pause and an insert was made, where they insert an algorithm. Block spikes in votes for JOE BIDEN were NOT paper

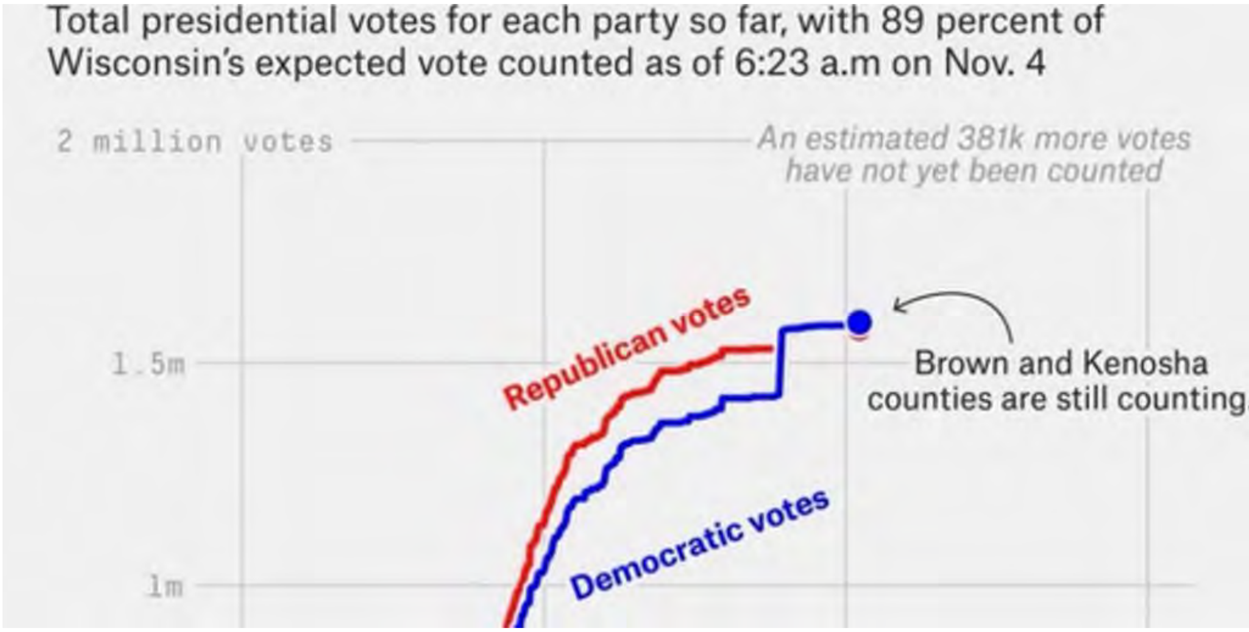
ballots being fed or THUMB DRIVES. The algorithm block adjusted itself and the PEOPLE were creating the evidence to BACK UP the block allocation.

75. I have witnessed the same behavior of the election software in countries outside of the United States and within the United States. In -------, the elections conducted behaved in the same manner by allocating BLOCK votes to the candidate "chosen" to win.
76. Observing the data of the contested states (and others) the algorithm deployed is identical to that which was deployed in 2012 providing Barack Hussein Obama a block allocation to win the 2012 Presidential Elections.
77. The algorithm looks to have been set to give Joe Biden a 52% win even with an initial 50K+ vote block allocation was provided initially as tallying began (as in case of Arizona too). In the am of November 4, 2020 the algorithm stopped working, therefore another "block allocation" to remedy the failure of the algorithm. This was done manually as ALL the SYSTEMS shut down NATIONWIDE to avoid detection.
78. 

79. In Georgia during the 2016 Presidential Elections a failed attempt to deploy the scripts to block allocate votes from a centralized location where the "trap-door" key lay an attempt by someone using

the DHS servers was detected by the state of GA. The GA leadership assumed that it was “Russians” but later they found out that the IP address was that of DHS.

80. In the state of Wisconsin, we observed a considerable BLOCK vote allocation by the algorithm at the SAME TIME it happened across the nation. All systems shut down at around the same time.

81. 

82. In Wisconsin there are also irregularities in respect to BALLOT requests. (names AND address Hidden for privacy)

83.

F	G	H	V	W	X	Y	AB	AC	AD	AG	AH	AI	AJ	AK	AL	A
Active	Registered	Military	Brown County	11/01/2020	Online	Military		Official	Active	Not Returned	Online	11/01/2020				
Active	Registered	Regular	Brown County	10/23/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	10/23/2020	10/23/2020			
Active	Registered	Military	Brown County	11/01/2020	Online	Military		Official	Active	Not Returned	Online	11/01/2020				
Active	Registered	Regular	Brown County	11/01/2020	Online											
Active	Registered	Regular	Brown County	11/01/2020	Email	Regular		Official	Active	Returned	Mail	10/31/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/01/2020	Email	Regular		Official	Active	Returned	Mail	10/31/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Online											
Active	Registered	Regular	Brown County	11/02/2020	Received In Persor	Hospitaliz		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Email	Hospitaliz		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020			
Active	Registered	Military	Brown County	11/02/2020	Mail											
Active	Registered	Regular	Brown County	11/02/2020	Mail	Regular		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020			
Active	Registered	Regular	Brown County	11/02/2020	Mail	Regular		Official	Active	Returned	Appointed Agent		11/02/2020			
Active	Registered	Military	Brown County	11/02/2020	Online	Military		Official	Active	Not Returned	Online	11/02/2020				
Active	Registered	Military	Brown County	11/02/2020	Online	Military		Official	Active	Not Returned	Online	11/02/2020				
Active	Registered	Regular	Brown County	11/02/2020	Online											
Active	Registered	Military	Brown County	11/02/2020	FPCA	Military		Official	Active	Not Returned	Mail	11/02/2020				
Active	Registered	Military	Brown County	11/02/2020	FPCA	Military		Official	Active	Returned	Email	11/02/2020	11/03/2020			
Active	Registered	Regular	Brown County	11/03/2020	Voted in Person	Regular		Official	Inactive	Voter Spoiled	Voted In Person	11/03/2020	11/03/2020			
Active	Registered	Military	Brown County	11/03/2020	Mail	Military	Certification insufficient	Federal Absent	Active	Returned, to be Rejected	Mail	11/03/2020	11/03/2020			
Active	Registered	Military	Brown County	11/03/2020	Mail	Military		Official	Active	Not Returned	Mail	11/03/2020				
Active	Registered	Military	Brown County	11/03/2020	Online											
Active	Registered	Regular	Brown County	11/03/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											
Active	Registered	Regular	Brown County	11/04/2020	Online											

84.

Active	Registered	Regular	Brown County	11/03/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/04/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/05/2020	Online
Active	Registered	Regular	Brown County	11/06/2020	Online
Active	Registered	Regular	Brown County	11/06/2020	Online

85. I can personally attest that in 2013 discussions by the Obama / Biden administration were being had with various agencies in the deployment of such election software to be deployed in ----- in 2013.
86. On or about April 2013 a one year plan was set to fund and usher elections in -----.
87. Joe Biden was designated by Barack Hussein Obama to ensure the ----- accepted assistance.
88. John Owen Brennan and James (Jim) Clapper were responsible for the ushering of the intelligence surrounding the elections in -----.
89. Under the guise of Crisis support the US Federal Tax Payers funded the deployment of the election software and machines in ------ signing on with Scytl.

The White House
Office of the Press Secretary

For Immediate Release — April 21, 2014

SHARE THIS: TWITTER FACEBOOK EMAIL

FACT SHEET: U.S. Crisis Support Package for Ukraine

President Obama and Vice President Biden have made U.S. support for Ukraine an urgent priority as the Ukrainian government works to establish security and stability, pursue democratic elections and constitutional reform, revive its economy, and ensure government institutions are transparent and accountable to the Ukrainian people. Ukraine embarks on this reform path in the face of severe challenges to its sovereignty and territorial integrity, which we are working to address together with Ukraine and our partners in the international community. The United States is committed to ensuring that Ukrainians alone are able to determine their country's future without intimidation or coercion from outside forces. To support Ukraine, we are today announcing a new package of assistance totaling **$50 million** to help Ukraine pursue political and economic reform and strengthen the partnership between the United States and Ukraine.

90.

91. Right before the ----- elections it was alleged that CyberBerkut a pro-Russia group infiltrated --- central election computers and **deleted key files**. These actions supposedly rendered the vote-tallying system inoperable.
92. In fact, the KEY FILES were the Commitment keys to allow Scytl to tally the votes rather than the election machines. The group had disclosed emails and other documents proving that their election was rigged and that they tried to avoid a fixed election.
93. The elections were held on May 25, 2014 but in the early AM hours the election results were BLOCKED and the final tally was DELAYED flipping the election in favor of -----.
94. The claim was that there was a DDoS attack by Russians when in actual fact it was a mitigation of the algorithm to inject block votes as we observed was done for Joe Biden because the KEYS were unable to be deployed. In the case of -----, the trap-door key was "altered"/deleted/ rendered ineffective. In the case of the US elections, representatives of Dominion/ ES&S/ Smartmatic/ Hart Intercivic would have to manually deploy them since if the entry points into the systems seemed to have failed.
95. The vote tallying of all states NATIONWIDE stalled and hung for days – as in the case of Alaska that has about 300K registered voters but was stuck at 56% reporting for almost a week.
96. This "hanging" indicates a failed deployment of the scripts to block allocate remotely from one location as observed in ------ on May 26, 2014.
97. This would justify the presence of the election machine software representatives making physical appearances in the states where the election results are currently being contested.
98. A Dominion Executive appeared at the polling center in Detroit after midnight.
99. Considering that the hardware of the machines has NOT been examined in Michigan since 2017 by Pro V& V according to Michigan's own reporting. COTS are an avenue that hackers and bad actors seek to penetrate in order to control operations. Their software updates are the reason vulnerabilities to foreign interference in all operations exist.
100. The importance of VSTLs in underrated to protect up from foreign interference by way of open access via COTS software. Pro V& V who's EAC certification EXPIRED on 24 FEB 2017 was contracted with the state of WISCONSIN.
101. In the United States each state is tasked to conduct and IV& V (Independent Verification and Validation) to provide assurance of the integrity of the votes.
102. If the "accredited" non-federal entities have NOT received EAC accreditation this is a failure of the states to uphold their own states standards that are federally regulated.
103. In addition, if the entities had NIST certificates they are NOT sufficing according the HAVA ACT 2002 as the role of NIST is clear.
104. Curiously, both companies PRO V&V and SLI GAMING received NIST certifications OUTSIDE the 24 month scope.

105. PRO V& V received a NIST certification on 26MAR2020 for ONE YEAR. Normally the NIST certification is good for two years to align with that of EAC certification that is good for two years.

106.

United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200978-0

Pro V&V
Huntsville, AL

is accredited by the National Voluntary Laboratory Accreditation Program for specific services, listed on the Scope of Accreditation, for:

Voting System Testing

This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).

2020-03-26 through 2021-03-31
Effective Dates

DEPARTMENT OF COMMERCE * UNITED STATES OF AMERICA

For the National Voluntary Laboratory Accreditation Program

107. The last PRO V& V EAC accreditation certificate (Item 8) of this declaration expired in February 2017 which means that the IV & V conducted by Michigan claiming that they were accredited is false.

108. The significance of VSTLs being accredited and examining the HARDWARE is key. COTS software updates are the avenues of entry.

109. As per DOMINION'S own petition, the modems they use are COTS therefore failure to have an accredited VSTL examine the hardware for points of entry by their software is key.

*Compact Flash Cards	***SanDisk Ultra: SDCFHS-004G SDCFHS-008G RiData: CFC-14A RDF8G-233XMCB2-1 RDF16G-233XMCB2-1 RDF32G-233XMCB2-1 SanDisk Extreme: SDCFX-016G SDCFX-032G SanDisk: SDFAA-008G		Memory device for ICP and ICE tabulators.
*Modems	Verizon USB Modem Pantech UMW190NCD USB Modem MultiTech MT9234MU CellGo Cellular Modem E-Device 3GPUSUS AT&T USB Modem MultiTech GSM MTD-H5 Fax Modem US Robotics 56K V.92.		Analog and wireless modems for transmitting unofficial election night results.

110.

111. For example and update of Verizon USB Modem Pantech undergoes multiple software updates a year for it's hardware. That is most likely the point of entry into the systems.

112. During the 2014 elections in ---- it was the modems that gave access to the systems where the commitment keys were deleted.

113. SLI Gaming is the other VSTL "accredited" by the EAC BUT there is no record of their accreditation. In fact, SLI was NIST ISO Certified 27 days before the election which means that PA IV&V was conducted without NIST cert for SLI being valid.

114. 

United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200733-0

SLI Compliance
Wheat Ridge, CO

is accredited by the National Voluntary Laboratory Accreditation Program for specific services, listed on the Scope of Accreditation, for:

Voting System Testing

This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).

2020-10-07 through 2020-12-31
Effective Dates

For the National Voluntary Laboratory Accreditation Program

115. In fact SLI was NIST ISO Certified for less than 90 days.

116. I can personally attest that high-level officials of the Obama/Biden administration and large private contracting firms met with a software company called GEMS which is ultimately the software ALL election machines run now running under the flag of DOMINION.

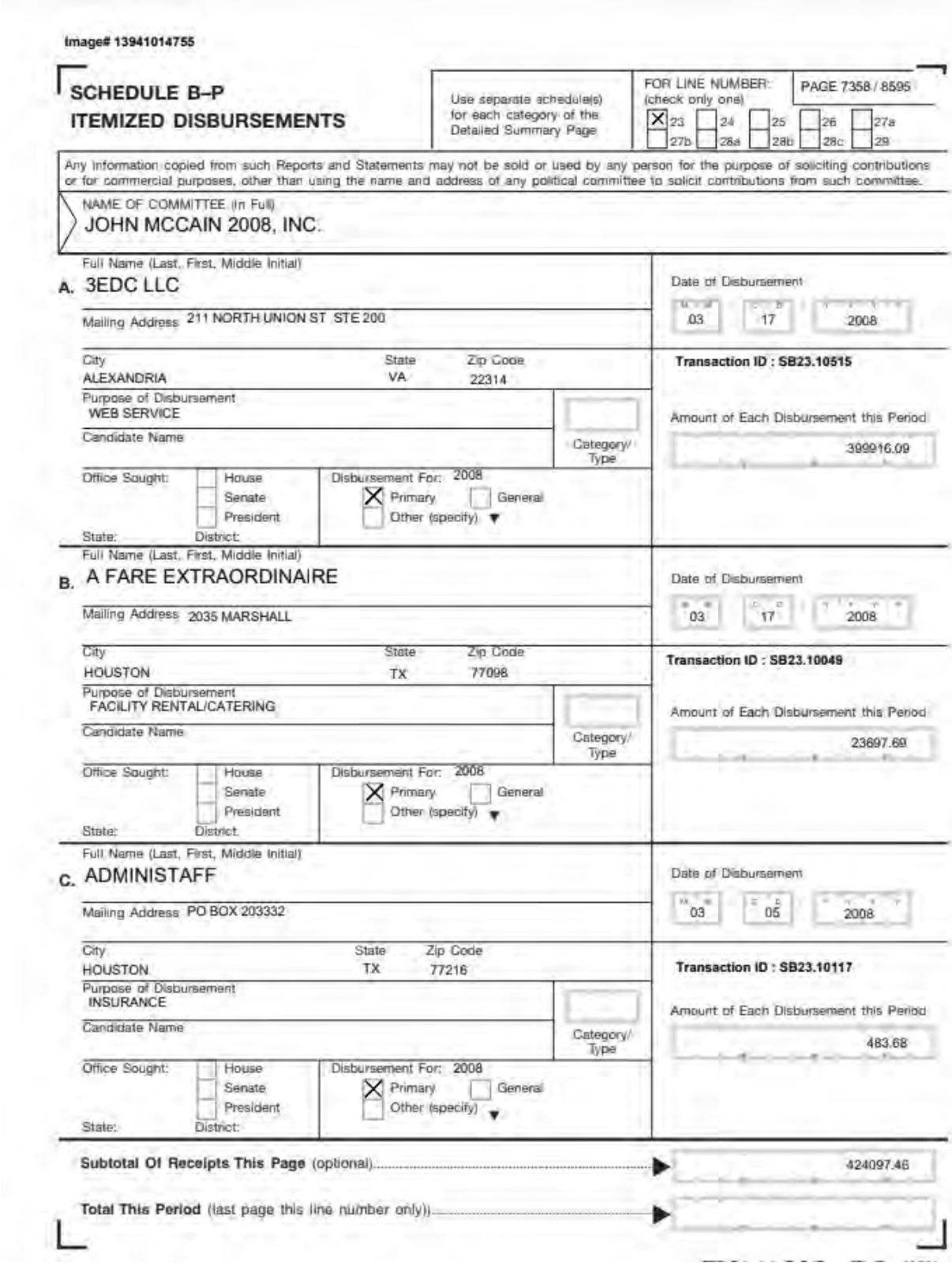
117. GEMS was manifested from SOE software purchased by SCYTL developers and US Federally Funded persons to develop it.

118. The only way GEMS can be deployed across ALL machines is IF all counties across the nation are housed under the same server networks.

119. GEMS was tasked in 2009 to a contractor in Tampa, Fl.

120. GEMS was also fine-tuned in Latvia, Belarus, Serbia and Spain to be localized for EU deployment as observed during the Swissport election debacle.

121. John McCain's campaign assisted in FUNDING the development of GEMS web monitoring via WEB Services with 3EDC and Dynology.



Image# 13941014755

SCHEDULE B–P
ITEMIZED DISBURSEMENTS

Use separate schedule(s) for each category of the Detailed Summary Page

FOR LINE NUMBER: (check only one)
☒ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27a
☐ 27b ☐ 28a ☐ 28b ☐ 28c ☐ 29

PAGE 7358 / 8595

Any information copied from such Reports and Statements may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes, other than using the name and address of any political committee to solicit contributions from such committee.

NAME OF COMMITTEE (In Full)
JOHN MCCAIN 2008, INC.

A. Full Name (Last, First, Middle Initial)
3EDC LLC
Mailing Address 211 NORTH UNION ST STE 200
City ALEXANDRIA State VA Zip Code 22314
Purpose of Disbursement: WEB SERVICE
Candidate Name
Category/ Type
Office Sought: ☐ House ☐ Senate ☐ President
State: District:
Disbursement For: 2008 ☒ Primary ☐ General ☐ Other (specify)
Date of Disbursement: 03 17 2008
Transaction ID : SB23.10515
Amount of Each Disbursement this Period: 399916.09

B. Full Name (Last, First, Middle Initial)
A FARE EXTRAORDINAIRE
Mailing Address 2035 MARSHALL
City HOUSTON State TX Zip Code 77098
Purpose of Disbursement: FACILITY RENTAL/CATERING
Candidate Name
Category/ Type
Office Sought: ☐ House ☐ Senate ☐ President
State: District:
Disbursement For: 2008 ☒ Primary ☐ General ☐ Other (specify)
Date of Disbursement: 03 17 2008
Transaction ID : SB23.10049
Amount of Each Disbursement this Period: 23697.69

C. Full Name (Last, First, Middle Initial)
ADMINISTAFF
Mailing Address PO BOX 203332
City HOUSTON State TX Zip Code 77216
Purpose of Disbursement: INSURANCE
Candidate Name
Category/ Type
Office Sought: ☐ House ☐ Senate ☐ President
State: District:
Disbursement For: 2008 ☒ Primary ☐ General ☐ Other (specify)
Date of Disbursement: 03 05 2008
Transaction ID : SB23.10117
Amount of Each Disbursement this Period: 483.68

Subtotal Of Receipts This Page (optional) ▶ 424097.46

Total This Period (last page this line number only) ▶

122.

123.

124. AKAMAI Technologies services SCYTL.

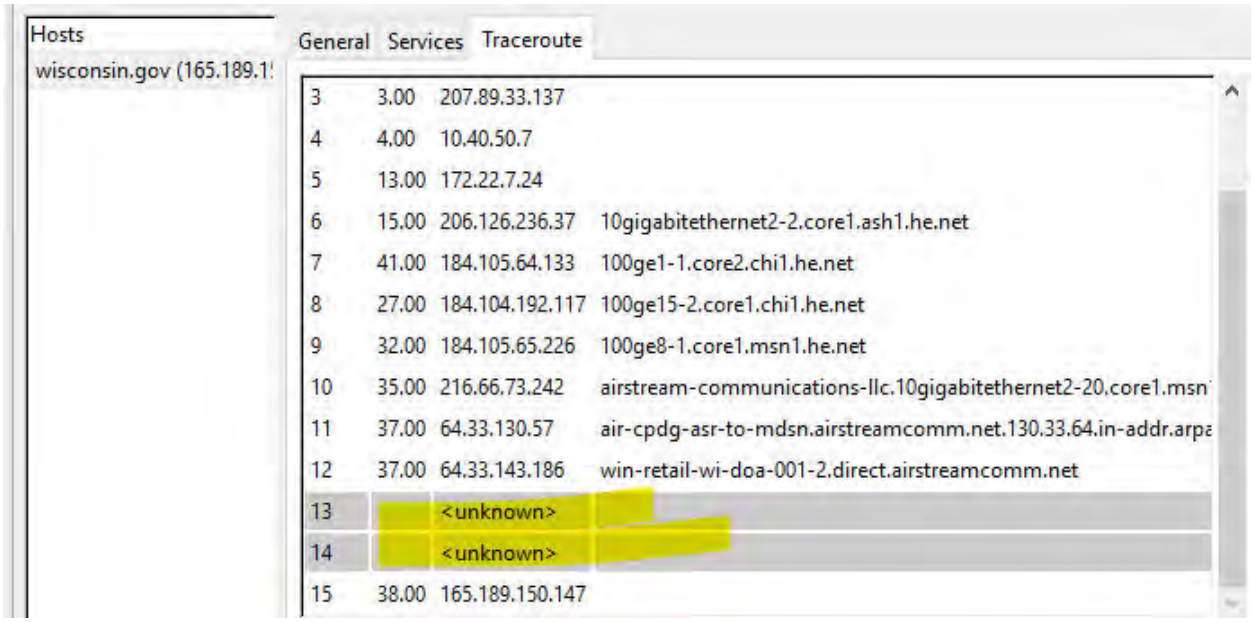
125. AKAMAI Technologies Houses ALL foreign government sites. (Please see White Paper by Akamai.)

126. AKAMAI Technologies houses ALL .gov state sites. (ref Item 123 Wisconsin.gov Example)

127. 

128. Wisconsin has EDGE GATEWAY port which is AKAMAI TECHNOLOGIES based out of GERMANY.

129. Using AKAMAI Technologies is allowing .gov sites to obfuscate and mask their systems by way of HURRICANE ELECTRIC (he.net) Kicking it to anonymous (AKAMAI Technologies) offshore servers.

130. 

131. AKAMAI Technologies has locations around the world.

132. AKAMAI Technologies has locations in China (ref item 22)

133. AKAMAI Technologies has locations in Iran as of 2019.

134. AKAMAI Technologies merged with UNICOM (CHINESE TELECOMM) in 2018.

135. AKAMAI Technologies house all state .gov information in GERMANY via TELIA AB.

136. In my professional opinion, this affidavit presents unambiguous evidence:

137. That there was Foreign interference, complicit behavior by the previous administrations from 1999 up until today to hinder the voice of the people and US persons knowingly and willingly colluding with foreign powers to steer our 2020 elections that can be named in a classified setting.

138. Foreign interference is present in the 2020 election in various means namely,

139. Foreign nationals assisted in the creation of GEMS (Dominion Software Foundation)

140. Akamai Technologies merged with a Chinese company that makes the COTS components of the election machines providing access to our electronic voting machines.

141. Foreign investments and interests in the creation of the GEMS software.

142. US persons holding an office and private individuals knowingly and willingly oversaw fail safes to secure our elections.

143. The EAC failed to abide by standards set in HAVA ACT 2002.

144. The IG of the EAC failed to address complaints since their appointment regarding vote integrity

145. Christy McCormick of the EAC failed to ensure that EAC conducted their duties as set forth by HAVA ACT 2002

146. Both Patricia Layfield (IG of EAC) and Christy McCormick (Chairwoman of EAC) were appointed by Barack Hussein Obama and have maintained their positions since then.

147. The EAC failed to have a quorum for over a calendar year leading to the inability to meet the standards of the EAC.

148. AKAMAI Technologies and Hurricane Electric raise serious concerns for NATSEC due to their ties with foreign hostile nations.

149. For all the reasons above a complete failure of duty to provide safe and just elections are observed.

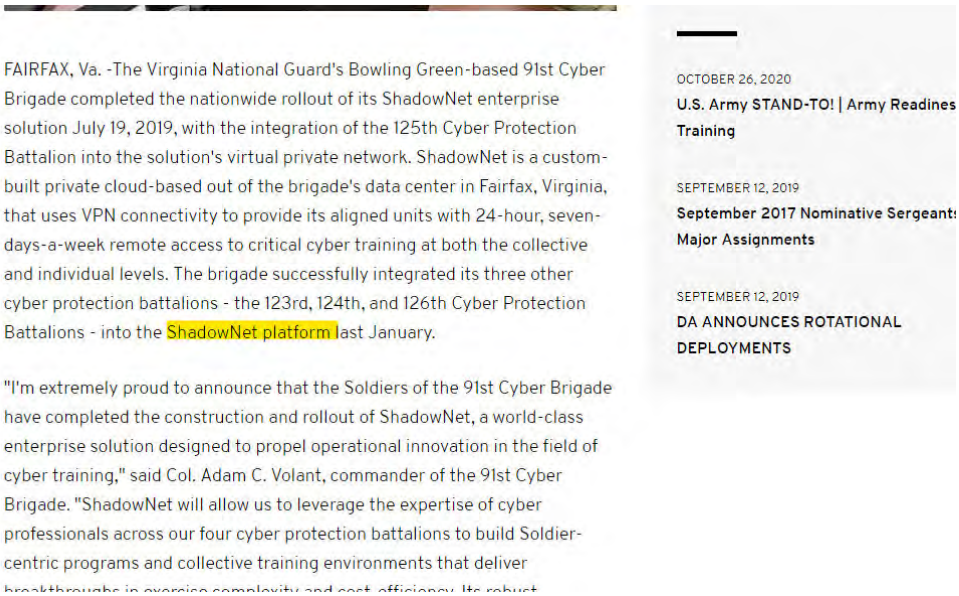
150. For the people of the United States to have confidence in their elections our cybersecurity standards should not be in the hands of foreign nations.

151. Those responsible within the Intelligence Community directly and indirectly by way of procurement of services should be held accountable for assisting in the development, implementation and promotion of GEMS.

152. GEMS ------- General Hayden.

153. In my opinion and from the data and events I have observed ---------- with the assistance of SHADOWNET under the guise of L3-Communications which is MPRI. This is also confirmed by us.army.mil making the statement that shadownet has been deployed to 30 states which all

happen to be using Dominion Machines.



FAIRFAX, Va. -The Virginia National Guard's Bowling Green-based 91st Cyber Brigade completed the nationwide rollout of its ShadowNet enterprise solution July 19, 2019, with the integration of the 125th Cyber Protection Battalion into the solution's virtual private network. ShadowNet is a custom-built private cloud-based out of the brigade's data center in Fairfax, Virginia, that uses VPN connectivity to provide its aligned units with 24-hour, seven-days-a-week remote access to critical cyber training at both the collective and individual levels. The brigade successfully integrated its three other cyber protection battalions - the 123rd, 124th, and 126th Cyber Protection Battalions - into the ShadowNet platform last January.

"I'm extremely proud to announce that the Soldiers of the 91st Cyber Brigade have completed the construction and rollout of ShadowNet, a world-class enterprise solution designed to propel operational innovation in the field of cyber training," said Col. Adam C. Volant, commander of the 91st Cyber Brigade. "ShadowNet will allow us to leverage the expertise of cyber professionals across our four cyber protection battalions to build Soldier-centric programs and collective training environments that deliver

OCTOBER 26, 2020
U.S. Army STAND-TO! | Army Readines
Training

SEPTEMBER 12, 2019
September 2017 Nominative Sergeants
Major Assignments

SEPTEMBER 12, 2019
DA ANNOUNCES ROTATIONAL
DEPLOYMENTS

154. Based on my research of voter data – it appears that there are approximately 23,000 residents of a Department of Corrections Prison with requests for absentee ballot in Wisconsin. We are currently reviewing and verifying the data and will supplement.

	23230	Gutierrez	Mary	Jane		(262)994-9050	
23231	**23231**	Hansen	Luann	M		(262)994-9050	
23232	**23232**	Neberman	John	C		(262)994-9050	
23233	**23233**	Reynolds	Devi	J		(262)994-9050	
23234	**23234**	Rieckhoff	Kathryn	Susan		(262)994-9050	
23235	**23235**	Edwards	Mark	Landon		(262)994-9050	
23236	**23236**	Pfeiffer	Joseph	Patrick		(262)994-9050	
23237	**23237**	Hines	Dianna	K		(262)994-9050	
23238	**23238**	Beachem	Janice	F		(262)994-9050	
23239	**23239**	Blackstone	Thomas	Wayne		(262)994-9050	
23240	**23240**	Braun	Patricia	Ann		(262)994-9050	
23241	**23241**	Smith	Raymond	L		(262)994-9050	
23242	**23242**	Meyer	Steven	R		(262)994-9050	
23243	**23243**	Vincent	Herbert			(262)994-9050	
23244	**23244**	Guajardo	Juan	P		(262)994-9050	
23245	**23245**	Wallace	Kirk	R		(262)994-9050	
23246	**23246**	Kaplan	Bernard	L		(262)994-9050	
23247	**23247**	Bahrs	Michelle	M		(262)994-9050	
23248	**23248**	Shattuck	Elizabeth	L		(262)994-9050	
23249	**23249**	Munoz	Rosalio	S	JR	(262)994-9050	
23250	**23250**	Strunk	Amy	C		(262)994-9050	
23251	**23251**	Schendel	Michael	P	JR	(262)994-9050	
23252	**23252**	Mack	Kimberly	N		(262)994-9050	
23253	**23253**	Spikes	Debra	A		(262)994-9050	
23254	**23254**	Busarow	Suzanne	M		(262)994-9050	
23255	**23255**	Oliver	Timmy			(262)994-9050	
23256	**23256**	Wember	Jimmy	Dean		(262)994-9050	
23257	**23257**	Kosterman	Michael	Richard		(262)994-9050	
23258	**23258**	Szaradowski	Paul	M		(262)994-9050	
23259	**23259**	Oliver	Dale			(262)994-9050	
23260	**23260**	Derango	Nancy			(262)994-9050	
23261	**23261**	Smith	Arthur	J		(262)994-9050	SMITH24.3059@YAHOO
23262	**23262**	Brown	Michael	Edward		(262)994-9050	

155.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge. Executed this November 29th, 2020.

EXHIBIT 7

Cryptanalysis of FROG

David Wagner* Niels Ferguson† Bruce Schneier‡

October 23, 1999

Abstract

We examine some attacks on the FROG cipher. First we give a differential attack which uses about 2^{58} chosen plaintexts and very little time for the analysis; it works for about $2^{-33.0}$ of the keyspace. Then we describe a linear attack which uses 2^{56} known texts and works for $2^{-31.8}$ of the keyspace. The linear attack can also be converted to a ciphertext-only attack using 2^{64} known ciphertexts. Also, the decryption function of FROG is a lot weaker than the encryption function. We show a differential attack on the decryption function that requires 2^{36} chosen ciphertexts and works on $2^{-29.3}$ of the keyspace. Using our best attack an attacker with a sufficient number of cryptanalytical targets can expect to recover his first key after $2^{56.7}$ work.

Taken together, these observations suggest that FROG is not a very strong candidate for the AES.

1 Introduction

FROG [3] is a block cipher submitted to the AES competition with a novel internal structure. It uses 8 cycles, where each cycle consists of 16 rounds. Round r ($r = 0, \ldots, 15$) of the q-th cycle ($q = 0, \ldots, 7$) modifies the 16 bytes $X_{0\ldots15}$ of the internal block according to the three (sequential) operations

$$\begin{aligned} X_r &\leftarrow S_q(X_r \oplus K_{q,r}) \\ X_{r+1} &\leftarrow X_{r+1} \oplus X_r \\ X_{\pi_q(r)} &\leftarrow X_{\pi_q(r)} \oplus X_r, \end{aligned}$$

*University of California Berkeley, Soda Hall, Berkeley, CA 94720, USA; daw@cs.berkeley.edu.

†Counterpane Systems, 101 E Minnehaha Parkway, Minneapolis, MN 55419, USA; niels@counterpane.com.

‡Counterpane Systems; schneier@counterpane.com.

where the indices are to be taken modulo 16. Here the round subkeys consist of a bijective byte-wide S-box S_q, a so-called "bomb" permutation π_q of the symbols $\{0, 1, \ldots, 15\}$, and an array of subkey bytes $K_{q,r}$. In all, the cipher contains 128 rounds, and so the key schedule expands a k-bit master key ($k = 128, 192, 256$) into a large amount of subkey material.

The FROG expanded key has a redundancy in it. The input to the S-box consists of a data byte XORed with a key byte. If we take any value u we can XOR each of the key bytes with u and update the S-box to include an extra XOR with u at the input. This results in an equivalent expanded key. During an attack we can just set one key byte or one S-box entry in each round to an arbitrary value without loss of generality.

One aspect of FROG that complicates the analysis is the key-dependent nature of the internal structure: the quality of internal diffusion depends heavily on the (key-dependent) choice of the "bomb" permutations π_q. We deal with this issue by characterizing every attack with three parameters. The first one is the fraction of keys F for which the attack is successful. The second parameter is the complexity D of detecting if the key is within that fraction. The third parameter is the complexity C of the rest of the attack. Often C, D, and F can be traded off against each other.

This brings up the question how to compare attacks with different values of C, D, and F. We assume that the attacker has a ready supply of encryption black boxes with different keys, and use the amount of work an attacker has to do before finding the first key as a measure of the quality of the attack. The attacker has to about D/F operations to find a key that is weak plus C operations to recover the key which gives us the total work $D/F + C$. Normally the expression $D/F + C$ is either dominated by D/F (when finding a suitable weak key is the biggest problem) or by C. It is not worth considering attacks which have $D/F > 2^k$ or $C > 2^k$ where k is the key size as these are less useful than a simple exhaustive search.

In this paper, we show that diffusion failures in FROG can lead to real attacks on the full cipher. The key-dependent diffusion structure of FROG is in this respect a weakness as there is a fraction of the keys for which diffusion is weak. In particular, Section 2 describes several useful differential characteristics for FROG, and in Section 3 we give a simple differential attack which needs about 2^{58} chosen plaintexts and very little time for the analysis. The attack works for about $2^{-33.0}$ of the keyspace. Section 4 examines the application of linear cryptanalysis to FROG, showing how to break FROG with about 2^{56} known texts for about $2^{-31.8}$ of the keyspace. Section 5 extends those results to a ciphertext-only setting. In Section 6 we give a differential attack against the decryption function that requires 2^{36}

chosen plaintexts and works for $2^{-29.3}$ of the keyspace. Finally, Section 8 discusses Frog's performance as compared with other block ciphers and its suitability as an AES candidate.

2 Differential characteristics

Suppose the differential characteristic $a \rightarrow a$ holds with probability p_q for the S-box S_q, where $a \neq 0$ is an arbitrary byte-wide difference. Set

$$\beta_0 = (a, a, 0, \ldots, 0)$$

and let β_j be the result of rotating β_0 to right by j byte positions. Then the simple differential characteristic $\beta_1 \rightarrow \beta_0$ can be used to approximate one cycle of FROG with probability p_q when the key is favorable. We can classify the favorable keys as those where $\pi_q(1) = 0$, so it follows that 1/15 of the keyspace is favorable.[1]

We can also obtain 13 more characteristics of a similar form. Namely, $\beta_{j+1} \rightarrow \beta_j$ also holds (for $j = 0, \ldots, 13$) with the same probability, when $\pi_q(j+1) = j$. Of course, these characteristics can be pieced together nicely. This provides an easy way to build a n-cycle differential characteristic $\beta_{j+n} \rightarrow \beta_j$ with probability $\prod_q p_q$; the characteristic will work for $1/15^n$ of the keyspace.

A useful truncated differential characteristic is $\alpha \rightarrow \beta_{13}$, where

$$\alpha = (0, \ldots, 0, b, a)$$

Here b may be any non-zero byte difference. For each a, this holds with average probability 2^{-8} for 1/15 of the keyspace. The advantage of using this characteristic is that it enables us to bypass the first cycle by using structures.

These characteristics can be concatenated to obtain the differential characteristic $\alpha \rightarrow \beta_6$ for the whole 8-cycle cipher. This characteristic will hold with probability $p = 2^{-8} \cdot p_1 \cdot \ldots \cdot p_7$ for $1/15^8 \approx 2^{-31.3}$ of the keyspace. We shall describe in the next section how to use this to break FROG in a 0-R attack.

But first, we focus on analyzing the probability p of this characteristic. The propagation probability p is dependent on the key and on the choice

[1] The way in which π_q is generated results in a distribution very close to $\Pr(\pi_q(x) \in \{x, x+1\}) = 0$, $\Pr(\pi_q(x) = x+2) = 2/15$, and $\Pr(\pi_q(x) = y) = 1/15$ for all other values of y.

of the byte difference a, so we must resort to probabilistic approximations. First of all, modeling S_q as a random permutation suggests that the distribution of p_q is likely to be Poisson with parameter $1/2$. In other words,

$$\Pr[p_q = \frac{2j}{256}] = \frac{e^{-1/2}\, 2^{-j}}{j!}$$

Since we need $p > 0$, we require $p_r > 0$ for $r = 1, \ldots, 7$. Now $\Pr[p_q > 0] = 1 - e^{-1/2}$, so $\Pr[p > 0] = (1 - e^{-1/2})^7 \approx 0.00146$, under the heuristic assumption that the round subkeys behave as though they were chosen independently. There are 255 choices for a, so heuristically we expect that $p > 0$ for at least one of them with probability $1 - (1 - 0.00146)^{255} \approx 2^{-1.7}$. Again assuming the independence of S_q and π_q, this suggests that about $2^{-1.7}/15^8 \approx 2^{-33.0}$ of the keyspace is favorable. A key is said to be favorable if there is some a such that $\pi_q(15 - q) = 14 - q$ (for $q = 0, \ldots, 7$) and $p_q > 0$ (for $q = 1, \ldots, 7$). For a favorable key and a suitable a, the probability of the differential $\alpha \to \beta_6$ is at least $2^{-8} \cdot (2/256)^7 = 2^{-57}$.

Summarizing, we have found that the 8-cycle characteristic $\alpha \to \beta_6$ is expected to hold with probability at least 2^{-57} for $2^{-33.0}$ of the keyspace.

3 The attack

In the first phase of our attack on FROG, we search for a value of a such that the 8-cycle characteristic has probability $p \geq 2^{-57}$. We use a total of 2^{65} plaintext pairs, or 2^{57} pairs for each of the 256 possibilities for a. The required pairs can be generated with 2^{50} chosen plaintext queries by using structures.

Very efficient filtering is possible, since we can eliminate all but those ciphertexts with difference β_6. We should be very surprised if we see even one wrong pair.

As a result, when the key is favorable, we expect to be able to identify the useful value of a where $\alpha \to \beta_6$. (If the key is unfavorable, we can give up at this point.) For the remainder of the attack, we restrict our attention to pairs with this value of a.

In the second phase of our attack, we use knowledge of this value for a to generate 2^{65} more plaintext pairs with this value of a. By using structures, we can form the necessary pairs with about 2^{58} more chosen plaintext queries.

We expect to find about 256 right pairs where the characteristic is followed. These right pairs can be used to deduce the contents of the inverse of

the last-cycle S-box S_7^{-1} with some simple linear algebra. We may treat the 256 entries of S_7^{-1} as 256 formal unknowns. Then each pair of ciphertexts C, C' with $C \oplus C' = \beta_6$ gives us one linear equation on the entries of S_7:

$$S_7^{-1}(C_7) \oplus S_7^{-1}(C'_7) = a.$$

With 256 right pairs, we obtain 256 linear equations on 256 unknowns, which is enough to solve for S_7^{-1} nearly uniquely (up to an unknown XOR at the output of the S-box). We can ignore the remaining XOR freedom at the input since that only selects between equivalent expanded keys. Of course, this gives us most of the entries of S_7 by inversion[2].

Actually, there is a complication. If $\pi_7(j) = 7$ for some $j > 7$, then the previous approach will not work. However, a simple modification usually will. If the previous technique fails, we note that

$$S_7^{-1}(C_7 \oplus C_j) \oplus S_7^{-1}(C'_7 \oplus C_j) = a,$$

and try the linear algebra approach again eight more times for each of $j = 8, \ldots, 15$. With this modification, S_7 can be recovered with excellent probability.

In this way we can recover S_7 with very little work. At this point, we may continue by peeling off the outer cycles (making a few guesses where necessary) and repeating the attack, though a bit of care is required to make this work.

Using out terminology from section 1 this attack has $D = 2^{50}$, $F = 2^{-33.0}$ and $C = 2^{58}$. We thus expect that an attacker will recover a key after 2^{83} operations.

As stated, this is an adaptive chosen plaintext attack. However, the adaptivity may be easily removed by requesting all 2^{58} chosen plaintexts in advance. The only reason we stated the attack in its adaptive form is that the chosen text complexity is somewhat reduced when the key is not favorable.

Besides the differential $\alpha \to \beta_6$ there are six more differentials with the same properties. These are constructed by rotating the differential $\alpha \to \beta_6$ between 1 and 6 bytes positions to the left. Using structures we can run the attack for all seven differentials using the same plaintexts. This gives an improvement of a factor of 7 on the number of favorable keys without an increase in work.

[2]If necessary, we may continue to eliminate the few remaining gaps in our knowledge of S_7 by analyzing a few of the wrong pairs where the characteristic held in the first seven cycles but failed in the last one.

j	F	j	F	j	F	j	F	j	F
0	0.076	3	0.060	6	0.044	9	0.027	12	0.011
1	0.071	4	0.055	7	0.038	10	0.022	13	0.005
2	0.065	5	0.049	8	0.033	11	0.016	14	0.000

Table 1: Fraction F of the keyspace where $\Gamma_{j+1} \to \Gamma_j$ holds

4 Linear cryptanalysis

FROG also is susceptible to linear cryptanalysis. The linear attacks are not as clean or elegant as the differential attacks, but they allow one to relax the chosen-plaintext assumption required by a differential attack.

Suppose that $a \to a$ with bias b_q by the S-box S_q, where the bias is defined as

$$b_q = 4\left|\Pr[S_q(x \cdot a) = x \cdot a] - 1/2\right|^2.$$

Take $\Gamma_0 = (a, 0, \ldots, 0)$ and let Γ_j be the result of rotating Γ_0 right j positions.

Then $\Gamma_{j+1} \to \Gamma_j$ (for $j = 1, \ldots, 15$) forms a useful one-cycle linear characteristic with bias b_q. It is expected to work on between 1/15 and 1/30 of the keyspace, with the exact fraction depending on j; see Table 1 for empirical results.

A useful linear characteristic for the last cycle is $\Gamma_1 \to \Gamma'$, where $\Gamma'_0 = a$, $\Gamma'_1 = c$, $\Gamma'_{\pi_7^{-1}(0)} = a$, $\Gamma'_{\pi_7^{-1}(1)} = c$, and Γ' is zero elsewhere. Suppose $a \to c$ with bias b_7 by S_7; then the characteristic $\Gamma_1 \to \Gamma'$ for the last cycle has bias b_7 and holds for about 21% of the keyspace (according to empirical tests).

We can combine these one-cycle characteristic to obtain a eight-cycle linear characteristic for the whole cipher of the form $\Gamma_8 \to \Gamma'$. It will hold for $0.038 \cdot 0.044 \cdot \ldots \cdot 0.071 \cdot 0.21 \approx 2^{-31.8}$ of the keyspace. For a single fixed value of a, c, the bias will be $b(a, c) = b_0 \cdot \ldots \cdot b_7$.

The technique of multiple linear approximations [6] may be applied with some success here. We sum over all values a and c; according to [6], the equivalent bias for the multiple linear approximation will be approximately $B = \sum_{a,c} b(a, c)$. The multiple linear approximation involves eight bits of key material, namely $K_{0,8} \oplus \ldots \oplus K_{7,1}$, so we will need to guess all possible values for those eight key bits. We will also need to guess $\pi_7^{-1}(0)$ and $\pi_7^{-1}(1)$ so that we know which form of Γ' to use. According to Matsui's rule of thumb, we expect to need about $N = 32/B$ known texts to have a good chance of success.

The number N of texts needed may be estimated empirically with probabilistic methods. In our experiments, we found that N has expected value $E[N] \approx 2^{54.4}$. The number of texts needed is often not too much more than the expected value, and quite frequently is substantially less: for instance, $\Pr[N \leq 2^{48}] \approx 2^{-7}$ and $\Pr[N \leq 2^{51}] \approx 0.12$, while $\Pr[N > 2^{57}] < 2^{-10}$.

The attack proceeds as follows. We obtain about 2^{56} known plaintexts. Using the technique of multiple linear approximations, we expect to recover $K_{0,8} \oplus \ldots \oplus X_{7,1}$ with very good probability if the key is favorable. (If the key is unfavorable, that will also be detected, and we may halt the attack at once.)

Next, we attempt to derive information about the S-box S_0 in a second phase of the attack. We repeat the following procedure for each of the 256 possible inputs x to S_0. Without loss of generality we set $K_{0,8} = 0$. To learn the S-box entry $S_0(x)$, we restrict our attention temporarily to those plaintexts P where $P_8 = x$, so that the input to S_0 is x in the eighth round of the first cycle[3]. We then guess $S_0(x)$ and use the linear characteristic $\Gamma_7 \rightarrow \Gamma'$ for the last seven cycles to verify our guess at $S_0(x)$. Based on our simulations, we expect that only about 2^{43} texts are needed to find $S_0(x)$; since $2^{56}/2^8 = 2^{48}$ known texts should be available for each x, the second phase of the attack should succeed with very good probability. At the end of the second phase, we expect to have recovered S_0.

With similar techniques (and a bit more work), we can recover the entries of the S-box S_7 used in the last cycle. At this point, it will be helpful that we derived the values of $\pi_7^{-1}(0)$ and $\pi_7^{-1}(1)$ earlier in the attack, since that will help us to identify the output of S_7 in the first and second rounds of the last cycle.

Once S_0 and S_7 are known, we may peel off the outer cycles and repeat the attack iteratively to recover the remainder of the key. In practice, peeling off the last cycle is expected to be easier, so that is what we recommend.

Summarizing, our linear attack uses about 2^{56} known plaintexts, and is expected to work for about $2^{-31.8}$ of the keyspace. The time complexity is expected to be small compared to the number of texts needed in the attack.

This linear attack is only the result of a preliminary investigation, and it may be possible to improve it significantly. For example, one simple avenue

[3]Actually, there is a complication. This can fail when $\pi_0^{-1}(8) < 8$, which occurs with probability 0.57. However, the failure will be detected, and we may try each of the eight possibilities for $\pi_0^{-1}(8)$ in this case. Then $P_8 \oplus P_{\pi_0^{-1}(8)} = x$ implies that the input to S_0 in round 8 is x (with good probability), so we may still separate out the plaintexts as needed. Of course, we only need to search for $\pi_0^{-1}(8)$ once, and then it will be known for all the other values of x, so this should not be a significant burden in practice.

for improvement is to repeat the attack with other linear characteristics, such as rotated versions of $\Gamma_8 \rightarrow \Gamma'$; it should be possible to break a somewhat larger class of weak keys in this way. Alternatively, one could reduce the number of known texts needed at the cost of some reduction in the number of favorable keys. As another example, we suspect that it may be fruitful to mount a systematic search for other linear approximations; the ones given here were the result of a limited search by hand.

5 A ciphertext-only attack

The linear attack can also be generalized to a ciphertext-only attack. In the ciphertext-only attack, we assume that the plaintext is formed of ASCII text, so that the high bit of each byte is always zero. This is expected to be a relatively realistic model in practice.

Only slight modifications to the linear attack are needed to work in this model. Instead of considering all of the 2^{16} linear characteristics that result from allowing a, c to take on all possible values, we now fix $a = 128 = \texttt{0x80}$, so that the mask Γ_8 applied to the plaintext selects the high bit from the byte in position 8. We expect the overall bias to decrease by a factor of 2^8, so that the number of texts needed increases to about 2^{64}.

The analysis phase requires only cosmetic changes. It will no longer be possible to recover all of S_0 in the same way; in particular, we can only learn the high bit of each S-box entry. However, since we still allow c to vary over all 255 possibilities, we do expect to be able to recover S_7 as before. In this way, we can repeat the attack iteratively until we have recovered the entire key.

In summary, the ciphertext-only attack is expected to require about 2^{64} known ciphertexts on average and comparable time complexity. The ciphertext-only attack is applicable not only to ECB mode, but also to some chaining modes, including CBC mode.

6 Decryption

We now turn to cryptanalysis of the decryption. FROG exhibits surprisingly poor diffusion behavior in the reverse direction. In other words, if we decrypt two ciphertexts which differ in only one byte position, it will often take many (48–64) rounds before full avalanche is achieved. In contrast, in the forward direction, avalanche is expected to be achieved relatively quickly (about 16–24 rounds).

Ciphers with an asymmetrical internal structure (e.g., unbalanced Feistel networks [9]) often require extra care to avoid this sort of pitfall. Several other recent ciphers contain special precautions to avoid weaknesses in the reverse direction. As a notable example, Skipjack [7, 10] alternates between one round structure (Rule A) and its inverse (Rule B) to avoid asymmetries between encryption and decryption. Additionally, the MARS submission [2] explicitly steers clear of this pitfall; the CAST-256 submission [1] also manages to avoid this pitfall[4]; and an early design considered by the Twofish team was rejected due to asymmetry concerns.

We present a variation on our differential attack that works on the decryption function of FROG. Observe that if $A \rightarrow B$ is a differential characteristic of function f with probability p, then $B \rightarrow A$ is a differential of f^{-1} with the same probability. (This is easily seen when looking at the set of all pairs of plaintexts and ciphertexts.) We will use 5 cycles of the differential used in section 2. This gives us the differential $\beta_0 \rightarrow \beta_5$ after 5 cycles. In the sixth cycle we assume that $\pi_5(6) = 5$. This gives us the 6-cycle differential of

$$\beta_0 \rightarrow (0, 0, 0, 0, 0, 0, X, a, 0, \ldots, 0)$$

where X represents an arbitrary value. We now hope for a favorable propagation through the last two cycles. This propagation depends only on the values of π_6 and π_7. To make the attack easy we look for cases where the input differential of S_7 in the first byte is always a. This is the very last S-box computation of the decryption. We also need to have some redundancy for filtering. Every output byte with a difference of 0 or a provides redundancy that is useful for filtering. We say that the pair (π_6, π_7) is favorable if it provides at least 6 bytes of redundancy and the input difference a to the last S_7 computation.

The fraction of favorable keys can be determined as follows. For the first 6 cycles we require $\pi_q(x) = x - 1$ for some x. This holds for $1/15^6$ of all keys. We ran empirical tests on the last two permutation choices. We generated 2^{20} pairs of (π_6, π_7) and found that 0.031 of all pairs were

[4] In fairness to FROG, it is not clear whether the designers of CAST-256 were aware of the danger either. The alternation of forward rounds and backward rounds is justified in [1] on the basis of implementation considerations: the symmetry allows hardware implementations to use the same engine for both encryption and decryption. The security implications of asymmetric round structures were not mentioned in the CAST-256 submission. In fact, a CAST-256 variant consisting of backward rounds and then forward rounds is less secure. And it is possible that the NSA chose a "four-pass" pattern of Rule A - Rule B - Rule A - Rule B to avoid an attack against the simpler "two-pass" Rule A - Rule B.

favorable. Together this implies that about $2^{-28.5}$ of the keys are favorable.

For a favorable key, the probability of getting a useful pair through the entire cipher is determined by the S-boxes. We need the differential $a \to a$ for the $S_0, \ldots, S_4$. For any a the probability of this differential having a positive probability for all these boxes is $(1 - e^{-1/2})^5 \approx 0.00943$. The chance of this happening for at least one a is over 90% (for simplicity we ignore this factor in our analysis). The expected number of a for which the approximation has a positive probability is more than 2. For such an a, the probability of the differential is at least $(2/256)^5 = 2^{-35}$.

The attack now works as follows. Using structures we generate suitable input differentials and filter the output differences using the redundancy. This requires about 2^{37} chosen ciphertexts to generate 2^{36} pairs for each value of a. As there are on average more than 2 suitable values for a we expect to find two right pairs for each such useful value of a.

Identifying the right pairs and thus the useful values of a is not difficult. We look for an output pair with at least 6 bytes that have difference 0 or a. For each useful value of a, two right pairs will have the same redundancy pattern. For a wrong value of a, we expect to see about $2^{36} \cdot \binom{16}{6} \cdot 2^6/2^{48} \approx 2^7$ wrong pairs; according to the following calculation, they should all fall into different redundancy patterns. By the birthday paradox, the chance of seeing two wrong pairs with the same redundancy pattern is $1 - \exp -2^{7.2}/(2 \cdot \binom{16}{6} \cdot 2^6) \approx 0.016$. Thus, over all 255 values of a, we expect about $255 \cdot 0.016 \approx 4$ wrong values of a (in addition to the two right values of a) which contain at least two pairs falling in the same redundancy pattern. Then the two right values of a can be recognized because they both induce the same redundancy pattern.

From these right pairs we learn a suitable value for a and the pattern of the redundancy. Unfortunately there is a single input difference we are now interested in, so we cannot use structures for the remaining of the attack. We generate 2^{42} more pairs using 2^{43} chosen inputs. Given the known output redundancy pattern these can be filtered very easily. This gives us about 256 output pairs where the input difference to the last S-box computation was the known value a. We recover S_7 in the same way as the earlier differential attack.

We conclude that the FROG decryption has an attack with $F = 2^{-28.5}$, $D = 2^{37}$ and $C = 2^{43}$. Thus an attacker can be expected to recover a key after about $2^{65.5}$ work.

There are some obvious extensions. Instead of $\beta_0 \to \beta_5$ we can start with any of the shifts that don't wrap around. Furthermore, we can use additional differentials for the first round. For example $(a, 0, a, 0, \ldots, 0) \to \beta_2$. The

further the input pattern shifts to the right the more differentials can be used for the first round.

We ran our analysis of the permutations in the last two rounds for each of the shifted versions. The overall result is that this attack can be made to work with more or less the same complexity against about 2^{-24} of all keys. We have not investigated the details of how attacks against multiple cases can be combined using a single input structure, but we expect that this will lead to an improvement of about an order of magnitude.

There are several more improvements that can be made to this attack. We can reduce the number of cycles for which we use the differential, and leave the last 3 cycles free of restrictions. There is a large enough fraction of the keys that produce the right kind of input difference to the last S-box computation, but the avalanche is strong enough to limit the very simple filtering rules that we use to all but a small fraction of the keys. Using 5 bytes for filtering, we get a differential with probability 2^{-28} for $2^{-29.3}$ of all keys. We now expect that there are about 6 values of a for which the differential $a \rightarrow a$ has a nonzero probability in the first four S-boxes. Thus, using $2^{27.4}$ ciphertexts we can generate $2^{26.4}$ pairs for each a. As we expect 6 suitable values of a we now have a good chance of finding two right pairs. The two right pairs are easily recognized, as they have the same redundancy pattern; in comparison, only about $2^{7.9}$ wrong pairs are expected, which by the birthday paradox stands only a 18% chance of generating any false alarms. This improves the attack to $D = 2^{27.4}$, $F = 2^{-29.3}$ and $C = 2^{36}$, which means that the attacker can expect to recover his first key after $2^{56.7}$ work. Again there are several similar differentials; together they cover about $2^{-26.6}$ of the keyspace.

A better filtering method, or a better way of solving for S_7 could improve the overall attack greatly. If we drop the requirement of having at least 5 filtering bytes, the fraction of useable keys goes up to $2^{-22.6}$ for the most likely position, and the whole family of differentials cover up to 2^{-18} of the keyspace.

Another interesting point to look at is the first decryption cycle; maybe there are other differentials that we can use. This could make our structures more efficient, and thus reduce the complexity of the attack.

7 Further work

We have not implemented any of our attacks. Practical demonstrations of all of our attacks can be give by applying the attack against keys that are

known to be favorable.

These attacks are the result of a preliminary analysis of FROG. A more thorough analysis will no doubt turn up better attacks.

8 Conclusions

As a result of a preliminary analysis of the FROG cipher, we have found several attacks that allow one to recover the key significantly more quickly than brute force, for a small portion of the keyspace. One of these attacks even works under a ciphertext-only model. This indicates that FROG has a significant problem with weak keys.

The internal diffusion structure of FROG is weak, especially in the decryption direction. One would probably have to double the number of rounds to eliminate the attacks described here.

Furthermore, the performance of FROG is significantly slower than many of the other AES contenders. One back-of-the-envelope estimate [12] suggests that FROG requires at least 48 clocks/byte (as a theoretical minimum) on a Pentium, and probably closer to about 70 clocks/byte in practice due to potential instruction pairing problems, for hand-tuned assembly-language implementations. This is faster than triple-DES (at about 120 clocks/byte), but much slower than some other modern ciphers such as Blowfish, Square, and RC5, which operate at 20–25 clocks/byte [5, 4, 11, 12]. Even DES (at 43 clocks/byte) is faster than FROG. Increasing the number of rounds by a factor of 2 to counteract our attacks would only widen the gap.

Finally, FROG seems ill-suited for smartcards, since it requires at least 2500 bytes of RAM for the keying material [3], as opposed to about a tenth of that for other AES submissions (e.g., Twofish [8]). Smart card suitability is likely to become extremely important for any general-purpose encryption algorithm.

In our opinion, this is enough to suggest that FROG is not a very strong candidate for the AES.

9 Acknowledgements

We are very grateful to Doug Whiting for his help with performance estimates. Of course, the authors are responsible for any errors in this document.

We would also like to thank Don Coppersmith for pointing out the importance of symmetry between encryption and decryption.

References

[1] C. Adams, "The CAST-256 Encryption Algorithm," AES submission, 1998.

[2] C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford, and N. Zunic, "MARS — A Candidate Cipher for AES," AES submission, 1998.

[3] D. Georgoudis, D. Leroux, and B.S. Chaves, "The 'FROG' Encryption Algorithm," AES submission, 1998.

[4] C. Hall, J. Kelsey, V. Rijmen, B. Schneier, and D. Wagner, "Cryptanalysis of SPEED," *Proceedings of SAC 98*, Springer-Verlag, to appear.

[5] C. Hall, J. Kelsey, B. Schneier, and D. Wagner, "Cryptanalysis of SPEED," *Financial Cryptography '98 Proceedings*, Springer-Verlag, 1998, to appear.

[6] B. Kaliski Jr., and M. Robshaw, "Linear Cryptanalysis Using Multiple Approximations," *Advances in Cryptology — CRYPTO '94 Proceedings*, Springer-Verlag, 1994, pp. 26–39.

[7] National Security Agency, "Skipjack and KEA algorithm specifications," May 1998. `http://csrc.ncsl.nist.gov/encryption/skipjack-1.pdf`

[8] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Fergusen, "Twofish: A 128-Bit Block Cipher," AES Submission, 1998.

[9] B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block Cipher Design," *Fast Software Encryption, 3rd International Workshop Proceedings*, Springer-Verlag, 1996, pp. 121–144.

[10] National Security Agency, "NSA Releases Fortezza Algorithms," Press Release, June 24, 1998. `http://csrc.ncsl.nist.gov/encryption/nsa-press.pdf`

[11] B. Schneier and D. Whiting, "Fast Software Encryption: Designing Encryption Algorithms for Optimal Speed on the Intel Pentium Processor," *Fast Software Encryption, 4th International Workshop Proceedings*, Springer-Verlag, 1997, pp. 242–259.

[12] D. Whiting, personal communications, July 30 1998.

EXHIBIT 8

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 IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** **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. State Defendants characterize Georgia's BMD-based election system as "an electronic voting system used throughout the country,"[1] and they remark that BMDs are used in "six of the ten largest counties in the country, including Los Angeles, California; Cook County/City of Chicago; Maricopa, Arizona; San Diego,

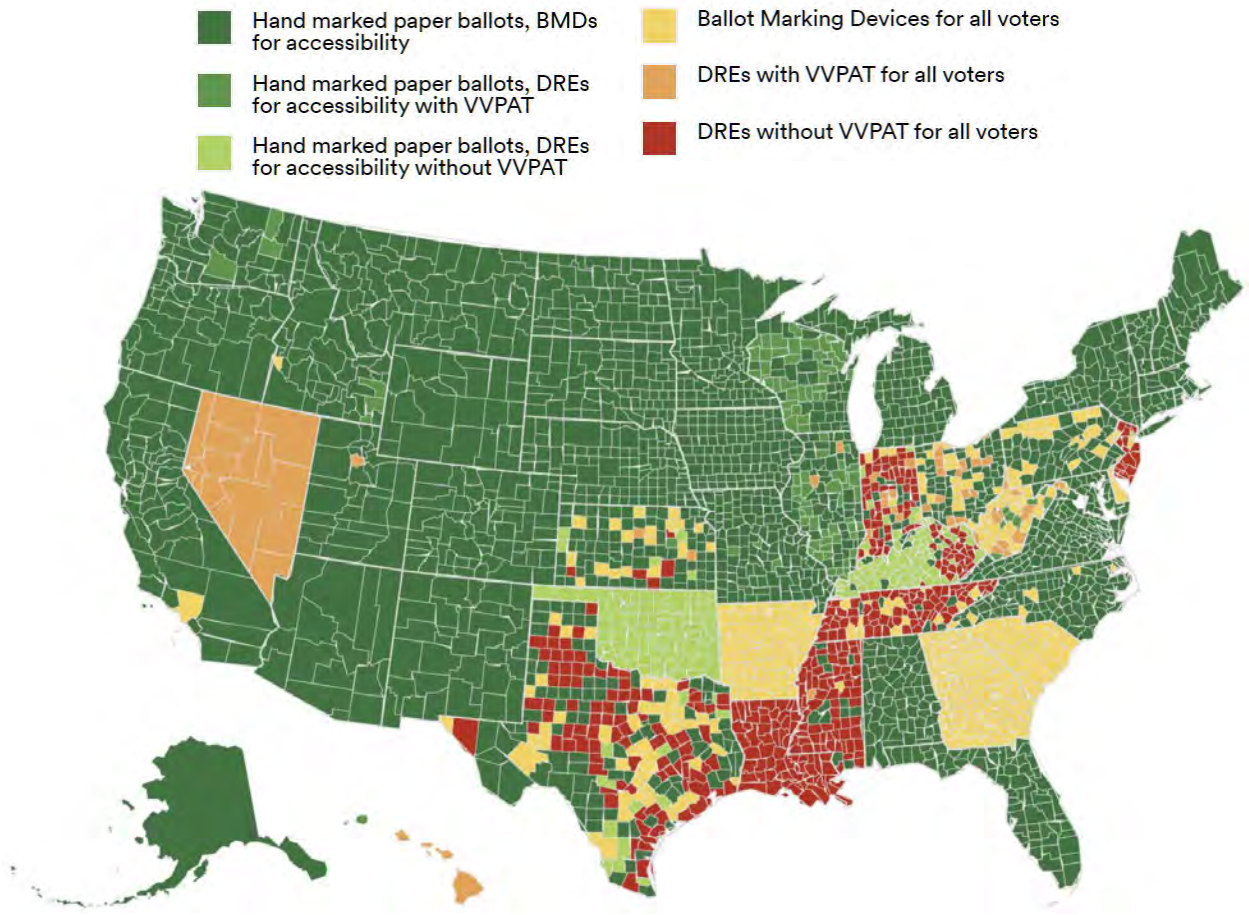
[1] State Defendants' Response in Opposition to Curling Plaintiffs' Fourth Motion for Preliminary Injunction, Dckt. 821 at 1.

California; Dallas, Texas; and Riverside, California."[2] These statements are misleading. The vast majority of jurisdictions that use BMDs use hand-marked paper ballots as the primary method of voting and reserve BMDs for accessibility purposes—including four of the six localities that State Defendants cite (all but Los Angeles and Dallas).[3] I explained in my previous declaration that BMDs are much safer when used by only a small fraction of voters, as in these localities.[4]

3. The map below shows the primary in-person voting technology that will be used in each U.S. county this November. The great majority of states, counties, and voters will use hand-marked paper ballots with BMDs available for accessibility (shown in dark green).

---

[2] *Id*. at 19.
[3] Verified Voting, *The Verifier*, https://verifiedvoting.org/verifier/ (accessed Aug. 30, 2020.)
[4] Decl. of J. Alex Halderman (Aug. 19, 2020), Dckt. 785-2 at 47-50.



Primary Polling-Place Equipment by County, November 2020

(Data/image: Verified Voting, *The Verifier*, https://verifiedvoting.org/verifier/.)

4. State Defendants further characterize Georgia's BMD-based election system as "a system recommended by the National Academy of Sciences and the U.S. [*sic*.] Intelligence Committee."[5] Again, this statement is misleading. Both the

[5] Dckt. 821 at 1.

National Academies[6] and the Senate Select Committee on Intelligence[7] recommended the use of voter-verified paper ballots, as opposed to paperless DREs or DREs with VVPAT printers. These recommendations were based on testimony heard in 2017 and 2018, including my own testimony to each body. At the time, only about 1% of voters lived in jurisdictions with BMDs as the primary method of voting, while nearly a quarter of voters used paperless DREs. Moreover, there had been little research about whether BMD ballots were accurately verified by voters. An election system like Georgia's, which uses barcode-based BMDs for nearly all in-person voters statewide, was not specifically addressed in either report.

---

[6] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy* (2018) at 80, available at http://nap.edu/25120. "Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner). […] Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible."

[7] U.S. Senate Select Committee on Intelligence, "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 1: Russian Efforts Against Election Infrastructure" (June 2019) at 59, available at https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf. "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."

5. The Academies' 2018 report also notes that "[w]ell designed, voter-marked [i.e., marked by hand] paper ballots are the standard for usability for voters without disabilities. Research on VVPATs has shown that they are not usable/reliable for verifying that the ballot of record accurately reflects the voter's intent, but there is limited research on the usability of BMDs for this purpose. […] Additional research on ballots produced by BMDs will be necessary to understand the effectiveness of such ballots."[8] It goes on to call on the National Science Foundation and other federal agencies to fund research to "determine voter practices regarding the verification of ballot marking device–generated ballots and the likelihood of voters, both with and without disabilities, will recognize errors or omissions."[9]

6. Last year, with National Science Foundation funding, my research group conducted an extensive study on this question, which I discuss at length in a previous declaration.[10] Our study was peer reviewed and published in January 2020 at the IEEE Symposium on Security and Privacy,[11] which is the most selective top-tier

---

[8] *Securing the Vote* at 79-80.
[9] *Id*. at 124.
[10] Decl. of J. Alex Halderman, Dckt. 682 (Dec. 16, 2019) at 25-33.
[11] 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 *Proceedings of the 41st IEEE Symposium on*

publication venue for computer security research. The work received special commendation from the review committee as the best research paper with a graduate student as the first author to appear in this year's symposium. The main findings of the study were that 60% of voters failed to review their ballots at all, and voters only reported 6.6% of misprinted ballots caused by a hacked BMD. We also tested a variety of procedural interventions, including those practiced in Georgia, to see how much they improved verification, but the magnitude of the improvements was likely too small to allow election officials to reliably detect BMD attacks in close races.

7. Other recent research, which State Defendants' and their expert Dr. Gilbert cite favorably,[12] actually confirms the key results from my study. It found that although voters *who do* review BMD printouts often are able to spot errors, few voters review the printouts at all, which is corroborated by field reports from polling place observers. These findings are further bolstered by previous research in the contexts of VVPATs and DRE review screens, which found that voters are also unlikely to catch errors when using those technologies.[13]

Security and Privacy (2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

[12] Dckt. 821 at 11, "there is other research indicating that voters can detect manipulation of ballots."

[13] This literature is summarized in Bernhard et al., § II.B.

8. On this basis, I find it misleading for State Defendants to say that "the science is not yet settled" regarding whether voters accurately verify BMD printouts.[14] Although science is always open to new evidence, there are now several studies that strongly support the proposition that the voter population does not verify BMD printouts accurately enough to allow reliable detection of misprinting attacks. To my knowledge, there is no research at all that suggests the contrary.

9. State defendants incorrectly ascribe my technical conclusions about the relative security of different voting technologies to mere personal preference.[15] This mistakes cause for effect. Like other security experts, I generally recommend hand-marked paper ballots over DRE and all-BMD systems *because* only a primarily hand-marked system can be strongly defended in practice using existing technology. My recommendations would change as appropriate if technological breakthroughs or compelling new scientific results were to alter the security analysis.

10. State Defendants misread my earlier testimony and erroneously conclude that I have changed my views about BMD auditability: "While Dr.

---

[14] Dckt. 821 at 11.

[15] *Id*. at 17. "Dr. Halderman's opinions are based on his personal beliefs that hand-marked paper ballots are a superior election system. He simply decided, as a policy matter, that the only acceptable election system is hand-marked paper ballots and reasons backward from that conclusion."

Halderman previously agreed that a sufficient audit of a BMD-generated ballot can 'detect and correct' the kinds of hypothetical hacking attacks about which he warns, [Doc. 619-2 at ¶¶ 6-7], he now says that no audit of any BMD system would ever be enough to satisfy him, [Doc. 785-2 at ¶ 51]."[16] There is no contradiction. Both declarations discuss two styles of attack: (1) changing both the barcode and the human-readable text and (2) changing only the barcode. Both declarations explain that the first kind of attack could not be detected by any kind of audit of the printouts, since all the records of the voter's intent would be fraudulent.[17] Both declarations also explain that the second kind of attack *could* be detected with a sufficiently rigorous audit that compared the contents of the barcode to the human-readable text,[18] but, to my knowledge, Georgia has no plans to conduct such an audit.

11. State Defendants falsely claim that "the evidence demonstrates that Georgia's new BMD system is completely separate from the DRE/GEMS systems, down to hand-entry from original source documents[.]"[19] To my knowledge, the only

---

[16] Dckt. 821 at 19.
[17] Dckt. 619-2 at 12; Dckt. 785-2 at 41.
[18] Dckt. 619-2 at 6-7; Dckt. 785-2 at 31-35. I was slightly imprecise in Dckt. 619-2 when I said that a sufficiently rigorous audit could "correct" a barcode-only attack in addition to detecting it. That is only the case if the auditors are somehow able to establish that the barcodes and not the human-readable text have been manipulated, but both would be suspect in the event that the BMDs had been hacked.
[19] Dckt. 821 at 8.

"evidence" for this claim appears to come from Mr. Coomer and Dr. Gilbert, but Dr. Gilbert never examined the Georgia system, and it is unclear what personal knowledge Mr. Coomer has, as there is no evidence he has conducted or participated in an examination of the Georgia system. In any event, neither could know what the workers with access to Georgia's technology are doing day to day, such as connecting USB devices to it that were connected to the prior system or connecting components to the Internet.

12. [redacted]

[20] [redacted]

[redacted]

13. While State Defendants are correct that the "Dominion system has been the subject of penetration testing" in other states,[24] they neglect to point out that this testing revealed a slate of serious vulnerabilities that likely remain unmitigated in the Dominion hardware and software used in Georgia. My previous declaration cites the results of penetration tests commissioned by the California Secretary of State, which found that attackers could modify the Dominion software installation files and "it would be possible to inject more lethal payloads into the installers", that the anti-virus software was insufficient or non-existent, and that the BMDs had

[21] Hamilton decl.
[22] The public facing portion of the ENR system is located at https://results.enr.clarityelections.com/GA/
[23] Dckt. 723 at 15 (Throop Decl.).
[24] Dckt. 821 at 10.

vulnerabilities that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider," among other problems.[25]

14. In the context of evidence that I discuss in my previous declarations regarding vulnerabilities in the Dominion equipment uncovered by certification testing in Texas,[26] State Defendants state incorrectly that the security problems "primarily relate to the optical scanners (ICP units), not the BMDs, which Curling Plaintiffs advocate the State continue using."[27] This is misleading. Both Texas and California found serious weaknesses impacting the BMDs, including the use of dangerously obsolete software and means by which the software could be manipulated by attackers. Both also found serious weaknesses impacting the scanners. Vulnerabilities in the BMDs are relevant to the relief that Plaintiffs' seek with respect to the use of hand-marked paper ballots, which are the only practical countermeasure to some BMD-based attacks. Vulnerabilities in the scanners are a threat to Georgia elections however the ballots are marked, and they are relevant to Plaintiffs' requested relief regarding rigorous auditing of the scanners' tallies.

---

[25] Dckt. 785-2 at 21-27.
[26] *Id*. at 19.
[27] Dckt. 821 at 8, fn. 7.

Status of Forensic Testing

15. Plaintiffs have asked me to update the Court about the status of the forensic analyses that I am performing on their behalf. My work is still in progress, but there are several preliminary findings I can report.

16. In December 2019, I received a copy of a forensic image created by the FBI of the server at the KSU Center for Election Systems.

17. In late July, I began a limited analysis of log files from approximately 4500 sequestered memory cards from Cobb, DeKalb, and Fulton counties to extract DRE serial numbers for statistical sampling. On August 13, 2020, shortly after the Court granted permission for a forensic examination of the memory cards, I began creating forensic images and have so far imaged around 25% of the cards.

18. On August 25, I received forensic images of the internal memory from six AccuVote-TS DREs from Athens-Clarke County. To facilitate imaging these machines, I created a software patch for the DREs' bootloader software, which a forensic technician programmed into a read-only memory chip and physically inserted into each DREs. On August 30, I received forensic images of three memory cards associated with those DREs.

19. To my knowledge, this is the first time that detailed forensic analysis of large parts of a state-wide DRE system has been conducted. Due to the scope and

complexity of the work, my analysis is necessarily still in an initial phase. I have had to developed specialized software and techniques to efficiently image and analyze the thousands of memory cards and the proprietary data formats of the DRE system.

20. The objective of my analysis is to determine the security posture of the DRE-based system as it was operated in Georgia. Although older and newer versions of the AccuVote DRE software have been shown to suffer from critical exploitable vulnerabilities, forensic analysis allows for direct confirmation that vulnerabilities were present in the specific hardware and software configuration Georgia used. The analysis also allows me to more fully assess what opportunities attackers would have had to spread malware through the Georgia system and manipulate election results.

21. As a secondary objective, the analysis may also uncover evidence that the election system was successfully compromised. However, one of the key deficiencies of paperless voting systems is that successful attacks might not leave forensic evidence, since well designed malware would remove the electronic records of its presence once its task was complete. Although there is a possibility that attackers were careless and did leave some digital traces, absence of evidence cannot support a strong conclusion that the system was not attacked.

22. Moreover, the digital records to which Plaintiffs have access are badly incomplete. Thus far, they have received memory cards from only three counties,

and most of these cards have records from only a single election. Only six DREs have been imaged, all from a single county. Log files from the CES server from before November 10, 2016 were erased prior to the server begin imaged by the FBI, severely limiting forensic visibility into the period of Russia's documented attacks against state election systems in the leadup to the 2016 election.[28] While these data sources provide abundant insight into how the DRE-based system was operated and ways in which it was vulnerable, finding a "smoking gun" proving that a Georgia election result was stolen by hackers is akin to finding the proverbial needle in a haystack, even assuming it occurred and left some trace in the data.

23. Nevertheless, there is evidence that hackers penetrated the system. My initial analysis of the CES server image has confirmed the principal findings that Logan Lamb described in his January 16, 2020 declaration.[29] The most important finding is that the CES server likely was compromised by an external attacker in December 2014. Mr. Lamb describes this evidence in detail.[30] Determining what actions the outside party took on the server is difficult, given the amount of time that elapsed before the server was imaged, but my analysis is ongoing.

---

[28] Suppl. Decl. of Logan Lamb, Dckt. 699-10 at 21-23.
[29] *Id*. at 11.
[30] *Id*. at 13-20.

24. Even if nothing more can be determined about the apparent attack, the evidence shows that the CES server was vulnerable to unauthorized access from the Internet for many years. Additionally, the FBI image shows that the CES server housed security-critical data, including installation files for the BallotStation software that ran on every DRE, the hash verification software that CES ran on its GEMS servers, and election databases. An outside attacker who infiltrated the server and compromised these files could have spread malicious software to the GEMS servers and DREs.

25. My initial analysis of the AccuVote-TS memory images confirms several severe vulnerabilities in the DREs themselves.

26. The bootloader software used in the DREs is version 1.0.2 and dates from June 2002. This software is critical to the DREs' security, since it runs every time they are powered on and controls sensitive operations such as loading the operating system and installing software updates. That it was not updated for 18 years demonstrates that Georgia's DRE systems were subject to an even wider range of vulnerabilities than had been previously established.

27. The version of the BallotStation election software installed on the DREs is 4.5.2!, which displays a 2004 copyright date. This confirms that the Georgia BallotStation software was not materially updated since that time.

28. The installed BallotStation software matches the contents of the installer file "BS_CE-TSR6-4-5-2!-DS.ins" found on CES's Internet-facing server. This is consistent with the assertion that copies of the software to be installed on the DREs were stored on the vulnerable CES server, where they could have been modified by an attacker. Although I have thus far been unable to determine whether the installation files on the server were modified by attackers, they had the opportunity to do so.

29. By analyzing the bootloader and BallotStation software, I have so far been able to confirm the presence of several critical vulnerabilities.

a) The vulnerability discovered by Harri Hursti in 2006 and described by Michael Shamos as "one of the most severe security flaws ever discovered in a voting system" is present in the DREs software that was used in Georgia until this year.

b) The vulnerabilities I exploited in a 2007 study to create vote-stealing malware that spreads from machine-to-machine as a computer virus[31] is present in the DREs software that was used in Georgia until this year.

---

[31] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine," in *Proc. USENIX/ACCURATE Electronic Voting Technology Workshop* (2007).

c) The vulnerability I exploited to demonstrate a vote-stealing attack to the Court in 2018 is present in the DREs software that was used in Georgia until this year.

30. All the memory cards and DREs I have analyzed use the same encryption key, `F2654hD4`. This is the default encryption key that was installed on the AccuVote DREs at the factory. It was publicly revealed by security researchers in 2003.[32]

31. Changing the encryption key to a different, secret value would have been straightforward for the state, but Georgia instead continued to use the manufacturer's default key for 17 years after that key was leaked to the public. Since the key was publicly known during that period, all confidentiality and integrity protections provided by the cryptography were completely negated. For instance, anyone with access to the memory cards could have read or modified any of the election data they contained.

32. The election log files from the county memory cards record that those cards were used in 1945 separate DREs in Cobb County, 1982 in DeKalb County,

---

[32] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, "Analysis of an Electronic Voting System," in *IEEE Symposium on Security and Privacy* (2004), § 4.4. Available at https://avirubin.com/vote.pdf.

and 2123 in Fulton County. Analysis of the logs shows that all three counties engaged in practices that would have facilitated spreading viral malware throughout their election systems.

a) County workers sometimes reused the same card in hundreds of machines for testing and training purposes. For example, in DeKalb, one memory card was sequentially inserted into at least 288 DREs. If any of those DREs was infected with viral malware, the malware could have spread to the other DREs during this operation by exploiting the confirmed vulnerabilities I discuss above.

b) In each of Fulton and Cobb counties, a single DRE was used to process data from more than a thousand different cards. If that DRE was infected with malware, it could have spread directly to over a thousand other DREs.

c) Each county used only a small number of DREs to program memory cards from the GEMS server. In Fulton, every election represented in the log files was prepared using one of only 17 machines; in Cobb, 28 machines; and in DeKalb, 28 machines. These DREs would provide a centralized point from which to launch an attack. If they were infected

with malware, the malware could have spread directly to all other DREs in the counties.

33. Despite the assertion that Georgia operated a uniform voting system across all counties, the three counties represented in my analysis had starkly different practices for maintaining their memory cards. This indicates that counties developed their own *ad hoc* processes for important security tasks. Some of these county-specific processes would have further facilitated the spread of malware.

d) Although Fulton and DeKalb counties appear to have erased their cards before each election, Cobb County did not, and some cards I examined contained election data from as long ago as 2004. This failure to erase the cards means that if they were infected, malware could continue to spread to new machines for many election cycles.

e) DeKalb County appears to have erased cards by overwriting them with the contents of other cards—most likely by using a machine designed for duplicating the cards. Around 8% of the DeKalb cards I have analyzed so far are identical to other DeKalb cards. This practice could rapidly spread malware if the cards used as a source for the duplication were infected.

34. The log files from the memory cards record hundreds of instances of technical malfunctions, including data corruption, software crashes, and machines freezing and needing to be restarted during voting. There also appear to be frequent instances of human error and procedural deviation, such as failing to correctly perform logic and accuracy testing.

35. These findings directly confirm the vulnerability of the DRE system and reveal additional ways that malware could have spread through it, beyond those already in evidence. Since my analysis is still in an early stage, it is likely that additional problems will be uncovered as the work proceeds.

Rebuttal of Declaration of Jack Cobb[33]

36. Mr. Cobb gives only a partial history of certification tests that apply to Georgia's Dominion equipment.[34] His company, Pro V&V, appears never to have performed penetration testing on the Dominion equipment nor any security testing on the version of the Dominion system used in Georgia (5.5A). Although he states that his company performed certification tests for the U.S. Election Assistance Commission ("EAC") for version 5.5 of the software, EAC certification testing

[33] Decl. of Jack Cobb (Aug. 25, 2020), Dckt. 821-6.
[34] *Id*. at 5.

involves only limited security evaluation and not penetration testing. I find it interesting that Mr. Cobb points to security tests performed by another company, SLI Compliance, as part of certification testing for Pennsylvania, but that he neglects to point to later tests performed by the same company for California, which found a number of serious vulnerabilities.[35] I discuss these vulnerabilities and their impact in my previous declaration.[36] I also find it interesting that despite the fact that Pro V&V had never performed penetration testing of the Dominion system, the Secretary of State hired Pro V&V to perform certification tests for the State of Georgia.[37]

37. In reference to my August 19, 2020, declaration, Mr. Cobb opines that I "clearly [do] not understand the specific setup and nature of the Dominion system or its security features."[38] His first example concerns the QR codes (barcodes) printed on the BMD ballots. Based on his company's role in certifying the Dominion system for the EAC and the State of Georgia, I would expect Mr. Cobb to have a detailed technical understanding of these barcodes, which are central to the security

---

[35] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019) at 29, https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.
[36] Decl. of J. Alex Halderman (Aug. 19, 2020), Dckt. 785-2 at 21-27.
[37] Cobb decl. at 6.
[38] *Id*. at 9.

of votes cast using Dominion BMDs. Indeed, Mr. Cobb states that during the limited testing that his company conducted for the Secretary of State, "Pro V&V also verified the contents of the QR code which includes a digital signature and is encrypted."[39] He later states that, "In this system, the election files, including the QR codes, are digitally signed and encrypted."[40]

38. These technical claims about the Dominion QR codes used in Georgia are entirely wrong. Based on my own analysis of the QR codes from ballot images provided by Fayette County during discovery, which I understand to be scans of ballots cast during the June 9, 2020 election, no portion of the QR codes is encrypted.[41] I am prepared to demonstrate that the contents can be read and understood without the use of a secret key, thus proving they are not encrypted.

39. Moreover, Dominion QR codes do not include a digital signature, but rather what is known as a message authentication code ("MAC"). A MAC provides

---

[39] *Id*. at 6.
[40] *Id*. at 9.
[41] In my previous declaration, I myself incorrectly described the QR codes as "encrypted" (Dckt. 785-2 at 7(a), 32). My understanding at the time, before I had received a Georgia BMD ballot with which to conduct my own tests, was based on the California Secretary of State's test report. California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019): "The QR code is encrypted" (p. 14); "The ICX ballot marking device uses an encrypted QR code" (p. 28).

somewhat similar protections to a digital signature but is weaker in important aspects. The distinction between digital signatures and MACs is an elem-entary concept that I regularly test students about in introductory security classes.

40. Mr. Cobb's errors about these basic facts regarding the Dominion system and its security are troubling. They lead me to believe either that Mr. Cobb does not understand the specific setup and nature of the Dominion system or its security features, that he is not telling the truth when he states that his laboratory "verified the contents of the QR code" while testing the system for Georgia, or that Pro V&V's tests of critical aspects of the system were poorly conducted.

41. Mr. Cobb goes on to imply that the Dominion voting system software cannot be altered by attackers without detection, because the BMDs have "a built-in feature that will generate a SHA-256 hash value at any point before and during voting to allow for easy checks to determine if it matches with Georgia's version."[42] This view again reflects a misunderstanding of fundamental security concepts, such as what hash values are and how they can be used to verify the integrity of software.

42. In the security field, a hash value is a number that is calculated based on the contents of a file by applying an algorithm that is designed so that it is

[42] Cobb decl. at 7.

extremely difficult for an attacker to generate another file with different content that yields the same hash value. Given two files, I can apply a hash algorithm to compute the hash value of each file, and if the hash values are identical, I can conclude that the files' contents are also identical.

43. The scenario Mr. Cobb describes is completely different. Instead of Mr. Cobb calculating the hash values of the files on the BMD, he describes a scenario where the software on the BMD calculates *its own* hash value, which is then compared to the hash value of the software that is supposed to be installed—in essence, asking the BMD itself whether it is malicious. This is akin to a bouncer asking bar patrons to card themselves. If the BMD *has* been attacked and is running malicious software, that software can simply lie about its hash value.

44. Hash values are not trustworthy if the system used to compute and display them is compromised. In this case, the software running on the BMD is computing and displaying its own hash. If the software has been compromised because the machine has been infected with malware, the compromised software could display whatever hash the attacker has programmed—including the hash of the uncompromised software. This mechanism may have utility for administrative compliance (e.g., checking which version of the software is supposedly installed), but it has little or no value for deterring attacks.

45. Mr. Cobb also says his firm helped Georgia "perform acceptance testing of each BMD using a hash value. This ensured that the BMD had not been altered and had the correct software installed at the time it was accepted by the State."[43] Here, acceptance testing refers to checking the hash of the software on the machine at the time it is delivered from the manufacturer. Mr. Cobb does not specify the procedure he used to conduct these tests, but verifying the integrity of software running on an embedded device such as the ICX BMD is difficult to do securely. If there is already malware on the device, that malware can conceal its presence from other software using what is known as a rootkit. Therefore, computing hash values on the device itself is not a reliable method of acceptance testing. Nor can one simply remove the storage medium and hash it using a trusted computer, since the flash storage chips in the ICX are permanently integrated into the circuitry. In any event, Mr. Cobb only describes checking the integrity of the BMD software when the BMDs were first delivered, so this testing could not prevent the software from being altered later by attackers. Nor could it detect any subsequent attack.

46. Mr. Cobb also mistakenly concludes that "[i]f a QR code was somehow manipulated on the BMD (which I have never seen occur in any context using the

---

[43] *Id*. at 8.

Dominion system), the digital signature would also be altered and it would not be accepted by the scanner." Again, the QR codes do not contain a digital signature, but rather a MAC. Even then, the data protected by the MAC is the same in every ballot that has the same votes. This means, for example, that an attacker can simply duplicate the QR code from a ballot with votes he favors in order to produce another ballot with those same votes that will be accepted and counted by the scanner. This is an important security flaw that Pro V&V should have been aware of after reviewing the contents of the QR codes. Dominion could have designed the QR codes in a way that would have allowed the scanners to detect and prevent such duplication, but did not do so.

47. Mr. Cobb goes on to imply that malware cannot be spread to scanners or BMDs from the election management system ("EMS"), because "the election files, including the QR codes, are digitally signed and encrypted," and if the digital signatures do not match, "decryption fails and nothing is loaded on the machine."[44] Once again, this assertion is technically nonsensical, even aside from the fact that the QR codes are neither signed nor encrypted. Although the ballot programming that workers copy to the BMDs and scanners from the EMS may be encrypted and

[44] *Id*. at 10.

signed, this has no relevance to whether malware can spread from the EMS as part of those files. The EMS *generates* the ballot programming files. Therefore, malware running on the EMS could arbitrarily alter their contents before the encryption and signatures are applied, ensuring that the BMDs would accept the files as genuine.

48. In a similar vein, Mr. Cobb asserts that, "If a QR code was somehow manipulated on the BMD […], the digital signature would also be altered and it would not be accepted by the scanner."[45] This is, again, nonsense. First, the QR code contains a MAC rather than a digital signature. A MAC is a number that works similarly to a hash, except that its value can only be computed with knowledge of a secret key. Each QR code contains a MAC of the vote data that is computed using a secret key that is shared by the BMD and the scanner. The scanner reads the QR code, extracts the vote data and MAC, and uses the secret key to compute the correct MAC of the vote data. If the MAC from the QR code is different from the computed MAC, the scanner should reject the ballot.

49. This implies that in order to print *any* ballots that the scanner will accept, the software on the BMD must have access to the secret key. Therefore, if the BMD is infected with malware that modifies the operation of the software, the

[45] *Id*. at 11.

malware too will have access to the secret key, and will be able to generate QR codes that the scanner will accept as valid for whatever ballot choices the attacker prefers.

Rebuttal of Declarations of Juan E. Gilbert

50. State Defendants have refiled a declaration from Dr. Juan E. Gilbert November 13, 2019.[46] I respond to Dr. Gilbert's assertions in my declaration of December 16, 2019.[47]

51. In a brief supplemental declaration, Dr. Gilbert makes several additional statements that require clarification.[48]

52. Dr. Gilbert correctly notes new SEB rules require poll workers to verbally instruct voters to review their ballots.[49] As Dr. Gilbert points out, my own peer-reviewed research measured the effect of such instructions on verification and error detection rates and found them to have a small positive effect. However, even with such instructions, voters failed to detect about 86% of errors on BMD printouts (vs. 93% without instructions). As my study explains, voters would have to verify

[46] Decl. of Juan E. Gilbert, Dckt. 821-2, originally 658-3.
[47] Decl. of J. Alex Halderman (Dec. 19, 2019), Dckt. 682 at 16, 38-49.
[48] Supp. Decl. of Juan E. Gilbert, Dckt. 821-7.
[49] *Id*. at 7(A).

their ballots much more carefully than that in order to reliably detect outcome-changing fraud in close elections.

53. Dr. Gilbert also notes that SEB rules require reminding voters that a sample ballot is available to help with verification. My study suggests that voters who use a sample ballot do detect errors more reliably. However, the gain will be limited to the fraction of voters who can be induced to use a sample ballot. I am not aware of any research that shows verbal reminders are effective in this regard, and I would be surprised if they were.

54. Dr. Gilbert highlights a new SEB rule that holds that if, in any recount or audit, "a discrepancy is found between the voter's choice indicated by the printed text on the ballot and the result tabulated by the ballot scanner, the printed text shall control and be counted."[50] However, this rule does not provide an effective defense against BMD misprinting attacks. An attacker could cause a BMD to alter both the barcodes read by the scanners and the human readable text, in which case there would be no disagreement. And if there were a discrepancy between the barcodes and the human-readable ballot text, the reliably of both records would be in doubt, because either might have been altered.

---

[50] *Id*. at 7(B).

55. Dr. Gilbert cites a recent study by Byrne and Whitmore, which I also cite in my previous declaration.[51] Byrne and Whitemore's results are generally in agreement with my own BMD research (although, unlike my study, theirs has not been peer reviewed). Both studies find that few voters are likely to spot errors on BMD printouts. Of 108 participants who voted on a hacked BMD, Byrne and Whitemore report that only 17.5% detected alterations to the printout. This average includes both voters who were heavily primed to review their ballots through repeated verbal and written instructions and voters who were not. Unsurprisingly, the study finds that verification performance is much better among voters who actually examine their ballots, but the fact remains that only 23% of their subjects did so. This is further evidence that voters do not reliably detect errors on BMD printouts.

56. Dr. Gilbert questions why I "make no mention of interventions which foster higher review rates."[52] As I have discussed, the magnitude of the improvements that have been measured by these studies for practical kinds of interventions are simply too small to reliably uncover cheating in close elections.

---

[51] *Id*. at 8-11.
[52] *Id*. at 11 and 13.

57. Dr. Gilbert's assertion that barcode manipulation attacks could occur with hand-marked paper ballots defies common sense.[53] Although timing marks or the placement of vote targets could be manipulated, this kind of problem would be detected during routine logic and accuracy testing. Election workers would simply need to perform L&A testing with one ballot and flip through the remaining stack of blank ballots to verify that they are all the same.

58. Dr. Gilbert argues that BMD barcode manipulation attacks are "an unlikely avenue for a bad actor since, as other scholars have recently noted, such an attack is unlikely to go undetected in a jurisdiction conducting RLAs[.]"[54] The only scholar Dr. Gilbert cites for this proposition is Dr. Dan Wallach, who, like Dr. Gilbert, is the creator of a BMD system that use barcodes. The proposition is incorrect. While it is true that "an audit which recognizes a single inconsistent barcode/text combination would signal a significant problem", in order to find even a single inconsistency, the audit would have to sample at least one manipulated ballot *and* actually compare the barcode to the text. Georgia has announced no plans to inspect the barcodes during its intended audits. Even if it did, the proposed Georgia RLA is designed to target only a single race to be selected by the SOS every two

[53] *Id*. at 12.
[54] *Id*. at 12.

years. There is no assurance that it will select enough ballots to uncover barcode-based cheating in races that are not targeted. For instance, if the Democratic Presidential Preference Primary had been selected for audit statewide (as it was in Fulton county), the probability that the audit would have detected barcode-based fraud sufficient to change the outcome of another state-wide race with a 1% margin of victory would be only around 30%, and that's under the counterfactual assumption that the auditors decoded the barcodes. In elections where no RLA was conducted (as in every election but the November general election in even years), the probability would be 0%.

59. Contrary to Dr. Gilbert's repeated implications, the issue is not whether interventions can improve voter verification rates *at all*, but whether they can ensure that *sufficiently many* voters carefully review their ballots.[55] The effectiveness of verification for detecting attacks increases dramatically only when the rate of verification is high. When the rate is low, as appears to be the case based on a growing number of studies, small increases (like those my study found were achieved by instructing voters to verify their ballots) have little utility.

[55] *Id*. at 13.

60. Moreover, the security of Georgia's voting system depends on whether voters are likely to spot errors when using the actual BMDs operated by the state—not theoretical future BMDs with transparent screens like those conceived by Dr. Gilbert or hypothetical interventions that somehow raise voters' verification performance well beyond the levels measured thus far. In fact, that Dr. Gilbert sees a need for such BMDs seems to indicate that he recognizes the unreliability of the ballots generated by the BMDs used in Georgia, lest there would be no need for transparent screens.

61. Dr. Gilbert and I agree that scanners can be hacked and that rigorous RLAs are necessary.[56] However, he fails to acknowledge that BMDs, particularly when they are used as the primary method of voting, as in Georgia, create a second place, in addition to the scanners, where outcome-changing attacks could succeed, multiplying the opportunities for attackers. In the absence of rigorous audits of a kind not now contemplated in Georgia, barcodes greatly magnify this risk. Dr. Gilbert does not seem to seriously dispute either claim.

---

[56] *Id.* at 14.

Rebuttal of Declaration of Mark Riccobono

62. State Defendants have refiled a declaration from Mark Riccobono, president of the National Federation of the Blind, dated August 1, 2019.[57] I respond to Mr. Riccobono's assertions in my declaration of December 16, 2019.[58]

Remarks on Declaration of David Hamilton[59]

63. [redacted]

64. [redacted]

[57] Decl. of Mark Riccobono, Dckt. 821-8, originally 658-4.
[58] Decl. of J. Alex Halderman (Dec. 19, 2019), Dckt. 682 at 34-37.
[59] [redacted]
[60] [redacted]
[61] [redacted]

65. [redacted]

66. [redacted]

67. [redacted]

---

[62] [redacted]

[63] [redacted]

[redacted]

68. [redacted]

[redacted]

---

[64] As the Court noted, the "assessment of the eNet voter registration systems and database rang serious alarm bells." Dckt. 579 at 76.
[65] Dckt. 579 footnote at 74. "On July 1, 2019 the SOS took over hosting eNet's voter registration database that creates the express pollbooks, but continued its

[redacted]

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 1st day of September, 2020 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

contract with PCC for licensed use of the PCC software and for PCC's maintenance and support of the PCC application."

[66] [redacted]

[67] [redacted]

EXHIBIT 9

US 20030208527A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2003/0208527 A1

Lglesais et al. (43) Pub. Date: Nov. 6, 2003

(54) METHOD FOR SMART DEVICE NETWORK APPLICATION INFRASTRUCTURE (SDNA)

(76) Inventors: **Lino Lglesais**, Caracas (VE); **Roger Pinate**, Caracas (VE); **Antonio Mugica**, Boca Raton, FL (US); **Paul Babic**, Caracas (VE); **Jeffrey Neveda**, Edo Miranda (VE); **Dany Farina**, Caracas (VE); **Rodrigo Meneses**, Caracas (VE); **Salvador Ponticelli**, Caracas (VE); **Gisela Goncalves**, Caracas (VE); **Yrem Caruso**, Caracas (VE)

Correspondence Address:
JEFFREY FURR
253 N. MAIN STREET
JOHNSTOWN, OH 43031 (US)

(21) Appl. No.: **09/682,103**

(22) Filed: **Jul. 20, 2001**

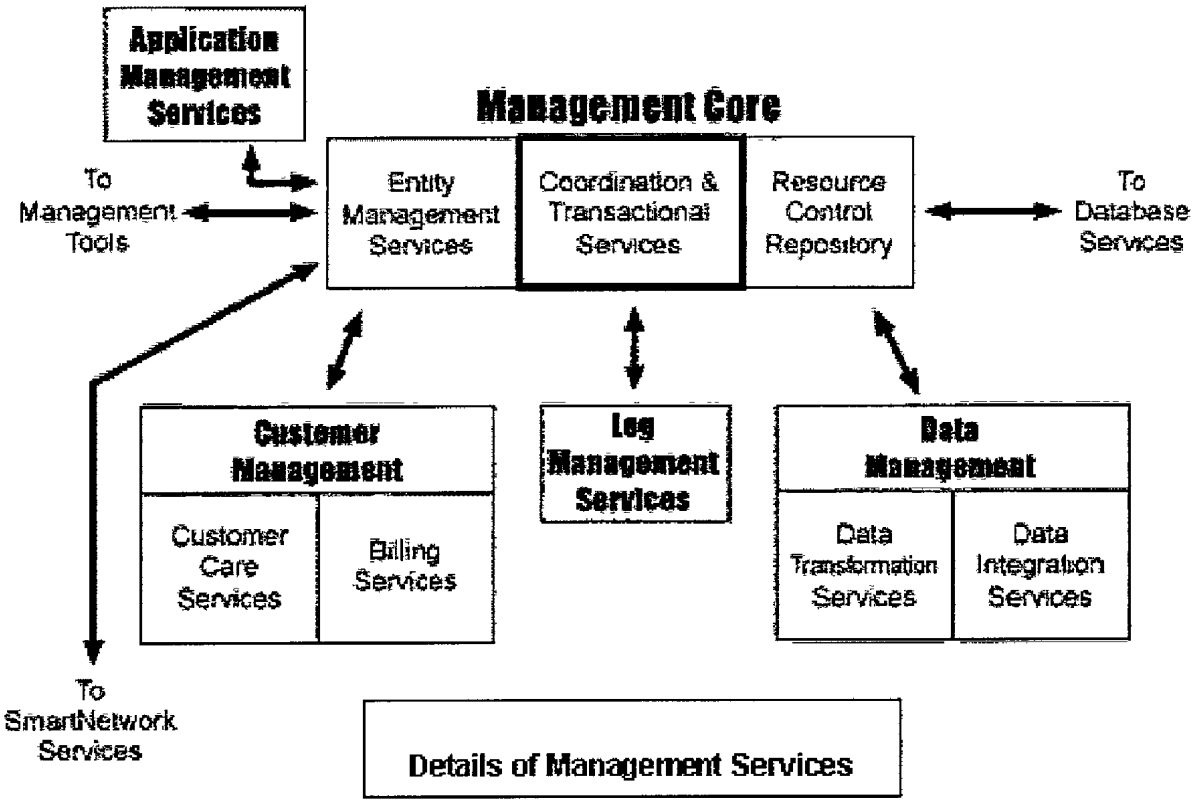
Publication Classification

(51) **Int. Cl.**[7] **G06F 15/16**

(52) **U.S. Cl.** **709/203**; 709/250

(57) **ABSTRACT**

The present invention discloses a novel method to implement a Smart Device Network Application Infrastructure (SDNA) that supports and facilitates the development, deployment and management of device networks and device network applications. The Smart Device Network Application infrastructure (SDNA) refers to an integrated processing platform that supports and facilitates the development, deployment and management of distributed applications based on device networks. It involves the concurrent execution of several processes that interact to provide support and resources for said applications.



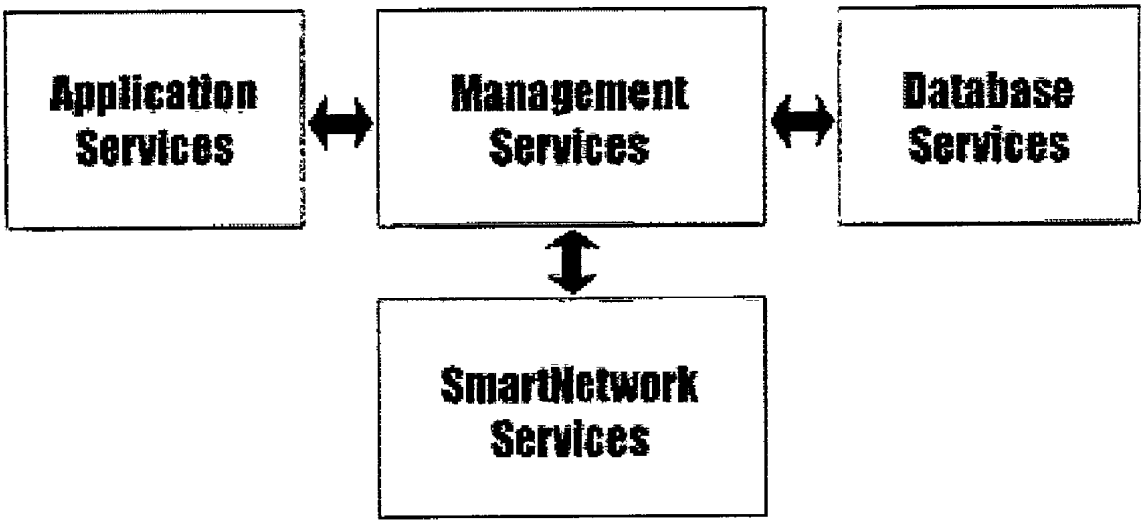


Fig 1
Condensed View of Architecture

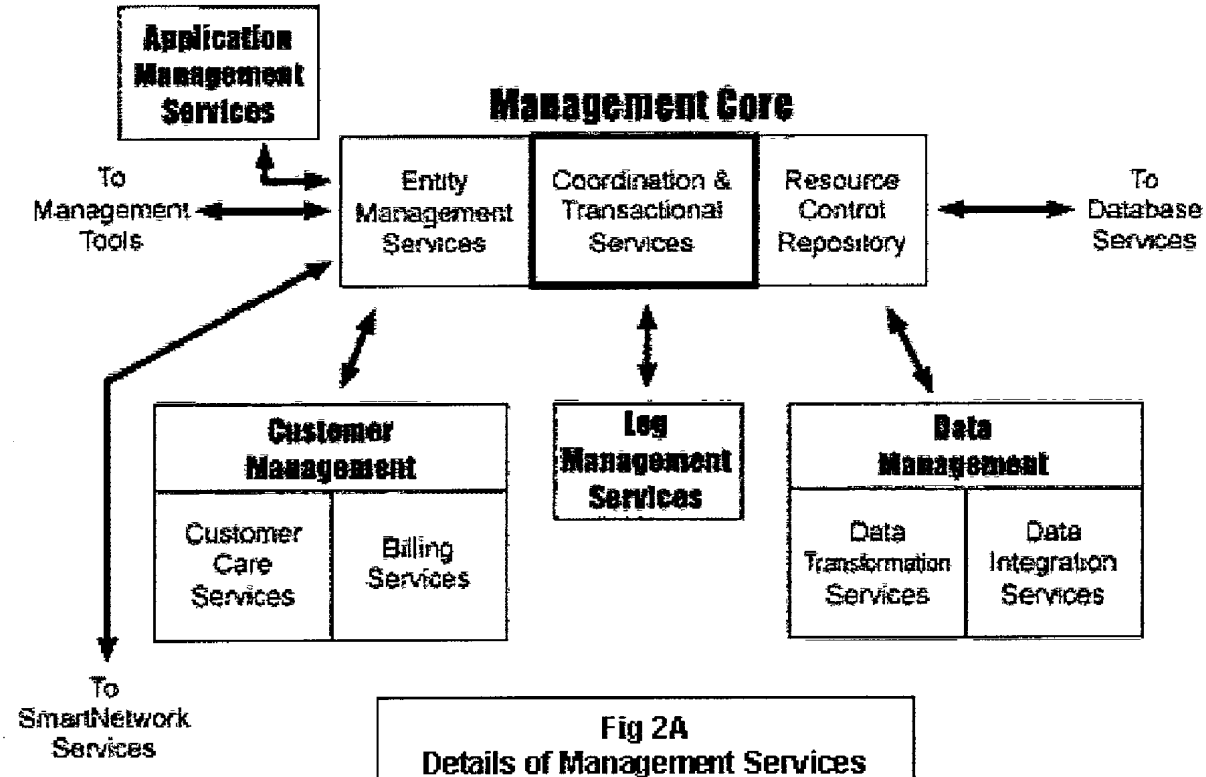


Fig 2A
Details of Management Services

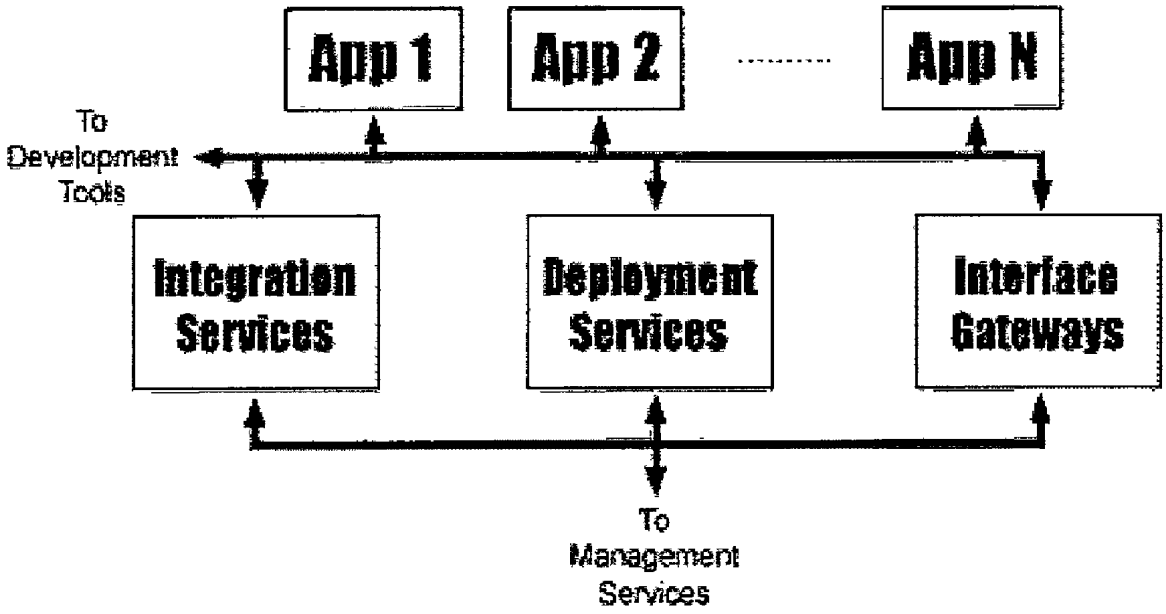


Fig 2B
Details of Application Services

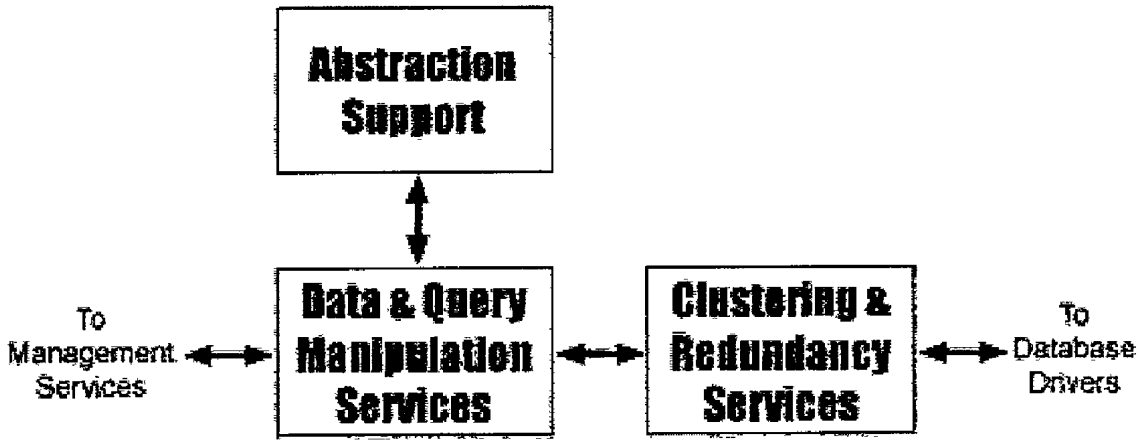


Fig 2C
Details of Database Services

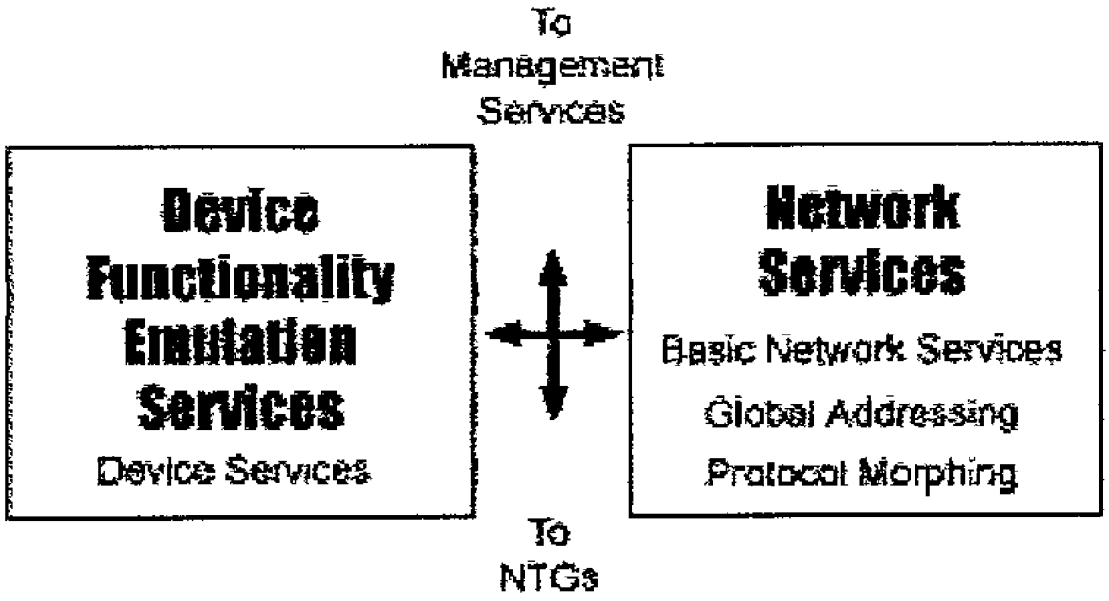


Fig 2D
Details of Smart Network Services

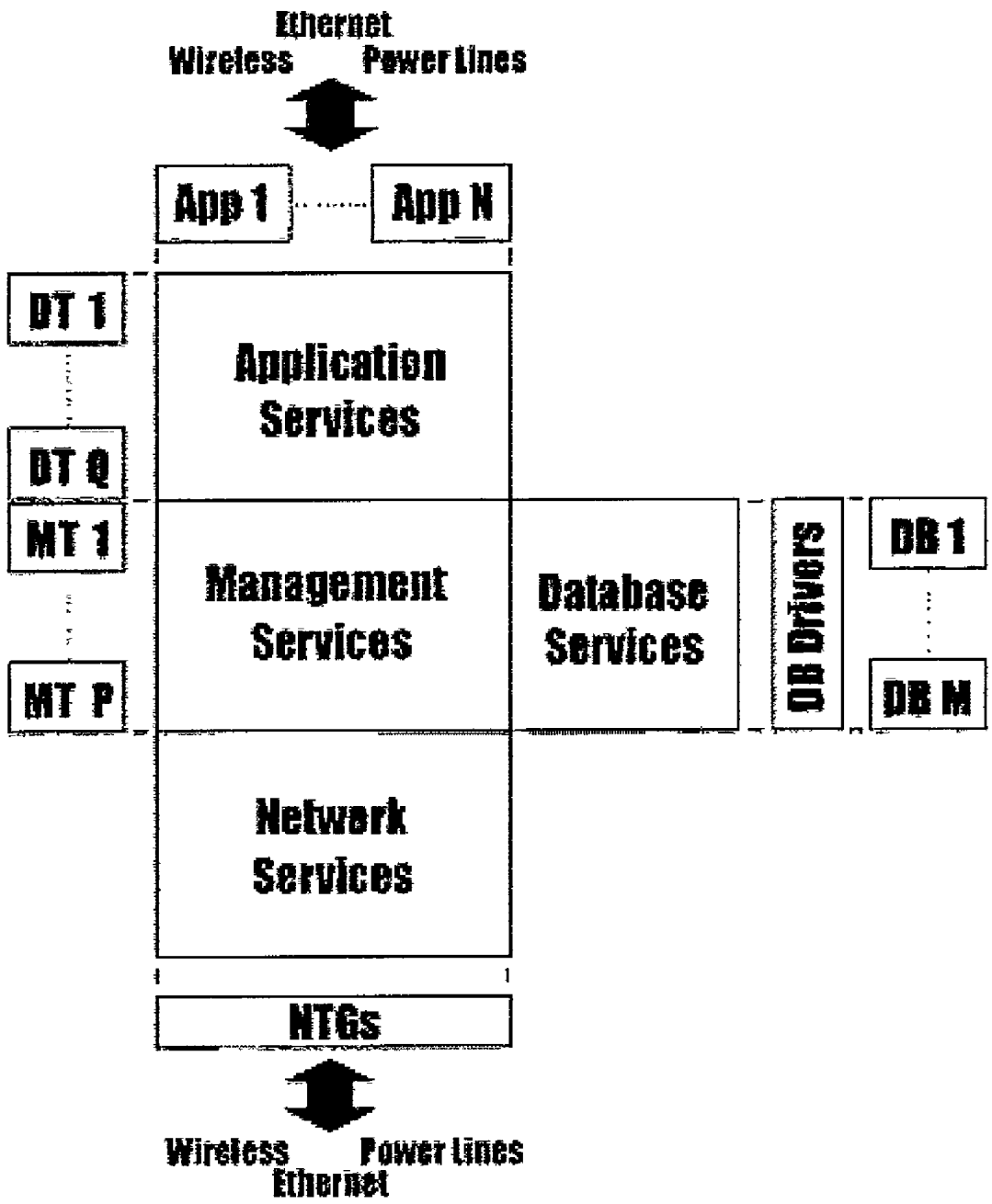


Fig 3
Detailed View of Architecture

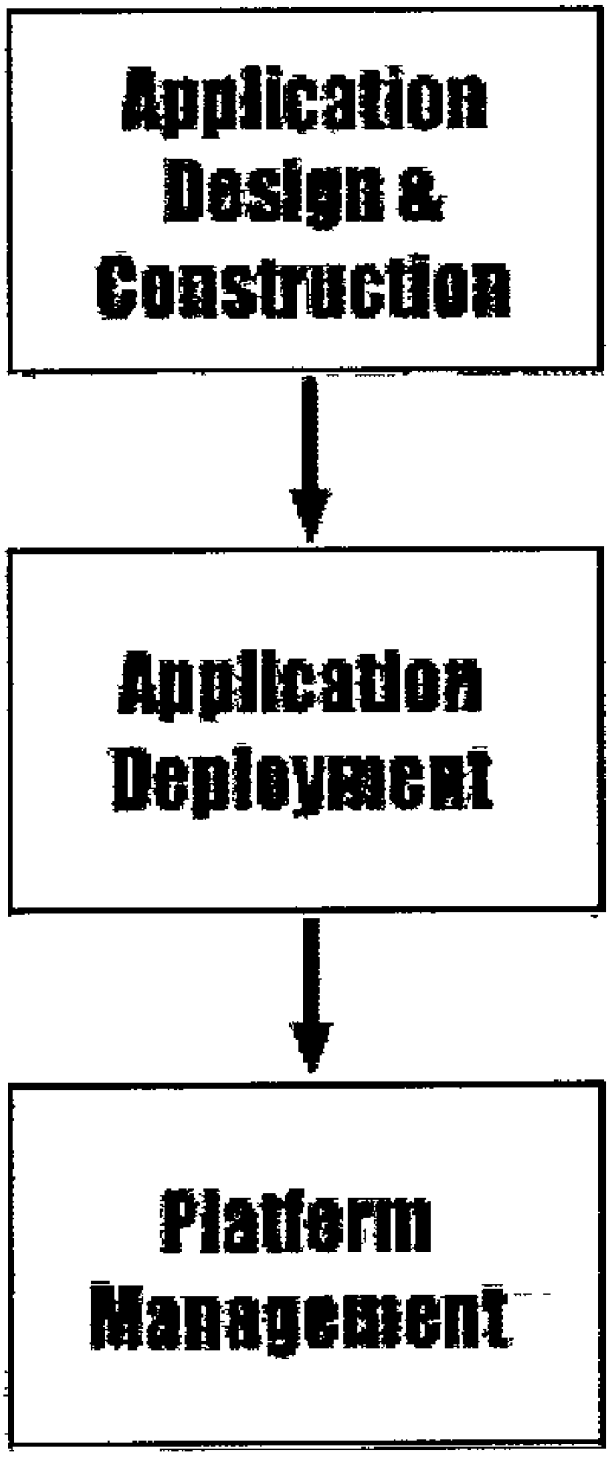


Fig 4
Overview of Operation

METHOD FOR SMART DEVICE NETWORK APPLICATION INFRASTRUCTURE (SDNA)

BACKGROUND RELATED APPLICATIONS

[0001] The present invention uses the concepts of True Distributed Control, Global Addressing and Protocol Morphing of our co-pending U.S. patent applications. Also, the term "device group" refers to the term "device tissue or organ" as used in our co-pending Single-Cell Control U.S. patent application.

BACKGROUND OF INVENTION

[0002] 1. Background Field of Invention

[0003] This invention relates to device network applications, specifically to an infrastructure platform that supports development, deployment and management of network applications based on smart devices.

[0004] 2. Background Discussion of Prior Art

[0005] The Cambridge Dictionary of American English defines a "device" to be an object or machine invented to fulfill a particular purpose. In technical literature, several types and definitions of devices are mentioned. The following are our definitions as used in the present disclosure.

[0006] In the present disclosure, the term "device" specifically refers to a unit comprising a combination of software and/or hardware that possesses configurable attributes and parameters that may uniquely identify and distinguish it from other units. The set of configurable attributes and parameters includes a program or application, which describes the operation of the device under all functional circumstances.

[0007] Depending on the application, a device may be as simple as a controller that opens an electric door when someone approaches it, or as complex as a composite controller that executes sensitive measurements within a petrochemical industrial process.

[0008] There are several types of devices, depending on their characteristics and operation:

[0009] Dumb device: refers to devices that lack intrinsic intelligence and cannot communicate with other devices. Dumb devices include conventional household appliances, electric lights, among others.

[0010] Intelligent Device: refers to devices that possess inherent intelligence, i.e., devices that have some processing power and are capable of performing logic functions. Typical intelligent devices include programmable microwave ovens, ABS brakes and traffic lights, among others.

[0011] Communication-enabled device: refers to devices capable of transmitting information over a simple communication medium, such as a serial port. Communication-enabled devices include controllers in master/slave control architectures, Ademco IR detectors, etc.

[0012] Network-enabled device: refers to devices fully capable of communicating with other devices across a network, such as personal computers. These

[0013] Smart device: refers to a device that is at once intelligent and network-enabled.

[0014] Beyond defining a device, other definitions are relevant to this disclosure, including those of device networks and device network applications.

[0015] The term "device network" refers to a collection of devices interconnected in a networking fashion in which they can communicate with one another to share information and resources. A device network is the underlying physical structure that supports a device network application, and its complexity, in general, depends on the complexity of the implemented application. A device network, if appropriately designed as per the present invention, can support execution of multiple concurrent applications, or execution of multiple instances of the same application. The term "device network" differs from the term "device group". The term "device group" refers to the method of uniting several devices into a logical group called device "tissue" or "organ", as described in the method of single-cell control.

[0016] The term "device network application" refers to a balanced combination of a software application and an underlying device network infrastructure. In a device network application, a software application makes use of a physical device network to accomplish an overall task. Some applications may involve interaction with an end-user, while some may not involve human interaction at all.

[0017] A home automation system illustrates a simple example of a device network application. It comprises a set of devices interconnected to form a device network (e.g., electric doors, electric lights, motion detectors, air conditioners, temperature sensors, garage door opener, cloth washer and drier, microwave oven, and others). A home automation application controls all these devices to perform according to a set plan. For instance, a siren is activated when an alarmed electric door is opened, electric lights are automatically switched on when you walk into a room, or the garage door opens automatically as your car approaches it.

[0018] A home automation system involves interaction with a user (i.e., end-user), who can perform device activations (e.g., turn lights on/off) or can perform system configuration.

[0019] In recent years, there have been many efforts invested to develop smart device technology. The results, however, have been limited to many specific technologies that produce intelligent devices and network-ready devices (specially Internet-ready). Yet, no efforts have been put towards creating a universal infrastructure that can at once support and facilitate development, deployment and management of smart device networks and smart device network applications.

[0020] Consequently, the present invention stands alone in its field as it fills an important void left by all other previous smart device-related inventions.

SUMMARY OF INVENTION

[0021] The present invention discloses a novel method to implement a Smart Device Network Application Infrastructure (SDNA) that supports and facilitates the development, deployment and management of device networks and device

[0022] Objects and Advantages

[0023] Accordingly, several objects and advantages of the present invention are:

[0024] a) To provide a comprehensive method for an integrated infrastructure that encloses all fundamental tools and environments for the development, deployment and management of device network applications;

[0025] b) To provide said method for an infrastructure in which device network applications may employ any combination of dumb, communications-enabled, intelligent, network-ready and smart devices;

[0026] c) To provide said method for an infrastructure that includes device network application development tools and environments sufficient for the implementation of all solutions leading to rapid and effective design and construction of full device network applications;

[0027] d) To provide said method for an infrastructure that includes device network application deployment tools and environments sufficient for the implementation of all solutions leading to efficient and effortless deployment of full device network applications;

[0028] e) To provide said method for an infrastructure that includes device network application management tools and environments sufficient for the implementation of all solutions leading to competent and resourceful management of full device network applications;

[0029] f) To provide said method for an infrastructure in which all tools and environments for development, deployment and management of device network applications can be universally and fully utilized in relation to all device network applications and in which no special application-specific tools and environments (other than those provided within the infrastructure) may be required;

[0030] g) To provide said method for an infrastructure that is independent of the networking technology used in building the underlying device network; h) To provide said method for an infrastructure that is independent of the technology used to build the underlying devices that form the device network, whether smart, dumb or other;

[0031] i) To provide said method for an infrastructure which is applicable to numerous device network application embodiments and whose preferred embodiment relates to the development, deployment and management of automation-related smart device network applications, such as home automation, industrial automation, transportation automation, among many others.

[0032] Other objects and advantages of this invention will become apparent from a consideration of the ensuing description and drawings.

BRIEF DESCRIPTION OF DRAWINGS

[0033] **FIG. 1** shows a condensed view of the present invention"s architecture containing only its fundamental

[0034] **FIG. 2A** illustrates details of the Management Services module.

[0035] **FIG. 2B** illustrates details of the Application Services module.

[0036] **FIG. 2C** illustrates details of the Smart Network Services module.

[0037] **FIG. 2D** illustrates details of the Database Services module.

[0038] **FIG. 3** shows the detailed view of the preferred embodiment of the architecture.

[0039] **FIG. 4** shows the overall utilization of the architecture.

DETAILED DESCRIPTION

[0040] The method herein disclosed will now be described by referring to the accompanying drawings that illustrate preferred embodiment of the invention.

[0041] The Smart Device Network Application infrastructure (SDNA) refers to an integrated processing platform that supports and facilitates the development, deployment and management of distributed applications based on device networks. It involves the concurrent execution of several processes that interact to provide support and resources for said applications,

[0042] SDNA is an integrated infrastructure because it incorporates into a single platform the complete lifecycle of device network applications, from inception and design, to construction and deployment, and finally to management, including application upgrade.

[0043] SDNA may operate over other basic technologies. Yet, its operation is not coupled to any specific (e.g., proprietary) technology. For instance, a device network is a fundamental requirement for the operation of SDNA, as SDNA device network applications operate on devices and device networks. However, SDNA does not require that a specific networking technology be used. SDNA is capable of interacting with the underlying device network, regardless of the network type, medium or protocol used.

[0044] Thus, SDNA is said to be independent of the underlying networking technology. In addition, a database engine is a fundamental requirement for the operation of SDNA, as SDNA internal operation and SDNA applications make use of a database engine to store essential operation, configuration and other data. However, SDNA does not require that a specific database technology be used. SDNA is capable of interacting with the underlying database engine, regardless of type, brand or other intrinsic aspects of the database. Thus, SDNA is said to be independent of the underlying database technology.

[0045] **FIG. 1** illustrates a condensed view of the SDNA architecture, showing its main processing modules, namely, Application Services (AS), Management Services (MS), Database Services (DBS) and Smart Network Services (SNS). In brief terms, the Application Services are the processes in charge of the creation of applications, the communications between different concurrent applications and deployment of applications. The Management Services implement general infrastructure management, including

application management. The Database Services implement efficient data storage, access and manipulation functionality. The Smart Network Services implement SDNA'S networking capabilities, including all inter-device communication and messaging functionality, among others functions.

[0046] Each of these processing modules is explained in detail next.

[0047] SDNA Management Services: Management Services implements SDNA'S core functionality. It is here that overall platform management is performed, including device network and application management. It also serves as an intelligent bridge between all other SDNA Services modules. It comprises the following components, as shown in **FIG. 2**A:

[0048] Coordination and Transactional Services

[0049] Entity Management Services

[0050] Resource Control Repository

[0051] Application Management Services

[0052] Logging Management Services

[0053] Data Management Services

[0054] Customer Management Services

[0055] Each of these is described in detailed next.

[0056] Coordination and Transactional Services: Coordination and Transactional Services (CTS) form the intelligent brain of SDNA. Its functions include operation as arbiter in the interaction of any two or more SDNA components, such as the interface between the Database Services and the Smart Network Services, etc.

[0057] In addition, CTS implement and support SDNA transactions. An SDNA transaction refers to a coherent set of operations carried out within the SDNA infrastructure. Said set of operations is performed as an undividable unit. The performing of an SDNA transaction is considered successful if and only if all operations involved in the transaction are carried out successfully. A detailed registry of all successful SDNA transactions and associated operations is stored so that they may be reverted if necessary (i.e., if one operation fails, all other transaction operations already carried out can be reverted).Additional CTS functions include synchronization between concurrent SDNA processes. Processes include any SDNA management service, applications, development tools, or other. Finally, CTS handles SDNA events, such as device network events, application events, user events, database events, and others.

[0058] SDNA Entity Management Services: An SDNA Entity refers to a logical abstraction that exists within the SDNA environment, having uniquely identifying attributes, serving a specific purpose and being capable of interacting with other similar abstractions. An SDNA entity may refer to a physical device, such as dumb and smart devices, or a virtual device, such as a user. Within SDNA, for instance, every user or physical device may be treated as an entity having configurable properties. The SDNA entity corresponding to a user may include properties such as name and address. The SDNA entity corresponding to a physical device may include properties such as device operation

[0059] Every SDNA entity exposes an interface of inputs and outputs through which it can communicate with everything outside of itself (e.g., other SDNA entities). Its set of inputs and outputs is called SDNA Entity Interface. Using an entity"s interface inputs, its properties may be reviewed and/or modified. An SDNA Entity may have more than one interface.

[0060] Further, coherent relationships between SDNA entities can be defined by specifying how two or more SDNA entities can connect to each other. By wisely defining relationships between basic SDNA entities, composite SDNA entities may be created. For instance, if an entity X"s outputs are connected to another entity Y"s inputs, the combination of entities X and Y may behave as a unitary entity having entity X"s inputs as inputs and entity Y"s outputs as outputs.

[0061] An exemplary composite SDNA entity is a "smart door". A smart door consists of the logical union of several basic physical devices, e.g., an infrared motion detector, an electric door and an electric lock, which themselves are basic SDNA entities. A smart door may thus be treated as a single device that, when approached, opens itself automatically.

[0062] The advantage of performing management on a basis of SDNA entities is that management of all objects within the SDNA infrastructure may be carried out as a single process, significantly simplifying system maintenance. SDNA Entity Manager controls all aspects of SDNA entities, including user management, device and device group management and resource ownership management.

[0063] In applications that involve end-users (e.g., home owners in a home automation application), user management involves end-user activation and deactivation, and application customization. End-user activation and deactivation employs user-related data that permits enabling and disabling of an application. This process may operate automatically for some applications and semi-automatically for applications requiring user interaction.

[0064] Device and device group management includes enabling and disabling of all devices in SDNA'S device networks. In addition, new devices can be detected as they are introduced into the device network, and may be registered and configured accordingly without need of human interaction.

[0065] Device and device group management implements a robust structure of support that is used in case of device failure or when system maintenance is necessary. All devices contained in SDNA'S underlying device network are interconnected into the same physical network. At a higher level, however, devices may be grouped into logical networks to which only end-users with specific control privileges may have access. Control privileges are entity properties assigned to users that allow them to perform specific application operations or access specific SDNA resources.

[0066] Each end-user of every SDNA application can control, locally or remotely, any device present on his or her own logical network, and cannot control or monitor logical networks that belong to other end-users. The privilege scheme is strictly enforced and verified at device level.

[0067] Resource Control Repository: SDNA comprises a

detailed information about every resource in the SDNA infrastructure, including whether it is being used, how it is being used and what process or application is using it, among others. The Coordination and Transactional Services, the Application Management Services and other parts of SDNA Management Services use this information records to handle distribution and allocation of resources to applications and other processes that may need them.

[0068] SDNA Application Management Services: SDNA Application Management Services (AMS) support the concurrent execution of multiple applications over one single device network through SDNA Application Manager. SDNA AMS controls application activation and deactivation, and handles all application upgrades and new end-user applications created by third parties or other. In addition, AMS (in conjunction with the RCR above) controls what system resources are made available to each application.

[0069] All embedded applications residing at operative devices on the device network can be modified dynamically while they are online. This allows applications to be directly downloaded into specific network devices from SDNA'S application console across the device network. No device or network downtime is required.

[0070] Data Management Services: SDNA Data Management Services (DMS) comprise two components, namely, data transformation services and data integration services. These two parts implement the module in charge of handling data preprocessing for back-office functions and domain-specific application software. Its functions include integration with other systems. SDNA'S data, originating from network event logging or other sources, can be translated into data structures used by other systems and subsequently exported. Similarly, SDNA can import and translate data originating in foreign data systems into SDNA'S internal data structures.

[0071] Through its data transformation and integration services, SDNA also offers support for any type of devices. Data originating in foreign devices can be translated into SDNA-readable data structures. SDNA'S data structures can be translated into foreign device-readable data structures and fed to the corresponding foreign devices.

[0072] Finally, SDNA offers several supported modes for construction of interfaces to interact with end-users, such as HTTP, WAP, XML and others.

[0073] Log Services Management: The occurrence of a single transaction or event in any SDNA layer, including device network events and others, triggers the generation of an associated record indicating the nature of the transaction or event, the application associated with the transaction and the devices and users involved in the transaction. This includes both successful and unsuccessful transactions.

[0074] SDNA implements a semantic data filter generator that permits the creation of a comprehensive collection of data filters. All data logged and stored in the Smartmatic Database may be intelligently filtered to produce reports or create interfaces with other enterprise systems, such as ERPs, statistical software and others. After establishing data semantics, the physical format may be selected and an output produced.

[0075] Customer Management Services: SDNA implements interfaces between SDNA'S internal data structures and a service provider"s existing customer care and billing systems. SDNA may be configured to automatically detect specific relevant transactions (e.g., related to resource usage, etc), register a complete record including the associated transaction data, and preprocess such data to produce information ready for input to customer care, billing and invoicing systems.

[0076] SDNA Application Services: Shown in **FIG. 2**B, SDNA Application Services comprise the main support for SDNA applications and the entry point of applications into SDNA.

[0077] There are three fundamental components, namely, Integration Services, Deployment Services and Interface Gateways.

[0078] Deployment Services: Deployment Services (DS) provide tools for remote installation, deinstallation, configuration, deployment and updating (both corrective updating and version updating) of an SDNA application. DS also verifies that an application that is to be deployed is concordant with the SDNA infrastructure guidelines. Deployment Services are used by SDNA Entity Management Services to configure the application to be deployed. Each application to be deployed must be packaged in a specific manner so that Deployment Services can obtain specific deployment parameters. Deployment parameters include start deployment time, end deployment time, deployment mode, among others. Application packaging also includes a detailed description of all SDNA entities used and made available by the application.

[0079] The Deployment Manager coordinates that all underlying network devices required for the use of the application are operative and ready. Deployment Services allow deployment, updating or upgrading of an application while a device is online, thus, requiring no device or device network downtime.

[0080] Integration Services: Integration Services are processes that construct, monitor and provide tools for the configuration of communication channels among SDNA applications. These processes handle inter-application messaging, information transfer, resource sharing, and high-level application interrupts, signals and semaphors. Said channels may be shared buffers, pipes or other, and enable both synchronous and asynchronous communications. Interaction among SDNA applications and non-SDNA applications is also supported.

[0081] Gateway Interface Services: Gateway Interface Services provide support for applications" presentation layers, such as applications that involve interaction with end-users. Gateway Interfaces operate in two modes, namely, server mode and translation mode. Under the server mode, SDNA listens to user-client requests, which may be done in a specific server-client protocol (such as HTTP), processes the requests, and generates replies based on the same protocol. Under the translation mode, user requests are translated into SDNA-specific rules, and then processed. Replies are accordingly translated back from SDNA-specific language into the client-specific protocol. In addition, applications may encapsulate SDNA-specific requests inside conventional protocols. SDNA registers requests, extracts SDNA-specific instructions, processes them, and encapsu-

120

[0082] SDNA Smart Network Services: Shown on **FIG. 2**C, SDNA Smart Network Services implement SDNA'S networking capabilities, including all inter-device communication and messaging functionality. The Smart Network Services implement basic network services, and the Global Addressing and Protocol Morphing methods, which support secure and reliable communications across hybrid networks of incompatible network protocols and/or media.

[0083] Basic Network Services: Basic Network Services implement the fundamental communication processes of SDNA, including one-to-one messaging among devices, including acknowledged and unacknowledged message delivery, and one-to-many device messaging, including multicast and broadcasts. All network services required that are not supported by the underlying network technology are emulated using the Protocol Morphing technology (see below).

[0084] Global Addressing: Global Addressing constitutes a method of source routing that implements device-to-device communications across hybrid device networks. The method is based in packet communications in which packets are structured so that they can be readily converted between communications protocols, and in which packets enclose routing information and parameters.

[0085] Protocol Morphing: Protocol Morphing represents the lowest level of SDNA'S network services. If the underlying network technology does not support all network services that are required for SDNA'S global addressing and all other network functionalities, protocol morphing can implement them. That is, protocol morphing constitutes a method of emulation of basic network services, such as point-to-point messaging, multicast and broadcast messaging, and both acknowledged and unacknowledged packet delivery. These services are emulated only if they are not supported by the underlying network technology.

[0086] Device Functionality Emulation Services: In some applications, it may be desirable to add dumb or otherwise limited devices that are not already intelligent or network-ready to the device network. Accordingly, SDNA provides support services to emulate the desired device functionality that permit transparent device integration. The result is a fully integrated, hybrid network comprising smart and dumb devices alike.

[0087] SDNA Database Services: Shown on **FIG. 2**D, SDNA Database Services implement all functionality required for efficient data storage, access and manipulation of all other SDNA modules.

[0088] SDNA Database The SDNA Database, also known as SDNA Data Model, is a robust database back-end that stores all data related to SDNA operation (including configuration data, service- and user-related data, etc) and to applications executing over SDNA.

[0089] Query and Data Manipulation Services: Beyond the operation of the device network and resource management, SDNA Database Services also provide tools to execute direct data queries and modifications to the SDNA Database. This way, low-level data operations can be performed by an administrator with in-depth knowledge of the workings of the SDNA platform.

[0090] Abstraction Support: The Database Services allow combination of simpler data objects. These constitute the data structures and routines underlying SDNA entities.

[0091] Clustering, Redundancy and Backup Services: Clustering, Redundancy and Backup Services are designed to create an extra layer of data protection to guarantee data integrity and availability in case of database engine failure or other artifacts.

[0092] Operation of Invention

[0093] The operation of the method herein disclosed will now be described by referring to the accompanying drawings that illustrate preferred embodiment of the invention. **FIG. 3** shows the detailed configuration of the preferred embodiment of the present method. Note that the infrastructure illustrated in **FIG. 1** is completely embedded into the core of **FIG. 3**. Furthermore, **FIG. 3** adds several blocks to the fundamental infrastructure. These will be described next.

[0094] Application Services: The basic functioning of SDNA Application Services has been described earlier. Beyond the details illustrated in **FIG. 1**, **FIG. 3** shows two additional features, namely, blocks labeled App1 to AppN and DT1 to DTQ. Blocks App1 to AppN (i.e., App1, App2, App3 up to AppN, for arbitrary N) refer to all applications (1 through N) that are supported by the SDNA infrastructure. As stated above, Application Services are the entry points of applications into the SDNA. SDNA applications comprise a presentation interface that may be exposed over a variety of media, including Ethernet, Power Lines or Wireless interfaces. Blocks DT1 to DTQ (i.e., DT1, DT2, DT3 up to DTQ, for arbitrary Q) refer to all development tools (1 through Q) that have been integrated into SDNA. Application Development tools implement a complete Application Building Environment that provides all software libraries and tools required to develop complete distributed device network applications for the SDNA platform, such as Software Development Kits, Application Program Interfaces (APIs), and visual tools for software development.

[0095] Using these tools, developers and integrators may build applications to monitor, control, manage and automate any physical devices or logical combination of devices connected to the device network. Applications may be as simple as point-to-point device applications, and as complex as true distributed control solutions comprising an advanced distributed logic framework based on the paradigm of True Distributed Control.

[0096] SDKs and APIs offer an extensive set of software components, libraries, documentation and guidelines for rapid development of applications over the SDNA Infrastructure. They support full interaction with underlying SDNA Components, including event logging, data import and export services, data translation services, and many others.

[0097] The visual tools for software development are tools for the creation of graphical user interfaces and interface gateways, based on the latest presentation technologies. These interfaces constitute an SDNA application's presentation layer. Examples of presentation technologies are HTML/DHTML, JavaScript, ASP, JSP, WAP and XML.

[0098] Management Services: The basic functioning of

Beyond the details featured in **FIG. 1**, **FIG. 3** illustrates one additional feature, namely, blocks MT1 to MTP.

[**0099**] Blocks MT1 to MTP (i.e., MT1, MT2, MT3 up to MTP, for arbitrary P) refer to all management tools (1 through P) that are supported by the SDNA infrastructure. Management tools include any operation managers, such as the SDNA Entity Manager, that interact with SDNA internal processes (i.e., SDNA Entity Management Services). SDNA Management tools enter the SDNA infrastructure through Coordination and Transactional Services.

[**0100**] Database Services: The basic functioning of SDNA Database Services has been described above. Beyond the details shown on **FIG. 1**, **FIG. 3** illustrates two additional features, namely, DB Drivers and DB1 to DBM.

[**0101**] The Database Services module connects to Database Drivers (DB Drivers). Database Drivers translate SDNA's internal data handling routines and structures into database engine-specific language. This allows SDNA to simultaneously interface with several databases using different database engines. The Database Services enable SDNA to operate independently of the underlying database technology. Blocks DB1 to DBM (i.e., DB1, DB2, DB3, up to DBM, for arbitrary M) refer to all underlying database engines being used by the SDNA infrastructure.

[**0102**] Smart Network Services: The functioning of the SDNA Smart Network services has been described above. Beyond the details shown on **FIG. 1**, **FIG. 3** illustrates an additional feature, namely, NTGs. NTG stands for Network Translation Gateway. SDNA supports the use of several NTGs. Smart Network Services connect to Network Translation Gateways, which translate SDNA's internal communication data structures into network protocol and medium-specific language for transmission. Smart Network Services effectively enable SDNA to operate independently of the underlying networking technology. Supported network protocols include TCP/IP, LonTalk, etc. Support network media include Ethernet, ATM, Wireless (e.g., CPDP, Radio Frequency) and Power Lines.

[**0103**] **FIG. 4** illustrates an exemplary application lifecycle with SDNA. It includes three steps: Application Design and Construction, Application Deployment and Platform Management. First, using SDNA Application Services and development tools, an application is designed and constructed. This also applies to application upgrades, updates, etc.

[**0104**] Second, using SDNA Deployment Services, the new application is deployed onto the device network. This may involve downloading specific configuration or program information into all or some devices on the device network.

[**0105**] Finally, all applications are managed using SDNA Management Tools. Using SDNA Management Tools the entire platform over which applications exist can be managed. As all applications existing over SDNA follow the same guidelines, all can be managed using the same tools.

[**0106**] Conclusion, Ramifications and Scope of Invention

[**0107**] Thus, the reader will see that the presented method of integrated smart device network application infrastructure provides a comprehensive environment in which distributed device network applications, regardless of complexity, can not bound to any specific proprietary technologies and can operate over any existing network technology and use any existing technology for smart devices and smart device networks.

[**0108**] While our above description contains many details, these should not be construed as limitations to the scope of the invention, but rather as an exemplification of one preferred embodiment thereof. Obviously, modifications and alterations will occur to others upon a reading and understanding of this specification.

[**0109**] For example, other specialized service processes can be added onto every fundamental processing module shown in **FIG. 1**. These specialized services can derive from existing services or can be new altogether.

[**0110**] In addition, some special SDNA uses are evident. This is the case for companies providing network services (i.e., network service providers). SDNA can be easily used as the main infrastructure on which all services (e.g., automation-related services and applications) can be developed, deployed and offered to all customers or other users.

[**0111**] The description above is intended, however, to include all such modifications and alterations insofar as they come within the scope of the appended claims or the equivalents thereof.

What is claimed is:

1. A method to implement a Smart Device Network Application Infrastructure that supports and facilitates the development, deployment and management of device networks and device network applications, the method comprising the following steps: Having a SDNA processing platform with an Application Services module, a Management Services module, a Database Services module, and a Smart Network Services module.

2. A method as in claim 1 in which said Management Service module implements the platform's core functionality and comprises the following components:

a) Coordination and Transactional Services which functions as an arbiter in the interaction of any two or more SDNA platform components, transaction support, synchronizing between concurrent SDNA platform processes, such as SDNA platform management service, applications, or development tools and handling SDNA platform events, such as device network events, application events, user events, and database events;

b) Entity Management Services which controls all aspects of SDNA platform entities which are a logical abstractions within the SDNA platform, including user management, device and device group management and resource ownership management;

c) Resource Control Repository which contains detailed information about every resource in the SDNA platform infrastructure, including whether it is being used, how it is being used and what process or application is using it;

d) Application Management Services which controls application activation and deactivation, and handles all application upgrades and it controls what system

e) Logging Management Services which register all events and transactions occurring in any SDNA layer, and implements a semantic data filter generator that permits the creation of a comprehensive collection of data filters which can be used to produce reports or interfaces to other systems;

f) Data Management Services which is comprised of data transformation services and data integration services; and

g) Customer Management Services which implements services that operate as interfaces between SDNA platform's internal data structures and other systems.

3. A method as in claim 1 in which said Application Service comprises the main support for SDNA platform applications and the entry point of applications into said SDNA platform and comprises the following components: a) Deployment Services which provide tools for remote installation, deinstallation, configuration, deployment and updating of an application; b) Integration Services which construct, monitor and provide tools for the configuration of communication channels among applications; and c) Gateway Interface Services which provides support for an applications" presentation layers.

4. A method as in claim 1 in which said Smart Network Services implement SDNA platform's networking capabilities, including all inter-device communication and messaging functionality and comprises the following components: a) Basic Network Services which implements the fundamental communication processes of SDNA platform; b) Global Addressing which constitutes a method of source routing that implements device-to-device communications across hybrid device network based on packet communications; c) Protocol Morphing which is a method of emulation of basic network services emulating all basic network services that are not implemented by the underlying network technology; and d) Device Functionality Emulation Services which provides support services to emulate the desired device functionality.

5. A method as in claim 1 in which said Database Services implements all functionality required for efficient data storage, access and manipulation and comprises the following components: a) The SDNA Database which is a database that stores all data related to SDNA platform operation; b) Query and Data Manipulation Services which are tools to execute direct data queries and modifications to the SDNA Database; c) Abstraction Support which allows the generation of abstract data objects derived from a logical combination of simpler data objects; and d) Clustering, Redundancy and Backup Services which creates an extra layer of data protection to guarantee data integrity and availability in case of database engine failure.

6. A computer program wherein the base component has interfaces and the program code for: Having a SDNA processing platform with an Application Services module, a Management Services module, a Database Services module, and a Smart Network Services module.

7. A computer program as in claim 6 wherein the base component has interfaces and the program code for said Management Service module to implement the platform's core functionality and comprises the following components: a) Coordination and Transactional Services which functions platform components, transaction support, synchronizing between concurrent SDNA platform processes, such as SDNA platform management service, applications, or development tools and handling SDNA platform events, such as device network events, application events, user events, and database events; b) Entity Management Services which controls all aspects of SDNA platform entities which are a logical abstractions within the SDNA platform, including user management, device and device group management and resource ownership management; c) Resource Control Repository which contains detailed information about every resource in the SDNA platform infrastructure, including whether it is being used, how it is being used and what process or application is using it; d) Application Management Services which controls application activation and deactivation, and handles all application upgrades and it controls what system resources are made available to each application; e) Logging Management Services which register all events and transactions occurring in any SDNA layer, and implements a semantic data filter generator that permits the creation of a comprehensive collection of data filters which can be used to produce reports or interfaces to other systems; f) Data Management Services which is comprised of data transformation services and data integration services; and g) Customer Management Services which implements services that operate as interfaces between SDNA platform's internal data structures and other systems.

8. A computer program as in claim 6 wherein the base component has interfaces and the program code for said Application Service to comprise the main support for SDNA platform applications and the entry point of applications into said SDNA platform and comprises the following components: a) Deployment Services which provide tools for remote installation, deinstallation, configuration, deployment and updating of an application; b) Integration Services which construct, monitor and provide tools for the configuration of communication channels among applications; and c) Gateway Interface Services which provides support for an applications" presentation layers.

9. A computer program as in claim 6 wherein the base component has interfaces and the program code for said Smart Network Services to implement SDNA platform's networking capabilities, including all inter-device communication and messaging functionality and comprises the following components: a) Basic Network Services which implements the fundamental communication processes of SDNA platform; b) Global Addressing which constitutes a method of source routing that implements device-to-device communications across hybrid device network based on packet communications; c) Protocol Morphing which is a method of emulation of basic network services emulating all basic network services that are not implemented by the underlying network technology; and d) Device Functionality Emulation Services which provides support services to emulate the desired device functionality.

10. A computer program as in claim 6 wherein the base component has interfaces and the program code for said

for efficient data storage, access and manipulation and comprises the following components: a) The SDNA Database which is a database that stores all data related to SDNA platform operation; b) Query and Data Manipulation Services which are tools to execute direct data queries and modifications to the SDNA Database; c) Abstraction Support which allows the generation of abstract data objects derived from a logical combination of simpler data objects; and d) Clustering, Redundancy and Backup Services which creates an extra layer of data protection to guarantee data integrity and availability in case of database engine failure.

* * * * *