No. _____

UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

In re: Christopher Earl Strunk, and Harold William Van Allen,

Petitioners.

PETITION WITH 28 USC §1651 FOR A WRIT OF MANDAMUS AND INJUNCTIVE EQUITY RELIEF PURSUANT TO THE NATIONAL EMERGENCY MANDATE(S) ISSUED BY THE COMMANDER-IN-CHIEF, DONALD JOHN TRUMP FOR AN ORDER:

A. TO PRESERVE, UNTIL FURTHER NOTICE BY THIS COURT, ALL PAPER BALLOTS CAST ON 6 NOVEMBER 2018 BY U.S. CITIZEN VOTERS AT THE NATIONAL MID-TERM GENERAL ELECTION IN THE STATE OF NEW YORK AND THE SEVERAL STATES AND TERRITORIES; AND

B. TO CONVENE A TITLE 10 §935. ART. 135. COURT OF INQUIRY INTO FOREIGN MEDDLING DURING THE 6 NOVEMBER 2018 ELECTION CYCLE; AND

C. TO ISSUE A REPORT FOR THE DEPARTMENT OF HOMELAND SECURITY SECRETARY KIRSTJEN M. NIELSEN; AND FOR

D. SUCH OTHER AND DIFFERENT RELIEF DEEMED NECESSARY.

Christopher Earl Strunk in esse Sui juris, in propria persona
141 Harris Avenue Lake Luzerne, New York Zip code excepted [12846]
Ph: 518-416-8743; Email: chris@privateamerciancitizen.org

Harold William Van Allen in esse Sui juris, in propria persona
351 North Road Hurley New York 12443
Ph: 845-389-4366; Email: billvanallen@icloud.com

TABLE OF CONTENTS

INTRODUCTION.....6

RELIEF SOUGHT 10

PETITIONERS 11

STATEMENT OF FACTS 12

ISSUES RAISED 28

CONCLUSION 30

STRUNK PETITION VERIFICATION AFFIDAVIT 31

VAN ALLEN PETITION VERIFICATION AFFIDAVIT.....32

PETITION COMPLIANCE STATEMENT 33

APPENDIX FOR THE PETITION WITH 28 USC §1651 FOR A WRIT OF MANDAMUS AND INJUNCTIVE EQUITY RELIEF PURSUANT TO THE NATIONAL EMERGENCY MANDATE(S) ISSUED BY THE COMMANDER-IN-CHIEF, DONALD JOHN TRUMP

DATE	EXHIBIT		PAGE
12 -Sep.-18	Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election		APX 001
14 -Mar.-18	*Americans for Innovation*: Senior Executive Service (SES) is ~10,000 Deep State shadow government employees who are sabotaging the American Republic for the globalist agenda		APX 009

4 -Apr.-18	American Intelligence Media (AIM) Plum Book (1980-2016) Analysis: Plum books hide SES employees in a blizzard of bad math and contradictory, nonsensical categories		APX 022
11 -Apr.-18	American Intelligence Media (AIM) : TENTACLES OF SERCO STRANGLE AMERICA		APX 037
11 -Apr.-18	SERCO U. S. GOVERNMENT CONTRACTS (ibid)		APX 062
4-Oct.-18	Remarks by Vice President Pence on the Administration's Policy Toward China		APX 080
22-Oct-18	STRUNK'S Absentee Ballot Warren County		APX 093
22-Oct-18	VAN ALLEN'S Sample Ulster County Ballot		APX 098
22-Oct-18	Selection of VAN ALLEN'S and STRUNK's New York State Court election Law cases		APX 100
23-Jul-18	Michael T. McKibben's /Leader Technologies Inc. Miller Act cover letter to POTUS Donald J Trump re Serco Inc / SES theft of Software Patent		APX 101
23-Jul-18	Michael T. McKibben's / Leader Technologies Inc. Miller Act Notice For Federal Work's Project 40 USC §3131 et seq. re Software Patent Theft		APX 104
23-Oct-18	Washington State Courts Appellate Court Case Summary for Petition for Writ of Mandamus, *James M. Miller v. Secretary of State, Kim Wyman* No. 96235-9 filed on 28 August 2018		APX 127
28-Aug-18	Petition for Writ of Mandamus, *James M. Miller v. Secretary of State, Kim Wyman* No. 96235-9 with Exhibits A thru L		APX 128

19-Jul-18	Special Note: No. 96235-9 re Exhibit D Letter to President Trump by Governors Jay Inslee and Andrew Cuomo re ongoing Foreign Interference in the 2018 State Election Cycle		APX 187
6-Jul-18	Special Note: No. 96235-9 re Exhibit G Chart of Chief Electronic Voting Scammers connected to Electronic Voting Machine Foreign Interference.		APX 199
18-Sep-15	Special Note: No. 96235-9 re Exhibit H EPA Letter to Volkswagen AG re Notice of Software Violation		APX 201
11-Jul-18	Special Note: No. 96235-9 re Exhibit I US Senator Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers		APX 207
17-Jul-18	Special Note: No. 96235-9 re Exhibit J MOTHERBOARD Report: PCANYWHERE Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States		APX 210
6-Aug-18	Special Note: No. 96235-9 re Exhibit L 8/5/18 Professional Experience & Resume of Plaintiff James M. Miller - with 8/6/18 statement on System Security - Election & Voting - WA Secretary of State and 10/17/17 Fortune Magazine analysis "This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings" by Don Reisinger		APX 224
6-Aug-18	Special Note: No. 96235-9 re Exhibit L Statement on System Security - Election & Voting - WA Secretary of State		APX 226
6-Aug-18	Special Note: No. 96235-9 re Exhibit L 10/17/17 Fortune Magazine analysis "This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings" by Don Reisinger		APX 230

12-Oct-18	Response to Petition No. 96235-9, on October 12, 2018, REBECCA R. GLASGOW, WSBA 32886 *Deputy Solicitor General* maneuvered to postpone hearing until after 6 November 2018		APX 241
26-Jul-18	Washington Examiner: On 26 July 2018 House Intelligence Committee Chairman Devin Nunes (R-Calif.) called for a ban on electronic voting systems in an interview that aired Thursday in Washington Examiner		APX 265
31-Jul-18	On 31 July 2018 the Department of Homeland Security Secretary Kirstjen M. Nielsen Keynote Speech issued at the National Cyber-security Summit		APX 266
13-Jul-17	Presidential Advisory Commission on Election Integrity update		APX 276
3-Jan-18	Statement by the Press Secretary on ending the Presidential Advisory Commission on Election Integrity Issued on: January 3, 2018		APX 281
1-Oct-18	Americans for Innovation Study Report update to the 15-Sept-2018 initial report: HILLARY CLINTON CONTROLS 50,000 FBI ENCRYPTION KEYS—PROVES MUELLER'S WITCH HUNT IS TREASONOUS (Re: ENTRUST)		APX 282
1-Oct-18	TIMELINE: BILL & HILLARY CLINTON BEGAN ORCHESTRATING UNFETTERED ACCESS TO THE FBI'S ENCRYPTION KEYS IN 1993 (Re: ENTRUST)		APX 290
13-Sep-18	ENTRUST (ENTU 1998-2009) 10-K, Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: Securities Exchange Commission (SEC) Edgar with Alpha Sort		APX 308
24-Oct-18	THE HILL: Officials prepare for potential of claims of election interference BY JACQUELINE THOMSEN - 10/24/18 06:00 AM EDT		APX 331

INTRODUCTION

PLEASE TAKE NOTICE That the honorable judges of this Court: Scott W. Stucky (Chief Judge.); Margaret A. Ryan; Kevin A. Ohlson; John E. Sparks; Gregory E. Maggs; are petitioned by *Accusers* defined by 10 USC 801-9 [1] for offenses against nationals of the United States outside the jurisdiction of any nation defined by 18 USC §7 -7 as if for special maritime and territorial jurisdiction of the United States using Court Rule 67(c) as to *Civil Affairs* [2] under the 12 USC §95(a) amended 50 USC App. §5(b) ongoing emergency [3] with the Military Government [4] U.S. Army duties in the Community under the Honorable Donald J. Trump POTUS / Commander-in-Chief (CINC), as was defined by the clarity of the U.S. Army Field Manual (FM) 41-10-1962 now amended into *Civil Affairs Operations*

---

[1] 10 USC §801 *Definitions* (9) The term "accuser" means a person who signs and swears to charges, any person who directs that charges nominally be signed and sworn to by another, and any other person who has an interest other than an official interest in the prosecution of the accused.

[2] FM 41-10-1962 Chapter 1 Paragraph 2 Definitions *a. Civil Affairs.* Those phases of the activities of a commander which embrace the relationship between the military forces and the civil authorities and people in a friendly (including US home territory) or occupied area where military forces are present. In an occupied country or area this may include the exercise of executive, legislative, and judicial authority by the occupying power.

[3] FM 41-10-1962 Chapter 1 Paragraph 2 Definitions ***d.*** *Civil Emergency.* Emergencies affecting public welfare as a result of enemy attack, insurrection, civil disturbance, earthquake, fire, flood, or other public disasters or equivalent emergencies which endanger life and property or disrupt the usual process of government. (Emphasis by Petitioners)

[4] FM 41-10-1962 Chapter 1 Paragraph 2 Definitions- *g. Military Government.* Form of administration by which an occupying power exercises executive, legislative, and judicial authority over occupied territory.

FM 3-57 dated 31 October 2011 applies with Chapter 4 Section 52 as to the civilian event of the early voting ongoing mid-term "elections" with the deadline of November 6. 2018 that affect military operations [5] CINC warned of with the 12 September 2018 *Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election* **(see APX 001** thru **APX 008);** and

Further accordingly, as now applies with Civil Affairs Operations FM 3-57 is changed in keeping with the Hague and Geneva Conventions with related law, as FM 41-10-1962 was used prior to the *International Covenant on Civil and Political Rights* (ICCPR) that adopted and opened for signature, ratification and accession by the United Nations General Assembly resolution 2200A (XXI) of 16 December 1966, with entry into force on 23 March 1976 in accordance with Article 49 that does not apply within the United States per se; and

Further, ICCPR was adopted, with reservations by Canada in 1982 concurrent with its Constitution, without recourse in the United States in 1992, and in the Russian Federation with its Constitution in 1992 without reservations; and

[5] US Army FM 3-51 Chapter 4-52. Just as there are different categories of civilians, there are different categories of civilian ***events*** that may affect military operations. Some examples are planting and harvest seasons, **elections**, riots, and evacuations (both voluntary and involuntary). Likewise, there are military events that affect the lives of civilians in an AO. Some examples are combat operations, including indirect fires, deployments, and redeployments. CAO/CMO planners determine what events are occurring, and analyze the events for their political, economic, psychological, environmental, and legal implications.

Further, without even ICCPR protection posed on paper for U.S. Citizen voters in this ongoing Mid-term 2018 election cycle - ICCPR does not apply herein; and furthermore, in the absence of any expectation of due process of law relief in any State and or Federal court to afford all voters national equal protection of the law plus being subject to the complete and utter absence of a so-called Justice Department (DOJ) with Attorney General Jeff Sessions (the Mr. Magoo of our time) who is absent without leave; and DOJ operates a vast criminal enterprise run by the 500 Senior Executive Service (SES) [6] member DOJ *central committee* (see **APX 009** thru **APX 036**) under the FISA warrant 'Robo-Signer'

[6] The **Senior Executive Service** (**SES**) is a position classification in the civil service of the United States federal government, equivalent to general officer or flag officer ranks in the U.S. Armed Forces; created in 1979 when the Civil Service Reform Act of 1978 went into effect under President Jimmy Carter, Zbigniew Brzezinski and Stansfield Turner.

According to the Office of Personnel Management, the SES was designed to be a corps of executives, who may not be U.S. Citizens or even qualify under a rigorous security background check, selected for their leadership qualifications, serving in key positions just below the top Presidential appointees as a link between them and the rest of the Federal (civil service) workforce. SES positions are considered to be above the GS-15 level of the General Schedule, and below Level III of the Executive Schedule. Career members of the SES ranks are eligible for the Presidential Rank Awards program.

Up to 10% of SES positions can be filled as political appointments rather than by career employees. About half of the SES is designated "Career Reserved", which can only be filled by career employees. The other half is designated "General", which can be filled by either career employees or political appointments as desired by the administration. Due to the 10% limitation, most General positions are still filled by career appointees.

Senior level employees of several agencies are exempt from the SES but have their own senior executive positions; these include the Federal Bureau of Investigation, Central Intelligence Agency, Transportation Security Administration, Federal Aviation Administration, Government Accountability Office, Members of the Foreign Service, and government corporations.

Unlike the General Schedule (GS) grades, SES pay is determined at agency discretion within certain parameters, and there is no locality pay adjustment. The minimum pay level for the SES is set at 120 percent of the basic pay for GS-15 Step 1 employees ($126,148 for 2018).

Rod Jay Rosenstein who affords silence for Christopher Wray, Gina Haspel, and General Paul M. Nakasone, USA (who assumed NSA command from Admiral Mike Rogers, USN) for the fifth Director of National Intelligence (DNI) Daniel Coats who was sworn in on March 16, 2017 (who seems pre-occupied to hide under the National Security rubric the $21 trillion of off balance sheet debt for a total $52 Trillion of indebtedness under the 85 year bankruptcy), all ignore AAG Rosenstein with his henchmen of the Chinese / Globalist intelligence community that includes Senator Diane Feinstein and other Congress persons whose staffers such as the Pakistani Awan Brothers are of the 10000 plus members of the constitutionally questionable fourth branch of government listed in the *Plum Book*, the Senior Executive Service and post employment SES Association who serve quid pro quo for SERCO INC. (see **APX 037** thru **APX 079**), and in effect warned of in ***Remarks by Vice President Pence on the Administration's Policy Toward China*** issued on October 4, 2018 at the The Hudson Institute of Washington, D.C. (see **APX 080** thru **APX 092**), stated quote:

> VP Pence: The Chinese Communist Party is rewarding or coercing American businesses, movie studios, universities, think tanks, scholars, journalists, and local, state, and federal officials.
>
> **And worst of all, China has initiated an unprecedented effort to influence American public opinion, the 2018 elections, and the environment leading into the 2020 presidential elections**. To put it bluntly, President Trump's leadership is working; and China wants a different American President.

> There can be no doubt: **China is meddling in America's democracy. As President Trump said just last week, we have, in his words, "found that China has been attempting to interfere in our upcoming [midterm] election[s]."**
>
> Our intelligence community says that "**China is targeting U.S. state and local governments and officials to exploit any divisions between federal and local levels on policy. It's using wedge issues, like trade tariffs, to advance Beijing's political influence**."

And as such with this said, Petitioners seek available remedy, afford fair notice only in this remaining true Article 1 court to obtain a Writ of Mandamus, and based upon our nearly forty years experience in the State and Federal judicial system along with SCOTUS, all appear to remain politically and ideological compromised.

RELIEF SOUGHT

Petitioners seek relief with 28 USC §1651 for a writ of mandamus with injunctive equity relief pursuant to the national emergency mandate(s) issued by the Commander-In-Chief, Donald John Trump for an order:

A. To preserve, until further notice by this court, all paper ballots cast on 6 November 2018 by U.S. Citizen voters at the national mid-term general election in the State of New York and the several states and territories; and

B. To convene a Title 10 §935. Art. 135. court of inquiry [7] into foreign meddling during the 6 November 2018 election cycle; and

---

7 **Title 10 §935. Art. 135. Courts of inquiry**

C. To issue a report for the Department of Homeland Security Secretary Kirstjen M. Nielsen; and for

D. Such other and different relief deemed necessary.

PETITIONERS

1. **Petitioner Christopher Earl Strunk** in esse Sui juris (Strunk), in propria

---

(a) Courts of inquiry to investigate any matter may be convened by any person authorized to convene a general court-martial or by any other person designated by the Secretary concerned for that purpose, whether or not the persons involved have requested such an inquiry.

(b) A court of inquiry consists of three or more commissioned officers. For each court of inquiry the convening authority shall also appoint counsel for the court.

(c) Any person subject to this chapter whose conduct is subject to inquiry shall be designated as a party. Any person subject to this chapter or employed by the Department of Defense who has a direct interest in the subject of inquiry has the right to be designated as a party upon request to the court. Any person designated as a party shall be given due notice and has the right to be present, to be represented by counsel, to cross-examine witnesses, and to introduce evidence.

(d) Members of a court of inquiry may be challenged by a party, but only for cause stated to the court.

(e) The members, counsel, the reporter, and interpreters of courts of inquiry shall take an oath to faithfully perform their duties.

(f) Witnesses may be summoned to appear and testify and be examined before courts of inquiry, as provided for courts-martial.

(g) Courts of inquiry shall make findings of fact but may not express opinions or make recommendations unless required to do so by the convening authority.

(h) Each court of inquiry shall keep a record of its proceedings, which shall be authenticated by the signatures of the president and counsel for the court and forwarded to the convening authority. If the record cannot be authenticated by the president, it shall be signed by a member in lieu of the president. If the record cannot be authenticated by the counsel for the court, it shall be signed by a member in lieu of the counsel. (Aug. 10, 1956, ch. 1041, 70A Stat. 76.)

In subsection (a), the words “Secretary concerned” are substituted for the words “Secretary of a Department”.

In subsection (b), the word “commissioned” is inserted for clarity. The word “consists” is substituted for the words “shall consist”.

In subsection (c), the word “has” is substituted for the words “shall have”.

In subsection (e), the words “or affirmation” are omitted as covered by the definition of the word “oath” in section 1 of title 1.

In subsection (g), the word “may” is substituted for the word “shall”.

In subsection (h), the word “If” is substituted for the words “In case”.

persona, with place for service at 141 Harris Avenue Lake Luzerne, New York Zip Code 12846 Ph: 518-416-8743; Email: chris@privateamerciancitizen.org (hereinafter "Petitioner" among the "Petitioners");

2. Strunk is a Vietnam Era Veteran having served honorably in the United States Air Force with rank of E-5 from December 7, 1966 thru December 6, 1972.

3. Strunk has a Public U.S. Citizen registration to vote in Warren County at New York's Federal Mid-term General Election scheduled for 6 November 2018, and Strunk cast a vote by mail on 22 October 2018 (see **APX 093** thru **APX 097**); and

4. **Petitioner Harold William Van Allen** in esse sui juris, in propria persona (Van Allen) with place for service at 351 North Road Hurley New York 12443 Ph: 845-389-4366; Email: billvanallen@icloud.com (hereinafter "Petitioner" among the "Petitioners"); and

5. Van Allen is a service related disabled Vietnam Era Veteran having served honorably in the United States Navy with rank of O-2 - June 1972 thru June 1978.

6. Van Allen has a Public U.S. Citizen registration to vote in the Ulster County New York's Federal Mid-term General Election scheduled for 6 November 2018 with the candidates shown in Exhibit (see **APX 098** thru **APX 099**).

STATEMENT OF FACTS

7. That Petitioners are aware of what General and then CINC Dwight D.

Eisenhower meant as he left Office on Jan. 17, 1961, warned the world about danger for tyranny arising from the Congressional *Military-Industrial Complex*.[8]

---

[8] **Military-Industrial Complex Speech, Dwight D. Eisenhower, 1961.** Quote:

"My fellow Americans:

Three days from now, after half a century in the service of our country, I shall lay down the responsibilities of office as, in traditional and solemn ceremony, the authority of the Presidency is vested in my successor.

This evening I come to you with a message of leave-taking and farewell, and to share a few final thoughts with you, my countrymen.

Like every other citizen, I wish the new President, and all who will labor with him, Godspeed. I pray that the coming years will be blessed with peace and prosperity for all.

Our people expect their President and the Congress to find essential agreement on issues of great moment, the wise resolution of which will better shape the future of the Nation.

My own relations with the Congress, which began on a remote and tenuous basis when, long ago, a member of the Senate appointed me to West Point, have since ranged to the intimate during the war and immediate post-war period, and, finally, to the mutually interdependent during these past eight years.

In this final relationship, the Congress and the Administration have, on most vital issues, cooperated well, to serve the national good rather than mere partisanship, and so have assured that the business of the Nation should go forward. So, my official relationship with the Congress ends in a feeling, on my part, of gratitude that we have been able to do so much together.

II.

We now stand ten years past the midpoint of a century that has witnessed four major wars among great nations. Three of these involved our own country. Despite these holocausts America is today the strongest, the most influential and most productive nation in the world. Understandably proud of this pre-eminence, we yet realize that America's leadership and prestige depend, not merely upon our unmatched material progress, riches and military strength, but on how we use our power in the interests of world peace and human betterment.

III.

Throughout America's adventure in free government, our basic purposes have been to keep the peace; to foster progress in human achievement, and to enhance liberty, dignity and integrity among people and among nations. To strive for less would be unworthy of a free and religious people. Any failure traceable to arrogance, or our lack of comprehension or readiness to sacrifice would inflict upon us grievous hurt both at home and abroad.

Progress toward these noble goals is persistently threatened by the conflict now engulfing the world. It commands our whole attention, absorbs our very beings. We face a hostile ideology -- global in scope, atheistic in character, ruthless in purpose, and insidious in method. Unhappily the danger is poses promises to be of indefinite duration. To meet it successfully, there is called for, not so much the emotional and transitory sacrifices of crisis, but rather those which enable us to carry forward steadily, surely, and without complaint the burdens of a prolonged and complex struggle -- with liberty the stake. Only thus shall we remain, despite every provocation, on our charted course toward permanent peace and human betterment.

Crises there will continue to be. In meeting them, whether foreign or domestic, great or small, there is a recurring temptation to feel that some spectacular and costly action could become the miraculous solution to all current difficulties. A huge increase in newer elements of our defense; development of unrealistic programs to cure every ill in agriculture; a dramatic expansion in basic and applied research -- these and many other possibilities, each possibly promising in itself, may be suggested as the only way to the road we wish to travel.

But each proposal must be weighed in the light of a broader consideration: the need to maintain balance in and among national programs -- balance between the private and the public economy, balance between cost and hoped for advantage -- balance between the clearly necessary and the comfortably desirable; balance between our essential requirements as a nation and the duties imposed by the nation upon the individual; balance between actions of the moment and the national welfare of the future. Good judgment seeks balance and progress; lack of it eventually finds imbalance and frustration.

The record of many decades stands as proof that our people and their government have, in the main, understood these truths and have responded to them well, in the face of stress and threat. But threats, new in kind or degree, constantly arise. I mention two only.

IV.

A vital element in keeping the peace is our military establishment. Our arms must be mighty, ready for instant action, so that no potential aggressor may be tempted to risk his own destruction.

Our military organization today bears little relation to that known by any of my predecessors in peacetime, or indeed by the fighting men of World War II or Korea.

Until the latest of our world conflicts, the United States had no armaments industry. American makers of plowshares could, with time and as required, make swords as well. But now we can no longer risk emergency improvisation of national defense; we have been compelled to create a permanent armaments industry of vast proportions. Added to this, three and a half million men and women are directly engaged in the defense establishment. We annually spend on military security more than the net income of all United States corporations.

This conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence -- economic, political, even spiritual -- is felt in every city, every State house, every office of the Federal government. We recognize the imperative need for this development. Yet we must not fail to comprehend its grave implications. Our toil, resources and livelihood are all involved; so is the very structure of our society.

In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military industrial complex. The potential for the disastrous rise of misplaced power exists and will persist.

We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals, so that security and liberty may prosper together.

Akin to, and largely responsible for the sweeping changes in our industrial-military posture, has been the technological revolution during recent decades.

In this revolution, research has become central; it also becomes more formalized, complex, and costly. A steadily increasing share is conducted for, by, or at the direction of, the Federal government.

Today, the solitary inventor, tinkering in his shop, has been overshadowed by task forces of scientists in laboratories and testing fields. In the same fashion, the free university, historically the fountainhead of free ideas and scientific discovery, has experienced a revolution in the conduct of research. Partly because of the huge costs involved, a government contract becomes virtually a substitute for intellectual curiosity. For every old blackboard there are now hundreds of new electronic computers.

The prospect of domination of the nation's scholars by Federal employment, project allocations, and the power of money is ever present

and is gravely to be regarded. Yet, in holding scientific research and discovery in respect, as we should, we must also be alert to the equal and opposite danger that public policy could itself become the captive of a scientific technological elite.

It is the task of statesmanship to mold, to balance, and to integrate these and other forces, new and old, within the principles of our democratic system -- ever aiming toward the supreme goals of our free society.

V.

Another factor in maintaining balance involves the element of time. As we peer into society's future, we -- you and I, and our government -- must avoid the impulse to live only for today, plundering, for our own ease and convenience, the precious resources of tomorrow. We cannot mortgage the material assets of our grandchildren without risking the loss also of their political and spiritual heritage. We want democracy to survive for all generations to come, not to become the insolvent phantom of tomorrow.

VI.

Down the long lane of the history yet to be written America knows that this world of ours, ever growing smaller, must avoid becoming a community of dreadful fear and hate, and be instead, a proud confederation of mutual trust and respect.

Such a confederation must be one of equals. The weakest must come to the conference table with the same confidence as do we, protected as we are by our moral, economic, and military strength. That table, though scarred by many past frustrations, cannot be abandoned for the certain agony of the battlefield.

Disarmament, with mutual honor and confidence, is a continuing imperative. Together we must learn how to compose differences, not with arms, but with intellect and decent purpose. Because this need is so sharp and apparent I confess that I lay down my official responsibilities in this field with a definite sense of disappointment. As one who has witnessed the horror and the lingering sadness of war -- as one who knows that another war could utterly destroy this civilization which has been so slowly and painfully built over thousands of years -- I wish I could say tonight that a lasting peace is in sight.

Happily, I can say that war has been avoided. Steady progress toward our ultimate goal has been made. But, so much remains to be done. As a private citizen, I shall never cease to do what little I can to help the world advance along that road.

VII.

So -- in this my last good night to you as your President -- I thank you for the many opportunities you have given me for public service in war and peace. I trust that in that service you find some things worthy; as for the rest of it, I know you will find ways to improve performance in the future.

8. Petitioners have been involved in dozens of State (see **APX 100**) and Federal election / suffrage rights related cases ourselves and by our associates for the sake of brevity some of which are listed without a description:

- In Re: Schulz etal v. The State of New York etal. NDNY 95cv133 (CGC) with Dr. Walker F. Todd Ph.D. Esq. as counsel for Plaintiffs;
- In Re: STRUNK v. UNITED STATES DEPARTMENT OF COMMERCE BUREAU OF THE CENSUS et al (1:09-cv-01295) (NG)
- In Re: Strunk v. US Dept of Housing Urban Development etal. EDNY 99cv6480 (NG)
- In Re: Loeber etal v. Spargo etal. NDNY 04cv1193 (LEK)
- In Re: Forjone etal v California etal. WDNY 06cv0080 / NDNY 06cv01002
- In Re: USA v NYS Board of Elections etal. NDNY 04cv0263 (GLS)
- In Re: Schulz etal. v State of New York etal. NDNY 07cv00943 (LEK) file a very large set of multidistrict cases one in each State of the several states with a separate Plaintiff in each State, therein challenging the

---

You and I -- my fellow citizens -- need to be strong in our faith that all nations, under God, will reach the goal of peace with justice. May we be ever unswerving in devotion to principle, confident but humble with power, diligent in pursuit of the Nation's great goals.

To all the peoples of the world, I once more give expression to America's prayerful and continuing aspiration: Source: Public Papers of the Presidents, Dwight D. Eisenhower, 1960, p. 1035- 1040 See https://youtu.be/orEurY6HdXU and text at http://avalon.law.yale.edu/20th_centuryeisenhower001.

unconstitutional use of electronic voting rather than paper ballots with a chain of custody for counting and tally and for which the corrupt civil courts buried the cases and terrorized Robert Schulz for the past 6 years;

- In Re: STRUNK V. C.I.A. EDNY Civil Action No. 08cv01196 (ARR)
- In Re: Jah Thomas, Basil Guilavigui and Christopher Earl Strunk v the Federal Reserve Bank of New York etal. DNY2007cv01171 (ARR)
- In Re: Strunk v NYS Board of Elections etal. NYS Kings Cty Sup. 6500-11
- In Re: Strunk v. DOS et al. DCD 08-cv-2234 (RJL)
- In Re: STRUNK v. U.S. DEPARTMENT OF COMMERCE BUREAU OF THE CENSUS et al (1:09-cv-01295) (RJL)
- In Re: Strunk v New York State Board of Elections, et al., Index No. 08-CV4289 (US Dist Ct, EDNY, Oct. 28, 2008, Ross, J.)
- In Re: Apr 24, 2016 - Strunk v DTCC etal USCA 2nd Circuit 15-3199. Strunk v DTCC, Robert Druskin etal SDNY 15cv6817.
- In Re: STRUNK v. THE STATE OF CALIFORNIA etal. NYND 16-cv-1496 (BKS/ DJS) was a challenge to the vote fraud involving illegal voters in California and New York to no avail in anticipation of results obtained by the Presidential 2016 Election Integrity Commission ordered 11 May 2017 that Judge Sannes dismissed the case without prejudice on 15 May 2017.

9. Our compatriot engineer, Michael T. McKibben founder of *Americans For*

Innovation (AFI) and *Leader Technologies Inc.*, is the actual inventor of social network scaling software that was stolen from the SERCO INC. controlled U.S. Patent Office and its agents for Google, Facebook and other social network platforms; and

10. Further, AFI investigation has proven the theft has affected every election cycle -since 2008, and that since Sep. 29, 1999 started when the C.I.A. began investing in hardware and software companies, thus essentially nationalizing largely in secret, America's emerging digital infrastructure; and

11. Further, having exhausted available remedy Mr. McKibben filed a Miller Act claim with CINC Trump (see **APX 101** thru **APX 126**); and

12. Further, based upon information and belief, in that the theft gave the C.I.A. an unprecedented and unaccountable ability to spy on everyone without a warrant, and given the C.I.A. theft has created government liability under the Miller Act (40 U.S.C. §§ 3131-3134) evidenced by voluminous spreadsheet summaries compiled by Leader Technologies, Inc. within the last week, available to this court upon request, are the contracts acquired by SERCO INC. between 20 September 2005 and 11 May 2018 [(9)] with the Department of Commerce (DOC), the U.S.

9 Serco-All-Federal-Agency-Prime-Contracts-between-Sep-30-2005-to-May-01-2018-USAspending-May-11-2018.
Serco-DOD-Prime-Contracts-between-Aug-14-2006-to-Apr-01-2018-USAspending-May-11-2018.csv
Serco-OPM-Contracts-between-Nov-28-2007-to-Nov-20-2015-USAspending-May-11-2018.csv
Serco-DUNS-014387489-Department-of-Homeland-Security-DHS-between-Jan-25-2008-to-Jan-25-2018-accessed-May-12-2018.csv

Office of Personnel Management (OPM), DOC Bureau of Census (BOC) DOC Patent Trademark Office (PTO), Department of Defense (DOD), Department of Homeland Security (DHS), Federal Acquisition Service (FAS) and other too numerous prime contracts too numerous to list herein but germane as to espionage; and

13. That based upon information and belief as a matter of foreign meddling and interference during the 6 November 2018 election cycle, there are no bid SERCO INC. contracts with Federal entities, since 2005 with reference to Footnote #9, that among other egregious exceptions to law are in violation of the Sherman and Robinson Patman Antitrust Acts that with impunity have afforded access and opportunity by Foreign enemies of the United States of America and its member States and Territories to conduct the crime of espionage by foreign enemies, and

14. Further that proof of these allegations as to spying have in part been established judicially in several cases heard before SES member Richard J. Leon, a District Court Judge in the District of Columbia, who at least regards proven egregious 4th amendment spying violations as unconstitutional, and

15. Further the said contracts summarized at Footnote #9 also involves the huge

---

Serco-Federal-Acquisitions-Service-FAS-between-Apr-20-2008-to-May-01-2018-USAspending-May-11-2018.csv
Serco-DOS-Prime-Contracts-between-Dec-29-2011-to-Dec-28-2015-USAspending-May-11-2018.csv
Serco-DOD-Subcontracts-between-Feb-04-2011-to-Mar-20-2018-USAspending-May-11-2018.csv

DOD and OPM personnel file theft disclosed in 2015 **(10)** affording jurisdiction of this Court over the Petitioners' Petition as a probable cause legal standard of proof above mere reasonable suspicion that the SES components of Government serving SERCO Inc., run by the Queen's Privy Council coordinated with the People's Republic of China (PRC) Communist Central Committee, and of course ALL the entities through their SES managers working with the SERCO INC. contracts referenced in Footnote #9 thereby actually facilitate election tampering in the United States and elsewhere that creates a civil responsibility properly based upon a major degree of military intrusion into the field of government; and

16. Further correspondingly, the scope of military authority under Civil Affairs Operations FM 3-57, is circumscribed here by the necessities of the ongoing national emergency or time of war with martial law provisions of the 12 USC §95(a) amended 50 USC App. §5(b) for extraordinary circumstances since March 6, 1933 beyond the control capability of normal government officials in application of International Law[(11)]; and whose duty falls upon the U.S. Army Chief of Staff's

---

10 https://www.opm.gov/cybersecurity/cybersecurity-incidents/ e.g. *Earlier in 2015,* OPM discovered that the personnel data of 4.2 million current and former Federal government employees had been stolen. ... may also have been impacted by the separate but related incident involving personnel records.

11 FM 41-10-1962 Chapter 1 Paragraph 8. Application of International Law. (a.) International law is usually regarded as having two branches, one dealing with the peaceful relations between states and the other concerned with armed hostilities between states. This division is not, however, absolute, and there are many facets of international relations that are difficult to regard as belonging to the law of peace or the law of war. Both branches as well as the undefined grey

authority over *Civil Affairs Functions* with civil agency(s) and the cabinet of the Commander-in-chief, with alleged dereliction of duty inter alia, for effective civil government, public finance, legal due process [(12)] .

---

area in between apply to civil affairs relations. The law of peace deals with such matters as recognition of states and governments, jurisdiction, nationality, diplomatic protocol, the prerequisites for and construction of international agreements, and, generally, the practices and standards observed by friendly states in their mutual relations. Evidence of the law of peace is to be found in law making treaties, the decisions of international and national judicial bodies, the writings of jurists, diplomatic correspondence, and other documentary material concerning the practice of states. The law of peace is particularly relevant to define the rights and obligations of a military force that is deployed in the territory of an allied state not only where there is a civil affairs agreement, but also where there is no applicable agreement or with respect to matters on which such agreement is silent. (Emphasis by Petitioners)

(b.) The law of war governs such matters as the conduct of hostilities on land, in the sea, and in the air; the status and treatment of persons affected by hostilities, such as POW'S, the sick and wounded, and civilian persons; the occupation of enemy territory, flags of truce, armistices and surrender agreements, neutrality, and war crimes. The law of war is derived from two principal sources, law making treaties, such as the Hague and Geneva Conventions, and custom, a body of unwritten law that is firmly established by the practice of nations and well defined by recognized authorities on international law. Ordinarily, a provision of an international agreement is binding on a state only to the extent that it has consented to be bound. However, a humanitarian principle enunciated in a law making treaty is binding. (Emphasis by Petitioners)

(e.) Of these' agreements, the NATO Status of Forces Agreement is particularly significant because of the precedent it has established concerning the law applicable to visiting military forces when they are in the territory of a friendly state. *The Hague Regulations are important because they are regarded as declaratory of law applicable between belligerents*. The 1949 Conventions supplement the Hague Regulations, which by their literal terns applied only to a "war" between parties signatory thereto, by broadening the scope of the Treaty law to cover not only "war" but also "any other armed conflict" and *"any partial or total occupation," involving their signatories (see FM 27-10*). An international agreement of particular significance to CA personnel is the Convention for the Protection of Cultural Property in the Event of Armed Conflict. The United States became a signatory to this agreement at the Hague in 1954. This Convention outlines the measures which armed forces shall take in the preservation of historical, cultural, and scientific properties in any enemy territory. As CA personnel will have principal responsibility for measures to be taken concerning cultural property, they should be thoroughly familiar with the legal obligations of the United States respecting artistic objects, archives, monuments, shrines, and other types of cultural property. (Emphasis by Petitioners)

[12] FM 41-10-62 CHAPTER 2 CIVIL AFFAIRS FUNCTIONS Paragraph 11 Governmental Functions. Included in this grouping of functions are those dealing with matters customarily involving governmental activity or control. The general areas of concern include the organization

and conduct of local government, political activities; review, advice, or correction of civil officials in accordance with competent directives, and implementation of policy decisions with respect to control or other relationships with government in the area of operations.

(a.) Civil Government. This function is concerned with the structure and conduct of local government. It encompasses methods of establishing legislative and executive agencies from national to local levels and the processes of these agencies in the administration of civil government. Included are such considerations as political. parties, eligibility for franchise, elections, tenure, and all other aspects of the development and operation of the apparatus of government. Commanders having area responsibility, their staffs, and CA units are charged, as appropriate, with

(1) Surveying governmental organization at all levels.

(2) Surveying lines of authority and influence having impact on political matters.

(3) Analyzing effectiveness of existing agencies of government or social control.

(4) Studying effectiveness of governmental officials and employees and of other community leaders; removing persons who are inimical to the United States or who are not in sympathy with its policies and objectives, and securing the appointment of leaders who will further desired programs.

(5) Negotiating to gain support or cooperation for United States forces.

(6) Recommending organization, functioning, staffing, and authority of agencies of government or social control.

(7) Advising, conducting liaison with, supervising, controlling, or replacing organs of government.

(8) Participating on joint commissions, committees, or councils concerned with governmental affairs.

(b.) *Legal.* This function is concerned with the legal system of the area and the application of international law in CA operations. Commanders having CA area responsibility, their staffs, and CA units are charged, as appropriate with-

(1) Translation of the legal aspect of CA operations into plans and directives.

(2) Analysis and interpretation of the civil and criminal laws of the territory, particularly restraints imposed upon the civil populace.

(3) Study of the organization of the judicial system including determination of legal status and jurisdiction of civil courts and law.

(4) Review of the local organization of the bar and determination of reliability of its members.

(5) Examination of locally accepted forms of judicial procedure including rules of evidence and rights of the accused.

(6) Assistance to commanders and staffs in the preparation of proclamations, ordinances, orders and directives, and as otherwise may be required.

(7) The establishment of necessary civil affairs tribunals and other judicial and administrative agencies, including their number, types, jurisdiction, procedures, and delegation of appointing authority.

(8) The closure or reopening of local tribunals, including courts, boards, and commissions; their jurisdiction, organization and procedure, and the class of cases triable therein.

(9) Recommendations concerning the suspension or abrogation of laws and procedural rules applicable to local courts.

(10) Recommendations concerning the alteration, suspension, or promulgation of laws to include civil legislation for the government of the area in which military forces are deployed. It may be necessary to deny enforcement effect to local legislation or to adopt new laws essential to the control of the area in question and the protection of U.S. forces. Such legislation must conform to applicable provisions of U.S. law and international law as, for example, the 1949 Geneva Civilian Convention.

(11) Supervision of the administration of civil and criminal laws by local officials.

(12) Provision of members for civil affairs tribunals.

(13) Review or administrative examination of cases tried in CA courts before referral to higher headquarters for final review.

(14) Arrangements for transmittal of civilian claims against the United States to the proper agency.

(f.) Public Finance. This function is of vast importance in the conduct of economic welfare and economic stabilization measures and assists in reducing support contributions by the United States. It includes control, supervision, and audit of fiscal resources; budget practices, taxation, expenditures of public funds, currency issues, and the banking agencies and affiliates. It is essential that the function be performed in an integrated and uniform manner within each national area. Commanders having area responsibility, their staffs, and CA units may be charged with tasks such as**:**

(1) Analysis of taxation systems and other sources of revenue, governmental expenditures, and estimates of adequacy of public funds for performance of governmental functions.

(2) Review of public laws and agencies regulating banking and financing.

(3) Analysis of financial structures including types and conditions of financial institutions.

(4) Analysis of types and amounts of circulating currencies, acceptance by population of such currencies, and current foreign exchange rates.

(5) Recommendations as to designation of type of circulating local currency.

(6) Recommendations as to provisions for military currency.

(7) Recommendations as to establishment of currency exchange rates.

(8) Establishment and enforcement of restrictions on exportation of currencies.

(9) Recommendations for control of foreign exchange.

17. Further, in addition Mr. McKibben has provided a copy of the Washington State Supreme Court Petition for Writ of Mandamus, *James M. Miller v. Secretary of State, Kim Wyman* No. 96235-9 filed on 28 August 2018 (Petition No. 96235-9), to safeguard paper ballots cast in the Federal Mid-term General Election scheduled for 6 November 2018, shown in Exhibit (see **APX 127** thru **APX 240**) for relief to:

> (1) eliminate electronic voting systems in Washington and require hand tabulation of ballots,
>
> (2) implement in-person voting with fingerprint verification, and
>
> (3) require "bipartisan groups" (rather than election officials) to process and tabulate ballots, all for the 2018 general election and future elections.

18. Further therein Petition 96235-9 Exhibit D (see **APX 186**), on July 16 2018 New York Governor Andrew Cuomo joined with Washington State Governor Jay Inslee (that arguendo defer their ineffectual individual State authority / power over the election process to Federal Jurisdiction) demand that CINC Trump protect the

---

(10) Establishment of controls over budget, taxation, expenditures, and public funds and determination of appropriate fiscal accounting procedures.

(11) Reestablishment or revision of taxation systems in accordance with policy directives.

(12) Liquidation, reorganization, opening, or closing of banks.

(13) Supervision over credit and provisions for credit needs.

(14) Regulation or supervision of governmental fiscal agencies, banks, credit cooperatives, and other financial institutions.

(15) Recommendations for advances of funds to governmental or private financial institutions.

(16) Recommendations as to emergency declaration of debt suspensions for specific types of debts.

(17) Recommendations for protection of public and private financial institutions and safeguarding funds, securities, and financial records.

electoral process from Foreign interference with the Federal Mid-term General Election cycle scheduled for 6 November 2018; and

19. Further, on 26 July 2018 House Intelligence Committee Chairman Devin Nunes (R-Calif.) called for a ban on electronic voting systems in an interview that aired Thursday in Washington Examiner (see **APX 265**); quote

> "The one thing we've been warning about for many, many years on the Intelligence committee is about the electronic voting systems," Nunes told Hill.TV's Buck Sexton, who sat with the lawmaker on Wednesday.
>
> "Those are really dangerous in my opinion, and should not be used. In California — at least in the counties that I represent — they do not use an electronic system," he continued.
> "I think anybody that does that, and that's communicating over the web, it's going to be a challenge. So you have to make sure that you limit that as much as possible, and we need a paper trail so that you can go back in case you have to do a manual recount," he said.
>
> In February, a DHS cybersecurity officials said that Russia had “in a small number of states in 2016" and warned California and 21 other states that Russia attempted to breach their systems.

20. Further yet to wit, on 31 July 2018 the Department of Homeland Security Secretary Kirstjen M. Nielsen issued at the National Cyber-security Summit by her Keynote Speech pledging to safeguard the Federal Mid-term General Election scheduled for 6 November 2018 from foreign interference (see **APX 266**); and

21. That in response to Petition No. 96235-9, on October 12, 2018, REBECCA R. GLASGOW, WSBA 32886 *Deputy Solicitor General* maneuvered to postponed hearing until after 6 November 2018, in CONCLUSION (see **APX 262**)

alleged that quote:

> "The Petition for Extraordinary Writ of Mandamus does not state a claim for relief because it does not identify any lawful basis for mandamus. The Secretary of State respectfully asks the Court to dismiss the petition with prejudice."

22. That following the 15 December 2016 filing of Strunk's election law case STRUNK v. THE STATE OF CALIFORNIA etal. NYND 16-cv-1496 (BKS/ DJS) dismissal without prejudice on 15 May 2017, that coincided with the President Donald J. Trump signed an Executive Order on 11 May 2017, establishing the Presidential Advisory Commission on Election Integrity. Vice President Mike Pence chairs the Commission, and Kansas Secretary of State Kris Kobach serves as the vice chair, see the time line at **APX 276**, and in which members of the Commission sabotaged the inquiry with court cases that resulted in cancellation of the inquiry on 3 January 2018 (see **APX 281**).

23. That on 1 October 2018, Michael T. McKibben and his researchers at American for Innovation, Leader Technologies, Inc and American Intelligence Media update the 15 September 2018 report inter alia on electronic espionage and foreign interference in the current 2016 Election cycle titled *HILLARY CLINTON CONTROLS 50,000 FBI ENCRYPTION KEYS—PROVES MUELLER'S WITCH HUNT IS TREASONOUS* and involving the foreign controlled entity ENTRUST (see **APX 282**).

24. Importantly, the Report shown starting at APX 282 explains the TIMELINE:

for how BILL & HILLARY CLINTON BEGAN ORCHESTRATING UNFETTERED ACCESS TO THE FBI'S ENCRYPTION KEYS IN 1993 for the PRC etal. in regards to ENTRUST and foreign espionage starts at **APX 290**.

25. That Michael T. McKibben of Leader Technologies, Inc. provided Strunk on 13 September 2018 his research done into the ENTRUST entity at the Securities Exchange Commission Edgar web facility to determine all the overlapping potential espionage / interference connections using an (ENTU 1998-2009) 10-K, Customer, Partner, Director, Officer, Dependent, Subsidiary (see **APX 308**).

26. That germane to this 2018 Election Cycle meddling / interference danger that is associated with ENTRUST etal., especially the psychological warfare intent of foreign interference in the ongoing election cycle, is the 24 October 2018 THE HILL article: *Officials prepare for potential of claims of election interference* by Jacqueline Thomsen (see **APX 331**).

27. That Petitioners based upon our New York experience (especially since the Clinton's PRC / Maoist crime machine moved here in the 1990s), allege that PRC national Jack Ma, the richest person on the PRC Central Committee, who had asset stripped ROC / Taiwan Industry to the PRC Mainland, and as the CEO of the PRC's *Alibaba* propaganda organization **(13)** just purchased 28,000 acres of New York Adirondack forest from the International Paper Company with the blessing of

13 http://www.nydailynews.com/news/ny-news-jack-ma-alibaba-stepping-down-20180910-story.html

New York Governor Andrew Cuomo, and that a Court Inquiry would be fruitful.

28. Based upon Petitioners experience, information and belief, the Indonesian poseur defacto President Barry Soetoro, Soebarkah, a.k.a. Barack Hussein Obama is a member of the Senior Executive Service from his time working for the Central Intelligence Agency at Business International Corporation as a non US Citizen, and as a SES member Indonesian Citizen who questionably issued Executive Order 13714 of December 15, 2015 Strengthening the Senior Executive Service.

ISSUES RAISED

Petitioners raise a series of troubling issues that are to be properly resolved in this Court related to 10 U.S. Code § 253 - Interference with State and Federal law **(14)** and or 10 U.S.C. 333 - Interference with State and Federal law, and as

---

[14] §253.1 Interference with State and Federal law.

The President, by using the militia or the armed forces, or both, or by any other means, shall take such measures as he considers necessary to suppress, in a State, any insurrection, domestic violence, unlawful combination, or conspiracy, if it-

(1) so hinders the execution of the laws of that State, and of the United States within the State, that any part or class of its people is deprived of a right, privilege, immunity, or protection named in the Constitution and secured by law, and the constituted authorities of that State are unable, fail, or refuse to protect that right, privilege, or immunity, or to give that protection; or

(2) opposes or obstructs the execution of the laws of the United States or impedes the course of justice under those laws.

In any situation covered by clause (1), the State shall be considered to have denied the equal protection of the laws secured by the Constitution.

(Aug. 10, 1956, ch. 1041, 70A Stat. 15 , §333; Pub. L. 109–364, div. A, title X, §1076(a)(1), Oct. 17, 2006, 120 Stat. 2404 ; Pub. L. 110–181, div. A, title X, §1068(a)(1), Jan. 28, 2008, 122 Stat. 325 ; renumbered §253, Pub. L. 114–328, div. A, title XII, §1241(a)(2), Dec. 23, 2016, 130 Stat. 2497 .)

would apply to the application and administration of 50 USC 212: Confiscation of property employed to aid insurrection **(15)**.

That these troubling issues require a court inquiry that derive from the purpose and use of The Sedition Act of 1918 (Pub.L. 65–150, 40 Stat. 553, enacted May 16, 1918) that was an Act of the United States Congress that extended the Espionage Act of 1917 to cover a broader range of offenses that Petitioners contend is related to the subject 2018 Election cycle foreign interference in the broader context of the Constitutionality of the Senior Executive Service per se that was created by the Civil Service Reform Act of 1978, (October 13, 1978, Pub.L. 95–454, 92 Stat. 1111) (CSRA), that reformed the civil service of the United States federal government, partly in response to the Watergate scandal, and in which CSRA questionably varied from the requirement of the Administrative Procedures Act (APA) from the due process standpoint and, in which CSRA abolished the U.S. Civil Service Commission and distributed its functions primarily among three

---

[15] §212. Confiscation of property employed to aid insurrection

Whenever during any insurrection against the Government of the United States, after the President shall have declared by proclamation that the laws of the United States are opposed, and the execution thereof obstructed, by combinations too powerful to be suppressed by the ordinary course of judicial proceedings, or by the power vested in the marshals by law, any person, or his agent, attorney, or employee, purchases or acquires, sells or gives, any property of whatsoever kind or description, with intent to use or employ the same, or suffers the same to be used or employed in aiding, abetting, or promoting such insurrection or resistance to the laws, or any person engaged therein; or being the owner of any such property, knowingly uses or employs, or consents to such use or employment of the same, all such property shall be lawful subject of prize and capture wherever found; and it shall be the duty of the President to cause the same to be seized, confiscated, and condemned.

new agencies: the Office of Personnel Management, the Merit Systems Protection Board, and the Federal Labor Relations Authority, and that has taken over as a foreign controlled fourth branch of government unconstitutionally.

CONCLUSION

Petitioners have been here previously on a related election issue during the 2016 cycle, and to the extent that Christopher Blaise Garvey is now on the 2018 Ballot in New York for its Attorney General otherwise he would be here too. However in this 2018 cycle, we have exhausted our available remedies below in both the State and Federal civil system to no avail under the continuing emergency government, and because time is of the essence with imminent irreparable harm that will permanently impact the entirety of our fellow citizens of each of the States of the several States and the ability of the limited republic of the United States of America to continue, we beseech this Court for the good of the entire country to grant the relief sought; and to the extent that there are Five states in the U.S. — Louisiana, Georgia, South Carolina, New Jersey, and Delaware that run their elections using direct recording electronic machines (DREs) only each must be ordered under the Help America to Vote Act to provide Paper Ballots accordingly to serve our Commander-in Chief during this time of upheaval with the special notice to the danger posed by the warning given by The Hill shown at APX 331 that *Officials prepare for potential for claims of election interference*.

PETITION VERIFICATION AFFIDAVIT

STATE OF NEW YORK)
) SS.
COUNTY OF WARREN)

Accordingly, I, **Christopher Earl Strunk**, being duly sworn, depose and say under penalty of perjury:

I have read the foregoing Petition and Appendix Exhibits marked **APX 001** thru **APX 333** under 28 USC §1651 and related law for a writ of mandamus and injunctive equity relief pursuant to the national emergency mandate(s) issued by the commander-in-chief, Donald John Trump for an order:

A. TO PRESERVE, UNTIL FURTHER NOTICE BY THIS COURT, ALL PAPER BALLOTS CAST ON 6 NOVEMBER 2018 BY U.S. CITIZEN VOTERS AT THE NATIONAL MID-TERM GENERAL ELECTION IN THE STATE OF NEW YORK AND THE SEVERAL STATES AND TERRITORIES; AND
B. TO CONVENE A TITLE 10 §935. ART. 135. COURT OF INQUIRY INTO FOREIGN MEDDLING DURING THE 6 NOVEMBER 2018 ELECTION CYCLE; AND
C. TO ISSUE A REPORT FOR THE DEPARTMENT OF HOMELAND SECURITY SECRETARY KIRSTJEN M. NIELSEN; AND FOR
D. SUCH OTHER AND DIFFERENT RELIEF DEEMED NECESSARY.

Whereas affirmant Petitioner is an Accuser defined by 10 USC 801-9 for offenses against nationals of the United States outside the jurisdiction of any nation defined by 18 USC §7 -7 as if for special maritime and territorial jurisdiction of the United States using Court Rule 67(c) as to *Civil Affairs* under the 12 USC §95(a) amended 50 USC App. §5(b) ongoing emergency with the Military Government U.S. Army duties in the Community under the Honorable Donald J. Trump POTUS / Commander-in-Chief (CINC), as is defined by the U.S. Army Field Manual (FM) now amended into *Civil Affairs Operations* FM 3-57 dated 31 October 2011 applies with Chapter 4 Section 52 as to the civilian event of the early voting ongoing mid-term "elections" with the deadline of 6 November 2018 that affect military operations CINC warned of with the 12 September 2018 *Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election Certain Sanctions in the Event of Foreign Interference in a United States Election* and that time is of the essence with imminent irreparable harm; and

Affirmant knows the contents thereof apply to me by misapplication and administration of laws and that the same is true to my own knowledge, except as to the matters therein stated to be alleged on information and belief, and as to those matters I believe it to be true, am available for testimony. The grounds of my beliefs as to all matters not stated upon information and belief are as follows: 3rd parties, books and records, and personal knowledge.

Christopher Earl Strunk in esse Sui juris
All Rights Reserved Without Prejudice

Subscribed and Sworn to before me
This 25th day of October 2018

Notary Public

KIMBERLY A. ROSS
Notary Public, State of New York
Warren Co. #01RO6303916
Commission Expires May 19, 2021

PETITION VERIFICATION AFFIDAVIT

STATE OF NEW YORK)
) SS.
COUNTY OF ULSTER)

Accordingly, I, **Harold William Van Allen**, being duly sworn, depose and say under penalty of perjury:

I have read the foregoing Petition and Appendix Exhibits marked **APX 001** thru **APX 333** under 28 USC §1651 and related law for a writ of mandamus and injunctive equity relief pursuant to the national emergency mandate(s) issued by the commander-in-chief, Donald John Trump for an order:

A. TO PRESERVE, UNTIL FURTHER NOTICE BY THIS COURT, ALL PAPER BALLOTS CAST ON 6 NOVEMBER 2018 BY U.S. CITIZEN VOTERS AT THE NATIONAL MID-TERM GENERAL ELECTION IN THE STATE OF NEW YORK AND THE SEVERAL STATES AND TERRITORIES; AND
B. TO CONVENE A TITLE 10 §935. ART. 135. COURT OF INQUIRY INTO FOREIGN MEDDLING DURING THE 6 NOVEMBER 2018 ELECTION CYCLE; AND
C. TO ISSUE A REPORT FOR THE DEPARTMENT OF HOMELAND SECURITY SECRETARY KIRSTJEN M. NIELSEN; AND FOR
D. SUCH OTHER AND DIFFERENT RELIEF DEEMED NECESSARY.

Whereas affirmant Petitioner is an Accuser defined by 10 USC 801-9 for offenses against nationals of the United States outside the jurisdiction of any nation defined by 18 USC §7 -7 as if for special maritime and territorial jurisdiction of the United States using Court Rule 67(c) as to *Civil Affairs* under the 12 USC §95(a) amended 50 USC App. §5(b) ongoing emergency with the Military Government U.S. Army duties in the Community under the Honorable Donald J. Trump POTUS / Commander-in-Chief (CINC), as is defined by the U.S. Army Field Manual (FM) now amended into *Civil Affairs Operations* FM 3-57 dated 31 October 2011 applies with Chapter 4 Section 52 as to the civilian event of the early voting ongoing mid-term "elections" with the deadline of 6 November 2018 that affect military operations CINC warned of with the 12 September 2018 *Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election Certain Sanctions in the Event of Foreign Interference in a United States Election* and that time is of the essence with imminent irreparable harm; and

Affirmant knows the contents thereof apply to me by misapplication and administration of laws and that the same is true to my own knowledge, except as to the matters therein stated to be alleged on information and belief, and as to those matters I believe it to be true, am available for testimony. The grounds of my beliefs as to all matters not stated upon information and belief are as follows: 3rd parties, books and records, and personal knowledge.

Harold William Van Allen in esse Sui juris
All Rights Reserved Without Prejudice

Subscribed and Sworn to before me
This 25 day of October 2018

Fairlene A. Rabenda

Notary Public STATE OF NEW YORK
FAIRLENE G. RABENDA
QUALIFIED IN DUTCHESS COUNTY
REG #01RA5061914 COMMISSION EXPIRES JUNE 17, 2022

10287 words

CERTIFICATE OF COMPLIANCE

No. _____

UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

In re: Christopher Earl Strunk, and Harold William Van Allen,
Petitioners.

As required by Rule , the Undersigned certifies that the PETITION WITH 28 USC §1651 FOR WRIT OF MANDAMUS AND INJUNCTION EQUITY RELIEF IN THE MATTER OF FOREIGN MEDDLING DURING THE 6 NOVEMBER 2018 ELECTION CYCLE; contains 10287 words including the Petition Text and Footnotes, excluding the parts of the petition that are exempted by rules, and uses Times New Roman font with 14 Point type in the Text and 12 Point type in Footnotes.

The undersigned states and declares under penalty of perjury that the foregoing is true and correct under 28 USC §1746:

Dated: October 27, 2018
Brooklyn, New York

Christopher Earl Strunk in esse Sui juris,
141 Harris Avenue Lake Luzerne, NY 12846
Ph: 518-416-8743; Email: chris@privateamerciancitizen.org
All Rights Reserved Without Prejudice

UNITED STATES COURT OF APPEALS FOR THE ARMED FORCES

In re: Christopher Earl Strunk, and Harold William Van Allen,

Petitioners.

APPENDIX

FOR THE PETITION WITH 28 USC §1651 FOR A WRIT OF MANDAMUS AND INJUNCTIVE EQUITY RELIEF PURSUANT TO THE NATIONAL EMERGENCY MANDATE(S) ISSUED BY THE COMMANDER-IN-CHIEF, DONALD JOHN TRUMP

EXECUTIVE ORDERS

Executive Order on Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election

— FOREIGN POLICY

Issued on: **September 12, 2018**

★ ★ ★

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that the ability of persons located, in whole or in substantial part, outside the United States to interfere in or undermine public confidence in United States elections, including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation, constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States. Although there has been no evidence of a foreign power altering the outcome or vote tabulation in any United States election, foreign powers have historically sought to exploit America's free and open political system. In recent years, the proliferation of digital devices and internet-based communications has created significant vulnerabilities and magnified the scope and intensity of the threat of foreign interference, as illustrated in the 2017 Intelligence Community Assessment. I hereby declare a national emergency to deal with this threat.

Accordingly, I hereby order:

Section 1. (a) Not later than 45 days after the conclusion of a United States election, the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies (agencies), shall conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in that election. The assessment shall identify, to the maximum extent ascertainable, the nature of any foreign interference and any methods employed to execute it, the persons involved, and the foreign government or governments that authorized, directed, sponsored, or supported it. The Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, and the Secretary of Homeland Security.

(b) Within 45 days of receiving the assessment and information described in section 1(a) of this order, the Attorney General and the Secretary of Homeland Security, in consultation with the heads of any other appropriate agencies and, as appropriate, State and local officials, shall deliver to the President, the Secretary of State, the Secretary of the Treasury, and the Secretary of Defense a report evaluating, with respect to the United States election that is the subject of the assessment described in section 1(a):

(i) the extent to which any foreign interference that targeted election infrastructure materially affected the security or integrity of that infrastructure, the tabulation of votes, or the timely transmission of election results; and

(ii) if any foreign interference involved activities targeting the infrastructure of, or pertaining to, a political organization, campaign, or candidate, the extent to which such activities materially affected the security or integrity of that infrastructure, including by unauthorized access to, disclosure or threatened disclosure of, or alteration or falsification of, information or data.

The report shall identify any material issues of fact with respect to these matters that the Attorney General and the Secretary of Homeland Security are unable to evaluate or reach agreement on at the time the report is submitted. The report shall also include updates and recommendations, when appropriate, regarding remedial actions to be taken by the United States Government, other than the sanctions described in sections 2 and 3 of this order.

(c) Heads of all relevant agencies shall transmit to the Director of National Intelligence any information relevant to the execution of the Director's duties pursuant to this order, as appropriate and consistent with applicable law. If relevant information emerges after the submission of the report mandated by section 1(a) of this order, the Director, in consultation with the heads of any other appropriate agencies, shall amend the report, as appropriate, and the Attorney General and the Secretary of Homeland Security shall amend the report required by section 1(b), as appropriate.

(d) Nothing in this order shall prevent the head of any agency or any other appropriate official from tendering to the President, at any time through an appropriate channel, any analysis, information, assessment, or evaluation of foreign interference in a United States election.

(e) If information indicating that foreign interference in a State, tribal, or local election within the United States has occurred is identified, it may be included, as appropriate, in the assessment mandated by section 1(a) of this order or in the report mandated by section 1(b) of this order, or submitted to the President in an independent report.

(f) Not later than 30 days following the date of this order, the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence shall develop a framework for the process that will be used to carry out their respective responsibilities pursuant to this order. The framework, which may be classified in whole or in part, shall focus on ensuring that agencies fulfill their responsibilities pursuant to this order in a manner that maintains methodological consistency; protects law enforcement or other sensitive information and intelligence sources and methods; maintains an appropriate separation between intelligence functions and policy and legal judgments; ensures that efforts to protect electoral processes and institutions are insulated from political bias; and respects the principles of free speech and open debate.

Sec. 2. (a) All property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person of the following persons are blocked and may not be transferred, paid, exported, withdrawn, or otherwise dealt in: any foreign person determined by the Secretary of the Treasury, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security:

(i) to have directly or indirectly engaged in, sponsored, concealed, or otherwise been complicit in foreign interference in a United States election;

(ii) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, any activity described in subsection (a)(i) of this section or any person whose property and interests in property are blocked pursuant to this order; or

(iii) to be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property or interests in property are blocked pursuant to this order.

(b) Executive Order 13694 of April 1, 2015, as amended by Executive Order 13757 of December 28, 2016, remains in effect. This order is not intended to, and does not, serve to limit the Secretary of the Treasury's discretion to exercise the authorities provided in Executive Order 13694. Where appropriate, the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, may exercise the authorities described in Executive Order 13694 or other authorities in conjunction with the Secretary of the Treasury's exercise of authorities provided in this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this order.

Sec. 3. Following the transmission of the assessment mandated by section 1(a) and the report mandated by section 1(b):

(a) the Secretary of the Treasury shall review the assessment mandated by section 1(a) and the report mandated by section 1(b), and, in consultation with the Secretary of State, the Attorney General, and the Secretary of Homeland Security, impose all appropriate sanctions pursuant to section 2(a) of this order and any appropriate sanctions described in section 2(b) of this order; and

(b) the Secretary of State and the Secretary of the Treasury, in consultation with the heads of other appropriate agencies, shall jointly prepare a recommendation for the President as to whether

additional sanctions against foreign persons may be appropriate in response to the identified foreign interference and in light of the evaluation in the report mandated by section 1(b) of this order, including, as appropriate and consistent with applicable law, proposed sanctions with respect to the largest business entities licensed or domiciled in a country whose government authorized, directed, sponsored, or supported election interference, including at least one entity from each of the following sectors: financial services, defense, energy, technology, and transportation (or, if inapplicable to that country's largest business entities, sectors of comparable strategic significance to that foreign government). The recommendation shall include an assessment of the effect of the recommended sanctions on the economic and national security interests of the United States and its allies. Any recommended sanctions shall be appropriately calibrated to the scope of the foreign interference identified, and may include one or more of the following with respect to each targeted foreign person:

(i) blocking and prohibiting all transactions in a person's property and interests in property subject to United States jurisdiction;

(ii) export license restrictions under any statute or regulation that requires the prior review and approval of the United States Government as a condition for the export or re-export of goods or services;

(iii) prohibitions on United States financial institutions making loans or providing credit to a person;

(iv) restrictions on transactions in foreign exchange in which a person has any interest;

(v) prohibitions on transfers of credit or payments between financial institutions, or by, through, or to any financial institution, for the benefit of a person;

(vi) prohibitions on United States persons investing in or purchasing equity or debt of a person;

(vii) exclusion of a person's alien corporate officers from the United States;

(viii) imposition on a person's alien principal executive officers of any of the sanctions described in this section; or

(ix) any other measures authorized by law.

Sec. 4. I hereby determine that the making of donations of the type of articles specified in section 203(b)(2) of IEEPA (50 U.S.C. 1702(b)(2)) by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order would seriously impair my ability to deal with the national emergency declared in this order, and I hereby prohibit such donations as provided by section 2 of this order.

Sec. 5. The prohibitions in section 2 of this order include the following:

(a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any person whose property and interests in property are blocked pursuant to this order; and

(b) the receipt of any contribution or provision of funds, goods, or services from any such person.

Sec. 6. I hereby find that the unrestricted immigrant and nonimmigrant entry into the United States of aliens whose property and interests in property are blocked pursuant to this order would be detrimental to the interests of the United States, and I hereby suspend entry into the United States, as immigrants or nonimmigrants, of such persons. Such persons shall be treated as persons covered by section 1 of Proclamation 8693 of July 24, 2011 (Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions).

Sec. 7. (a) Any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order is prohibited.

(b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.

Sec. 8. For the purposes of this order:

(a) the term "person" means an individual or entity;

(b) the term "entity" means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(c) the term "United States person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person (including a foreign person) in the United States;

(d) the term "election infrastructure" means information and communications technology and systems used by or on behalf of the Federal Government or a State or local government in managing the election process, including voter registration databases, voting machines, voting tabulation equipment, and equipment for the secure transmission of election results;

(e) the term "United States election" means any election for Federal office held on, or after, the date of this order;

(f) the term "foreign interference," with respect to an election, includes any covert, fraudulent, deceptive, or unlawful actions or attempted actions of a foreign government, or of any person acting as an agent of or on behalf of a foreign government, undertaken with the purpose or effect of influencing, undermining confidence in, or altering the result or reported result of, the election, or undermining public confidence in election processes or institutions;

(g) the term "foreign government" means any national, state, provincial, or other governing authority, any political party, or any official of any governing authority or political party, in each case of a country other than the United States;

(h) the term "covert," with respect to an action or attempted action, means characterized by an intent or apparent intent that the role of a foreign government will not be apparent or acknowledged publicly; and

(i) the term "State" means the several States or any of the territories, dependencies, or possessions of the United States.

Sec. 9. For those persons whose property and interests in property are blocked pursuant to this order who might have a constitutional presence in the United States, I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in this order, there need be no prior notice of a listing or determination made pursuant to section 2 of this order.

Sec. 10. Nothing in this order shall prohibit transactions for the conduct of the official business of the United States Government by employees, grantees, or contractors thereof.

Sec. 11. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President by IEEPA as may be necessary to carry out the purposes of this order. The Secretary of the Treasury may re-delegate any of these functions to other officers within the Department of the Treasury consistent with applicable law. All agencies of the United States Government are hereby directed to take all appropriate measures within their authority to carry out the provisions of this order.

Sec. 12. The Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, is hereby authorized to submit the recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 13. This order shall be implemented consistent with 50 U.S.C. 1702(b)(1) and (3).

Sec. 14. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

DONALD J. TRUMP

THE WHITE HOUSE,

Americans for Innovation™

To ensure you are reading the latest post, click the logo above.
SEARCH by topic, keyword or phrase. Type in Custom Search box e.g. "IBM Eclipse Foundation" or "racketeering"

Custom Search

Friday, March 16, 2018

OBAMA HIRED THEM. TRUMP CANNOT FIRE THEM. SO THEY SAY.

Senior Executive Service (SES) is ~10,000 Deep State shadow government employees who are sabotaging the American Republic for the globalist agenda

Download, study and share the "Crimeline" widely

CONTRIBUTING WRITERS | OPINION | *AMERICANS FOR INNOVATION* | MAR. 16, 2018, UPDATED APR. 16, 2018 | PDF | https://tinyurl.com/y9nughht

Fig. 1—The Untouchables. https://youtu.be/IFFnT9JaG2g | Raw *.mp4 video file

Video: American Intelligence Media, Americans for Innovation, Leader Technologies, Inc.

Se

DEEP STATE SHADOW GOVERNMENT POSTER

Member

Harvard | Yale | Stanford Sycophants

Bookmark: #stand-with-roger-stone

ROGER STONE SPEAKS: On Nov. 18, 2017, Twitter censored *New York Times* best-selling author Roger Stone completely. Every red-blooded American should be outraged, Republican, Democrat and Independent alike. If Roger's voice is silenced today, yours is next. We must *break* this embargo. Click here to read and share Roger's latest perspectives on the Battle for our Republic, including his responses to his critics (who have not been censored).

Updated Oct. 10, 2018.

CLICK HERE TO SEE COMBINED TIMELINE OF THE HIJACKING OF THE INTERNET

PAY-to-PLAY NEW WORLD ORDER

This timeline shows how insiders sell access & manipulate politicians, police, intelligence, judges and media to keep their secrets

Clintons, Obamas, Summers were paid in cash for outlandish speaking fees and Foundation donations. Sycophant judges, politicians, academics, bureaucrats and media were fed tips to mutual funds tied to insider stocks like Facebook. Risk of public exposure, blackmail, pedophilia, "snuff parties" (ritual child sexual abuse and murder) and Satanism have ensured silence among pay-to-play beneficiaries. The U.S. Patent Office is their toy box from which to steal new ideas.

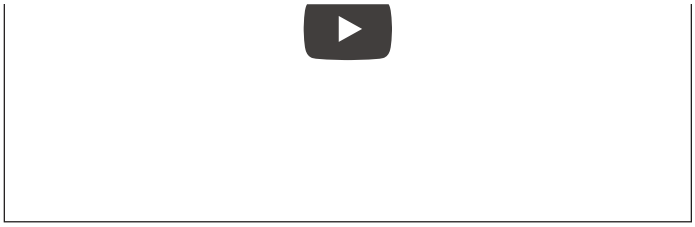


Fig. 2—Shadow Government is Collapsing. https://youtu.be/e2usmlq7oFE

Video: American Intelligence Media, Americans for Innovation, Leader Technologies, Inc.

Fig. 3—The American SS Exposed. https://youtu.be/hSvSqvFwfUk | Raw *.mp4 video file

Video: American Intelligence Media, Americans for Innovation, Leader Technologies, Inc.

Fig. 4—SeS Governing Council 500 Exposed. https://youtu.be/mZKTWjORitI | Raw *.mp4 video file

Video: American Intelligence Media, Americans for Innovation, Leader Technologies, Inc.

Bookmark: #new-ses-documents | https://tinyurl.com/yc3p8jyj

BREAKING MAR. 20, 2018

DEVASTATING SES / SERCO DOCUMENTS POURING IN FROM ANONYMOUS SOURCES

Americans for Innovation and *American Intelligence Media* are currently receiving a **devastating collection of SES documents** that prove the decades of treachery against the

G+

CONGRESS CONTACT LOOKUP

Contacting the Congress

= Universal Toxic Substance Symbol & Warning

FINANCIAL HOLDINGS OF OBAMA POLITICAL APPOINTEES, BY AGENCY

FOLLOW BY EMAIL

Email address... Submit

BLOG ARCHIVE

▼ 2018 (17)
- ► October (1)
- ► September (1)

American taxpayer by our government institutions themselves. *Since such documents have a way of disappearing magically, we strongly request that readers IMMEDIATELY download these documents and distribute them onto multiple computers so that they will not disappear. The site has a ZIP download button in the upper right hand corner. This is a compressed package of the entire set of documents in one file. Your techie friends will be able to unzip it, so download it even if you are not familiar with ZIP.* The number of documents appears to be growing daily. The SES documents contain names, dates, titles and events—all actionable and potentially indictable evidence.

Senior Executive Service (SES) Flag with Nazi Waffen SS logo superimposed. Click here for new document collection emerging.

Download SES files

Download as ZIP

305 MB, be patient!

Download SERCO files

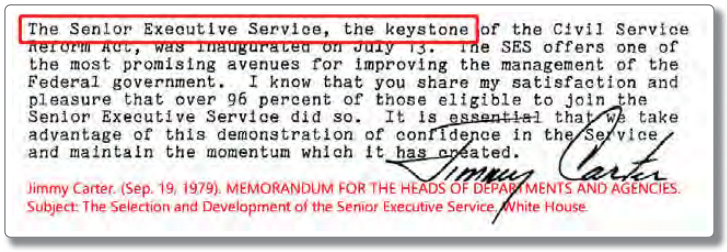
Download as ZIP

141 MB, be patient!

(MAR. 16, 2018)—The Senior Executive Services (SES) was created as Title IV in the Civil Rights Reform Act of 1978 under President Jimmy Carter.

The Act reformed the civil service of the federal government, partly in response to the Watergate scandal. It abolished the U.S. Civil Service Commission and distributed its functions primarily among four new agencies: the Office of Personnel Management (OPM), the Merit Systems Protection Board (MSPB), the Federal Labor Relations Authority (FLRA) and the Senior Executive Service (SES).

On Sep. 19, 1979, President Carter called SES "the keystone of the Civil Service Reform Act." Tellingly, Wikipedia describes it as an also-ran program. Also-ran or keystone? It cannot be both. President Carter's statement stands in stark contrast to the program's TOTAL lack of transparency and the public's total lack of awareness of its existence. Keystone for what? Hindsight provides the answer: racketeering, theft, obstruction of justice, conspiracy, fraud, treason and sedition.



The Senior Executive Service, the keystone of the Civil Service Reform Act, was inaugurated on July 13. The SES offers one of the most promising avenues for improving the management of the Federal government. I know that you share my satisfaction and pleasure that over 96 percent of those eligible to join the Senior Executive Service did so. It is essential that we take advantage of this demonstration of confidence in the Service and maintain the momentum which it has created.

Jimmy Carter

Jimmy Carter. (Sep. 19, 1979). MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES. Subject: The Selection and Development of the Senior Executive Service. White House.

- August (2)
- July (1)
- June (1)
- May (1)
- April (1)
- March (3)
  - OBAMA HIRED THEM. TRUMP CANNOT FIRE THEM. SO THEY ...
  - SPECIAL COUNSEL LEGAL AUTHORITY IS ILLEGITIMATE
  - THE TIMELINE OF EVIL GOES VIRAL
- February (3)
- January (3)
- 2017 (27)
- 2016 (39)
- 2015 (34)
- 2014 (26)
- 2013 (28)
- 2012 (6)

UPDATE MAR. 25, 2014

FIVE CRITICAL AFI POSTS ON JUDICIAL COMPROMISE

Fully updated Mar. 25, 2014 in the wake of the Scribd censorship:

1. **HOW PATENT JUDGES GROW RICH ON THE BACKS OF AMERICAN INVENTORS**

   Patent Office filings are shuffled out the USPTO backdoor to crony lawyers, banks and deep-pocket clients.
2. **WAS CHIEF JUSTICE ROBERTS BLACKMAILED** into supporting Obamacare by his ethical compromises in *Leader v. Facebook*?
3. **JUSTICE ROBERTS MENTORED**

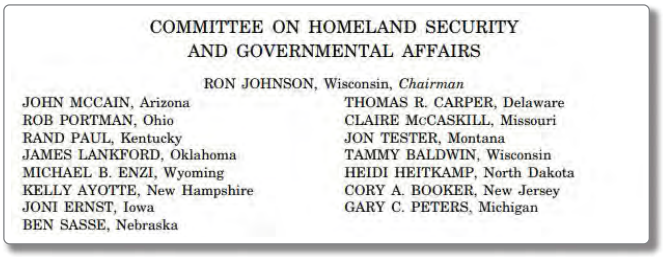
   Facebook Gibson Dunn LLP attorneys.
4. **JUSTICE ROBERTS HOLDS** substantial Facebook financial interests.
5. **JUDGE LEONARD STARK FAILED** to disclose his Facebook financial interests and his reliance on Facebook's Cooley Godward LLP attorneys for his appointment.

BARACK OBAMA'S DARK POOLS OF CORRUPTION

SES statement to Congress on Dec. 01, 2016, Appendix 2, last paragraph, PDF p. 228, "*Appointments to SES Positions*":

> "By law, the appointment or removal" of SES positions "shall not be subject, directly or indirectly to review or approval by an officer or entity within the Executive Office of the President." (*Is this not sedition?*)

Note: This SES statement was *endorsed* by the following Senators. Did they know what they were endorsing? Somebody needs to give at least Sen. Rand Paul a heads up because we cannot imagine that he knows about the SES' control of the NSA, who he has sued for its unchecked mass surveillance of American citizens in clear violation of the Fourth Amendement.



COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

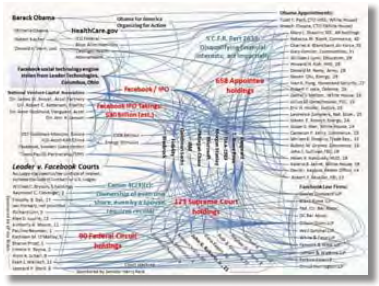
JOHN MCCAIN, Arizona	THOMAS R. CARPER, Delaware
ROB PORTMAN, Ohio	CLAIRE McCASKILL, Missouri
RAND PAUL, Kentucky	JON TESTER, Montana
JAMES LANKFORD, Oklahoma	TAMMY BALDWIN, Wisconsin
MICHAEL B. ENZI, Wyoming	HEIDI HEITKAMP, North Dakota
KELLY AYOTTE, New Hampshire	CORY A. BOOKER, New Jersey
JONI ERNST, Iowa	GARY C. PETERS, Michigan
BEN SASSE, Nebraska	

Let's get this straight. A Senate Committee that oversees the Department of Homeland Security—an agency of the Executive Branch, is telling the American People that the hiring and firing function of the SES—also an agency within the Executive Branch, is not subject to the Executive Branch in its hiring and firing of personnel? Are you kidding me? Is this not the very definiton of *sedition*. This is proof of a shadow government in the Congressional record.

Who knows anything about the SES? Almost nobody. It is the world's best kept secret. The SES are 8-10,000 highly paid federal bureaucrats who *grease the skids for the Deep State shadow government*. In short, they help insure that government corruption remains a perennially lucrative enterprise, free of the knowledge of, or reprisals from We The People.

The Title IV Senior Executive Service was sold to the public as a way to get experienced private sector executives to work for the federal government. The truth has been that corporate executives put their people in place at the SES, then those SES people feed contracts to their private sector cronies. In short, SES is the administrative arm of a fascist system where selected corporations profit as long as they do the bidding of their Deep State handlers.

Click to enlarge

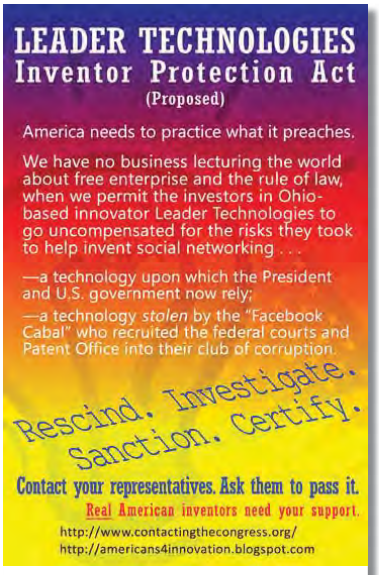


CLICK HERE FOR WASHINGTON'S ETHICAL DISEASE DISCOVERIES RE. FACEBOOK "DARK POOLS"

STOP FACEBOOK PROPERTY THEFT

WILL HUMANKIND EVER LEARN? Facebook's Orwellian doublespeak about property and privacy (theft) merely repeats the eventual dehumanization of the individual under MAO's Red Star, Stalin's SOVIET Hammer & Cycle and Hitler's NAZI Swastika. Respect for the inalienable rights of each individual is a bedrock value of democracy. The members of the Facebook Cabal abuse this principle at every opportunity. They evidently believe that they deserve special privileges and are willing to lie, cheat and steal in order to treat themselves to these privileges.

ASK CONGRESS: PASS THE INVENTOR PROTECTION ACT!



Click image above to download a poster-quality PDF optimized for a 11in. x 17in. (ledger-size) poster. America should not be in the business of cheating its entrepreneurial investors simply because the cheaters buy off judges with the money gained from their theft. Such permissiveness is obscene.

The SES was championed and organized by Kristine Marcy (nee McConnell)—a close companion and decades-long co-conspirator with the Clintons.

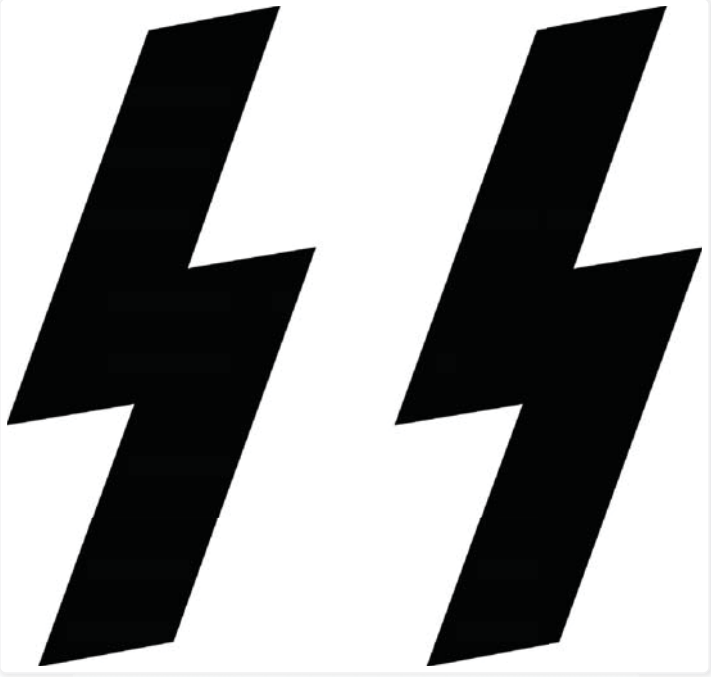
Marcy's brother, Field McConnell, is a retired pilot who flew fighter jets for the Navy, Air Force, Marines and National Guard. He also piloted commercial aircraft for Southern, Republic and Northwest Airlines.

McConnell was the first to discover a Boeing uninterruptible autopilot that could remotely take over or crash an airplane. His reporting to Boeing, FAA and the Defense Department have been aggressively suppressed, yet McConnell continues to speak out boldly.

See AFI. (Jan. 11, 2018). Meet The Person Who Can Remotely Crash Planes And Can Read Your Mind. *Americans for Innovation*.

McConnell and sister Marcy are estranged and he has publicly exposed his sister's treacherous conspiracies with Hillary and Bill Clinton to undermine our Republic.

Hindsight shows the SES to be little more than the spiritual children of the Nazi SS—the administrative shock troops of the rogue C.I.A. Deep State shadow government.



Every four years the SES publishes a "Plum Book" (named for its purple cover sheet). It lists the executives in each federal department and agency and their compensation, or at least it is

LEADER V. FACEBOOK BACKGROUND

Jul. 23, 2013 NOTICE: DonnaKlineNow! has gone offline. All her posts are available as a PDF collection here (now updated, post-Scribd censorship).

Mar. 20, 2014 READER NOTICE: On Mar. 7, 2014, all of our documents linked to Scribd were deleted by that "cloud" service using the flimsiest of arguments . Some of our documents have been there for two years and some had almost 20,000 reads.

George Orwell wrote in *1984* that one knows one is in a totalitarian state when telling the truth becomes an act of courage.

All the links below were updated Mar. 20, 2014 (many thanks to our volunteers!)

1. Summary of Motions, Appeal, Petition, Evidence, Analysis, Briefings (FULL CITATIONS) in *Leader Technologies, Inc. v. Facebook, Inc.*, 08-cv-862-JJF-LPS (D. Del. 2008), published as *Leader Techs, Inc. v. Facebook, Inc.*, 770 F. Supp. 2d 686 (D. Del. 2001)

2. Dr. Lakshmi Arunachalam's Censored Federal Circuit Filings (Archive)
3. Brief Summary of *Leader v. Facebook*
4. Backgrounder
5. Fenwick & West LLP Duplicity
6. Instagram-scam
7. USPTO-reexam Sham
8. Zynga-gate
9. James W. Breyer / Accel Partners LLP Insider Trading
10. Federal Circuit Disciplinary Complaints
11. Federal Circuit Cover-up
12. Congressional Briefings re. Leader v. Facebook judicial corruption
13. Prominent Americans Speak Out
14. Petition for Writ of Certiorari
15. Two Proposed Judicial Reforms
16. S. Crt. for Schemers or Inventors?
17. Attorney Patronage Hijacked DC?

18. Justice Denied | Battle Continues
19. FB Robber Barons Affirmed by S. Crt.
20. Judicial Misconduct WALL OF SHAME
21. Corruption Watch - "Oh what webs we weave, when first we practice to deceive"
22. Facebook | A Portrait of Corruption
23. White House Meddling
24. Georgia! AM 1080 McKibben Interview
25. Constitutional Crisis Exposed
26. Abuse of Judicial Immunity since *Stump*

supposed to. As you can see, numerous compensation amounts are blank.

We have located and compiled these 220-426 page reports. In addition, we have prepare Excel spreadsheets for the number of SES-related jobs by department and agency.

Today, SES and associated positions account for 9,033 employees across 166 departments and agencies at above the highest pay rates in government. Note the dramatic increase in the new job title "Inspector General" during Barack Obama's eight years. Evidently, Obama's SES Army installed a **buffer** between their Deep State shadow government handlers and the Law if they ran into legal trouble or got caught—more "insurance." (FBI counterterrorism director Peter P. Strzok secret text message to paramore FBI senior counsel Lisa C. Page).

Bookmarks: #ses-plum-books-1996-2016 | #barack-obama-treason

We encourage other patriots to download these files and set up a *searchable web folder* with a single search utility we can all share and embed in our various blogs and sites. This evidence has a way of disappearing inexplicably.

SEARCH SES EMPLOYEE ROSTERS IN THE TABLE BELOW

These SES employee disclosure files at the Federal Register are *intentionally broken* for searching. Google will normally index an entire PDF document unless blocked by the creator's intent. Engineers have discovered special characters embedded in the fonts themselves (not visible to the naked eye) that block web crawlers from searching and indexing the pages. Therefore, the names will not appear in Google / Bing / Yahoo / DuckDuckGo search results. More on this later. Therefore, these disclosure documents are not transparent. However, *Adobe Reader and Acrobat are able to search for individual names*. To use Advanced Search, choose the PDF file of interest. Select **Edit | Advanced Search** in the Adobe menu line. Type your keyword or phrase and view the list of all occurences in the search panel. *See* also Searching PDFs for full help.

Also, the Plum Books are not comprehensive lists of SES members. For example, the current Secret Service Special Agent in Charge in San Francisco CA, David Murray, advertises himself on LinkedIn as SES, yet neither Murray's name, nor the Secret Service in general, appear anywhere on the Congressional reports that we could find—which is obviously not a secret since he publishes it freely on LinkedIn.

Senior Executive Service (SES) "Plum Book" Policy and Supporting Positions published by various House and Senate Committees Updated Mar. 30,2018

President	*Reporting Year*	*SES Plum Book* Be Patient on downloads, these are large files	*Positions*	*Depts. & Agencies*	*Inspectors General (Deep State shadow gov't buffers)*	*Agency/Dept. Summary Spreadsheet*

Search Note: The versions of these documents at the Federal Register and GoogleDocs/GoogleDrive contain search blocks that prevent all the names in these documents from appearing on searches and being indexed by web search crawlers. We are unpacking these files and removing those booby traps. So, just because a name does not appear the first time you search, do not assume it is not there. It may have been intentionally rendered unsearchable. We are receiving many reports from whistleblowers that these official SES lists are not

27. Obamacare Scandal Principals are intertwined in the Leader v. Facebook scandal
28. S.E.C. duplicity re. Facebook

GIBSON DUNN LLP exposed as one of the most corrupt law firms in America

Investigative Reporter Julia Davis investigates **Facebook's *Leader v. Facebook* attorney Gibson Dunn LLP**. She credits this firm with the reason why not a single Wall Street banker has gone to jail since 2008. **Click here** to read her article "Everybody hates whistleblowers." *Examiner.com*, Apr. 10, 2012. Here's an excerpt:

> "Skillful manipulation of the firm's extensive media connections allows Gibson Dunn to promote their causes, while simultaneously smearing their opponents and silencing embarrassing news coverage."

This statement followed right after Davis cited Facebook's chief inside counsel in the *Leader v. Facebook* case, Theodore Ullyot, who appears to have helped lead the *Leader v. Facebook* judicial corruption. Interesting word choices associated with Gibson Dunn LLP: manipulation, smear. Attorneys swear a solemn oath to act morally, ethically, and in support of democratic principles. They promise to conduct themselves in a manner than instills confidence among the citizenry in the rule of law and the judicial system. These promises appear to be meaningless. **Click here** for a PDF version of Julie Davis' article.

POPULAR POSTS

OBAMA HIRED THEM. TRUMP CANNOT FIRE THEM. SO THEY SAY.
Senior Executive Service (SES) is ~10,000 Deep State shadow government employees who are sabotaging the American Republic for the globali...

PROOF: ROBERT MUELLER CANNOT BE IMPARTIAL IN THE RUSSIA INVESTIGATION
Mueller's Deep State relationships will politicize the FBI yet again
Contributing Writers | Opinion | AMERICANS FOR INNOVATION | ...

LEADER TECHNOLOGIES FILES TRILLION DOLLAR BOND LIEN ON THE U.S. GOVERNMENT
President Trump is asked to compensate Leader for the theft of their inventions by the Deep State shadow government Leader's social net...

comprehensive and are only the "tip of the iceberg" of total SES federal employees. Reading between the lines of their disclosure rules, SES has dozens of ways of making people's names and salaries secret, and as they say in every document, they cannot be hired or fired by the President (that statement is usually the last paragraph of APPENDIX NO. 2).
Bookmark: #ses-obfuscation-blizzard | https://tinyurl.com/yanznx2n

NEW! ANALYSIS (100 hrs. unpacking the Plum Books): Anonymous Patriots. (Apr. 04, 2018). Plum Books hide SES employees in a blizzard of bad math and contradictory, nonsensical categories. *American Intelligence Media.*

EXPERT CONCLUSION: *Everyone* in the Plum Book is SES, whether directly designated or secretly associated by convoluted policies.

Jimmy Carter	1980	PDF		8,600		18	
Ronald Reagan	1984	PDF		8,000		20	
	1988	PDF		8,000		14	
George H.W. Bush	1992	PDF		8,600		12	
Bill Clinton	1996	PDF		7,303	104	30	XLSX
	2000	PDF	DOCX	7,323	115	?	XLSX
George W. Bush	2004	PDF	DOCX	9,357	119	?	XLSX
	2008	PDF	DOCX	8,221	115	?	XLSX
Barack Obama	2012	PDF	DOCX	11,392	164	25	XLSX
	2016	PDF	DOCX	9,033	166	25	XLSX
		Standing SES (DOJ) Performance Review Boards*					
		Fed. Reg. PDF*	Declawed PDF*	500	Office of Attorney General	DOJ SeS 500 - DOJ Paymasters HTML	Declawed XLSX*
Various	1979-	SITE		NSA, CIA, DTIC, DOD			
Various	Various	ZIP		SERCO British/Int'l arm of SES (has controlled the U.S. Patent Office since 2006)			

Table 1: Senior Executive Service (SES) Plum Book disclosing the U.S. shadow government. Click on any file. To search inside a file, click **Ctrl + F** (find) then type a search word or phrase. Or, select Edit | Advanced Search.

* This Federal Register file is *severely tampered with* to prevent search crawlers from indexing it, and even from normal cut and paste and file conversion actions. Essentially, it had to be retyped in order to strip out the embedded malware in the fonts themselves. This tampering hints at possible collusion with Microsoft and possibly Adobe to recognize hidden HEX characters inside certain fonts that automatically *junks up the text record,* thus preventing normal portability of the data to other programs. This one file took approx. 14 experienced man-hours to render it to full searchability. The effort to "hide this file in plain site" was evident to the engineers.

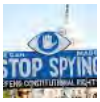
Fig. 5—Bill Valdez. (Dec. 07, 2017). 2017 Presidential Rank Awards Leadership Summit [Senior Executive Services (SES)], p. 31. Senior Executives Association.

LEADER PROPOSES TRILLION DOLLAR FED REVENUE WHILE LOWERING TAXES

User fee on social networking will generate $300+ billion a year to fund major initiatives Surcharge on social networking will pay for 17...

OHIO STATE'S PRESIDENT MICHAEL V. DRAKE MIRED IN PERSONAL CONFLICTS OF INTEREST

Trustees and Provost promote learning technology that benefits trustee clients and is stolen from OSU alums Contributing Writers | Opini...



AMERICAN MORAL UNDERPINNINGS ARE UNDER SIEGE BY GODLESS DEEP STATE CORPORATE GLOBALISTS

Trump under surveillance for many years MSM fake news is INTENDED to degrade our Republic Judeo-Christian moral values of our Founde...

HILLARY CLINTON CONTROLS 50,000 FBI ENCRYPTION KEYS—PROVES MUELLER'S WITCH HUNT IS TREASONOUS

With these encryption keys, nothing in our digital lives is off limits to the Clinton's and their conspirators President Trump's n...

MEET THE PERSON WHO CAN REMOTELY CRASH PLANES AND CAN READ YOUR MIND

Monstrous Patent calls people "wet ware" Implanted devices deliver electric shock, poisons, dopamine, adrenaline, emit mind control freq...

OSU BAND INVESTIGATION UNEARTHS SURPRISE TRUSTEE COLLUSION IN PATENT THEFT

Breaking News, Sep. 3, 2014 , 10:05am OSU Trustee President, Jeffrey Wadsworth, "counterattacks" the Band Alumni leadership T...

THE SHADOW GOVERNMENT USES SES, SERCO AND OPIC AS PORTALS INTO HORRIFIC CORRUPTION

These lawyers, bankers, academics, journalists, bureaucrats and self-styled elitists sponge off the actual wealth-creation of hard working ...

EDITORIALS

1. DC Bar refuses to investigate attorney misconduct in Leader v. Facebook - Unwillingness of DC attorneys to self-police may explain why Washington is broken, Dec. 30, 2012

2. Will the U.S. Supreme court support schemers or real American inventors? Facebook's case dangles on a doctored interrogatory. Eighteen (18) areas of

SES = SS ?

This comparison of the SES with the Nazi SS appears to be more than metaphorical.

The Church Committee (1976) revealed that the rogue C.I.A. imported tens of thousands of former Nazi executives to work with their secret American industry partners like IBM.

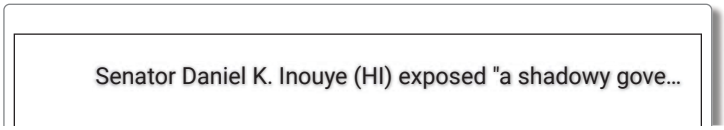
WHAT AVERAGE PERSON HAS THE TIME TO ENGAGE IN THIS SUSTAINED IMMORALITY?

I mean ask yourself, is it even reasonable to assume that there is so much seathing rage in the world that the following events have occurred spontaneously and without substantial financing by the rogue C.I.A. (SeS) who *has been proven* to be funding programs in population control (MKUltra), the space race (NASA, NRO), depopulation eugenics (Planned Parenthood), pedophilia, drug-sex-arms trafficking, money laundering, false flags to scare the public and enrich their hedge funds (Gulf of Tonkin, 911, 2008 Bank 'Crisis,' Rwanda, Kosovo, Syria, Libya, Lockerbie, Oklahoma City, Waco, Sandy Hook, Las Vegas, Parkland, etc.) and mass propaganda (CBS, NBC, ABC, CNN, MSNBC, New York Times, NPR, Washington Post), among others.

Senator F. Frank Church (D-Idaho) wrote in 1976 in his final Committee report which is posted on the Senate website:

> "Intelligence agencies have undermined the constitutional rights of citizens," the final report concluded, "primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied."

Clearly nothing had changed after 1976 because in 1987 Senator Daniel K. Inouye (D-Hawaii) continued to sound the alarm about the Deep State shadow government run by the rogue C.I.A. See video following:



question shout for attention, Dec. 27, 2012

3. Two Policy Changes That Will Make America More Democratic (and less contentious), Dec. 21, 2012

OUR MISSION

American citizens must fight abuse of the constitutional right for authors and inventors to enjoy the fruits of their inventions, as a matter of matter of basic property rights and sound public policy. Otherwise, instead of innovation, creativity, genius, ideas, vision, courage, entrepreneurship, respect, property, rejuvenation, morals, ethics, values, renewal, truth, facts, rights, privacy, solutions and judicial faithfulness,

. . . our society and economy will be dragged down (and eventually destroyed) by copying, infringement, thievery, counterfeiting, hacking, greed, misinformation, exploitation, abuse, waste, disrespect, falsity, corruption, bribery, coercion, intimidation, doublespeak, misconduct, lies, deception, attorney "dark arts," destruction, confusion, dishonesty, judicial chicanery and lawlessness.

If we do not speak up, impeach derelict judges and imprison corrupt attorneys, we cannot possibly hope to start fixing the current ills in our society. Without justice and respect for private property, democracy has no sure foundation.

CURRENT EDITORIAL FOCUS

We are an opinion blog that advocates for strong intellectual property rights. We welcome commenters and contributors. The *Leader v. Facebook* patent infringement case first came to our attention after learning that the trial judge, Leonard P. Stark, U.S. District Court of Delaware, ignored his jury's admission that they had no evidence to support their on-sale bar verdict, but the judge supported it anyway.

The judicial misconduct has deteriorated from there, replete with two of the three judges on the Federal Circuit appeal panel, Judges Alan D. Lourie and Kimberly A. Moore, holding Facebook stock that they did not disclose to the litigants, and later tried to excuse through a quick motion slipped in at the last minute by the Clerk of Court, Jan Horbaly, and his close friends at The Federal Circuit Bar Association. (The DC Bar subsequently revealed that Mr. Horbaly is not licensed to practice law in Washington D.C.)

The judges ignored shocking new evidence that Mark Zuckerberg withheld 28 hard drives of 2003-2004 evidence from Leader Technologies that could prove actual theft (and therefore claims even more serious than infringement). In addition, Facebook's appeal attorney, Thomas G. Hungar of Gibson Dunn LLP, has close personal ties to just about every judicial player in this story. The misconduct appears to reach into the U.S. Patent Office through abuse of the

Fig. 6—Senator Daniel Inouye (D-HI) exposed "a shadowy goverment" in 1987. This speech was given just nine years after the Senior Executive Service (SES) was formed.
https://youtu.be/QOM8lVpEC1I | Raw *.mp4 video file | Transcript | Timeline

Video: U.S. Congress..

BARACK OBAMA'S & HILLARY'S DEEP STATE SHADOW GOVERNMENT "SES CADRE"

On Dec. 15, 2015, Barack Obama Executive Order 13714 titled "Strengthening the Senior Executive Service." Not once, but twice, Obama referred to his "SES cadre." We believe that the use of the word "cadre" was not accidental (like their use of the word IBM Eclipse Foundation, as in eclipse the Constitution). Cadre means "a small group of people specially trained for a particular purpose or profession."

Very evidently, the SES is the secret army of the Deep State shadow government. They are "the Swamp."

Following their theft of Leader Technologies' social networking invention, they were able to dramatically streamline their secret organizing capabilities *completely outside of their official federal government communications systems*. These are the

reexamination process by Facebook. We will stay focused on *Leader v. Facebook* until justice is served, but we also welcome news and analysis of intellectual property abuse in other cases as well.

WELCOME TO DONNA KLINE NOW! READERS!

AFI has been supporting Donna and is now picking up the main Leader v. Facebook coverage (she will continue coverage as well).

Anonymous Posts Are Welcomed! Blogger has more posting constraints than Donna's WordPress, but we will continue to welcome anonymous posts. Simply send us an email at **NEW Leader® Private Email: afi@leader.com** with your post. Once the moderator verifies that your email address is real, your comment will be posted using your real name or handle, whatever you wish, like John Smith or Tex.

Click here to view a complete *Donna Kline Now!* posts archive.

systems Hillary and Bill Clinton used to communicate with on their private Westchester, New York "home brew" email server in total violation of U.S. law while she was Secretary of State.

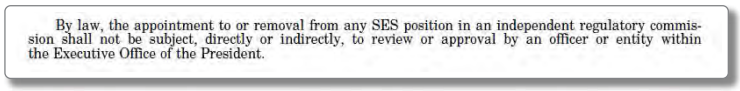
See AFI. (Nov. 22, 2017). The Weaponization of Social Media Should Concern Us All. *Americans for Innovation*.

Leader Technologies says that their invention included a highly securable messaging system.

Facebook initially offered that email system to the public, but then pulled it back. Thanks to corruption watchdog Judicial Watch, we see that private Facebook communication with Hillary Clinton and her State Department on Sep. 26, 2009 when she contracted with Facebook to build an "template for winning elections" to rig coming elections. More treason.

THE ROGUE SES SAYS THE PRESIDENT CANNOT FIRE THEM!

Here is the regulation they cite:



By law, the appointment to or removal from any SES position in an independent regulatory commission shall not be subject, directly or indirectly, to review or approval by an officer or entity within the Executive Office of the President.

Fig. 7—S. Prt. 114-26. (Dec. 01, 2016). Plum Book, Policy and Supporting Positions. Committee on Homeland Security and Governmental Affairs. U.S. Senate, 114th Congress, 2d Session, PDF p. 228. GPO.

IS SES ABOVE THE LAW?

We don't think so. As with every convoluted law and regulation that these people have had a hand in, it's a two-edged sword. When the American people were not aware of them, they exploited *their* loopholes for *their* benefit. Now that we are awake, their abortion of the Constitution has holes large enough to drive a Mack Truck through. For starters, how about military tribunals and Guantanamo prison?

We must return to what we believed to be regular order in the Republic.

We elected our leaders thinking that they would hire qualified people on our behalf and do the people's work.

What we now see is that the SES is a secret army of political and economic saboteurs who pay themselves well and support their

CODE OF CONDUCT FOR U.S. JUDGES

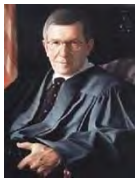
"CANON 2: A JUDGE SHOULD AVOID IMPROPRIETY AND THE APPEARANCE OF IMPROPRIETY IN ALL ACTIVITIES"

GALLERY OF JUDICIAL MISCONDUCT

Judge Leonard P. Stark, U.S. District Court of Delaware, trial judge in *Leader Techs, Inc. v. Facebook, Inc.*, 770 F. Supp. 2d 686 (D.Del. 2011). Judge Stark heard his jury foreman admit that the jury made the on-sale bar decision *without any evidence other than speculation*, and yet he supported that verdict anyway. Just months before trial, Judge Stark allowed Facebook to add the on-sale bar claim after the close of all fact discovery and blocked Leader from preparing its defenses to this new claim. Judge Stark allowed the claims despite Leader's prophetic argument that the action would confuse the jury and prejudice Leader. He also permitted the jury to ignore the *Pfaff v. Wells Electronics, Inc.* test for on-sale bar, even after instructing the jury to use it. (See that Jury Instruction No. 4.7 here.) He also contradicted his own instruction to Leader to answer Interrogatory No. 9 in the present tense (2009), then permitted the jury to interpret it as a 2002 admission as well. Facebook's entire on-sale bar case is based upon this interrogatory. (*Editorial*: Hardly sufficient to meet the "heavy burden" of the clear and convincing evidence standard.)

Like

Like



Judge Alan D. Lourie, U.S. Court of Appeals for the Federal Circuit, panel judge in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Lourie stood to

globalist Deep State shadow government task masters. Just look at their faces, *they all look guilty*.

These SES people know what they have done. The jig is up.

These saboteurs of the American Republic must be punished for their treason, it seems to us.

We call on SES whistleblowers to step forward.

* * *

Bookmark: #ses-vermin | https://tinyurl.com/y7xdhm26

Fig. 8—SES Vermin Among Us. https://youtu.be/SMuYU5euwfM | Raw *.mp4 video file

Video: American Intelligence Media, Americans for Innovation, Leader Technologies, Inc.

Bookmark: #zuckerberg-facebook-foreign-election-interference-hard-proof | https://tinyurl.com/y8b5j35g

Fig. 9—Facebook Commits Crimes Against the State. https://youtu.be/fb30lP06Sxs | Raw *.mp4 video file

Video: American Intelligence Media, Americans for Innovation, Leader Technologies, Inc.

POSTSCRIPT

benefit financially from undisclosed holdings in Facebook. See analysis of Judge Lourie's T. Rowe Price holdings re. the Facebook IPO. Judge Lourie also failed to apply his own law-test in *Group One v. Hallmark Cards* to the evidence. After debunking all of Facebook's evidence on appeal, Judge Lourie created new argument in the secrecy of chambers to support Facebook and prevent the on-sale bar verdict from being overturned—a clear breach of constitutional due process.

Like

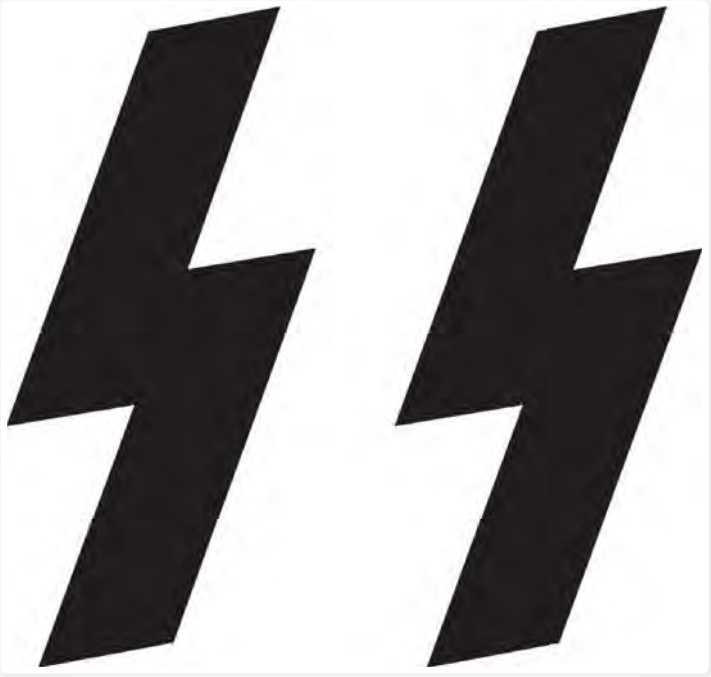
Judge Kimberly A. Moore, U.S. Court of Appeals for the Federal Circuit, panel judge in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Moore stood to benefit financially from undisclosed holdings in Facebook. See disclosure of substantial holdings in Facebook and Facebook-related stocks. Judge Moore failed to follow the long-held precedent for testing on-sale bar evidence in *Pfaff v. Wells Electronics, Inc.*—an evident and intentional omission coming from a former patent law professor. After debunking all of Facebook's evidence on appeal, Judge Moore created new argument in the secrecy of chambers to support Facebook and prevent the on-sale bar verdict from being overturned—a clear breach of constitutional due process.

Like

Judge Evan J. Wallach, U.S. Court of Appeals for the Federal Circuit, member of the three-judge panel in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Wallach is not a patent attorney. This begs the question as to why a judge with no knowledge of patent law was assigned to the case. Would anyone ask a dentist to perform brain surgery? The Federal Circuit was specially formed to appoint patent-knowledgeable judges to patent cases. There is no evidence so far in the judicial disclosures that Judge Wallach holds stock in Facebook, although

WAFFEN S(E)S HIDDEN IN PLAIN SIGHT

By An Anonymous Patriot Contributing Writer



It seems that the Nazi practice perfected under the "Third Reich" has been perfected inside the American Republic.

The new "Waffen SS" is none-other than the "Senior Executive Service'. Their enterprises consist of highjacked patents in the technology world, specifically associated with controlling the "Internet of Things."

The "Neo-Waffen SS" leverages stolen technology, in particular Leader Technologies into trillions of dollars of leveraged assets, using metadata collection for advertising, bribery, and blackmail.

The advertising is performed with "warrantless" search engine metadata capture to create monetized links to every person on the planet.

This information is sold at tremendous profit to companies who then leverage revenue income through targeted sales. The same "metadata" capture is used to create "dark profiles" on every citizen globally to be "un-masked" when convenient.

When it is "convenient," such as being "elected" to a public position of authority, this "authority'" can then be turned by

when he was asked on a motion to disclose potential Facebook holdings and other conflicts of interest, he refused along with the other judges. See Motion to Disclose Conflicts of Interest. Judge Wallach continued in silence even after Clerk of Court Horbaly failed to provide him with Dr. Lakshmi Arunachalam's motions (according to his Federal Circuit staffer Valeri White), and yet the Clerk signed an order regarding that motion on Judge Wallach's behalf. See a full analysis of these events at Donna Kline Now! Judge Wallach also failed to police his court's violation of Leader's Fifth and 14th Amendment constitutional right to due process when he participated in the fabrication of new arguments and evidence for Facebook in the secrecy of judge's chambers after he had just invalidated Facebook's sole remaining item of evidence (using disbelieved testimony as ostensible evidence of an opposite). Judge Wallach also failed to police his court when he failed to apply the Supreme Court's *Pfaff v. Wells Electronics, Inc.* test for on-sale bar evidence, which included even the Federal Circuit's own *Group One v. Hallmark Cards, Inc.* test—a test which Judge Lourie should have advised Judge Wallach to follow since Judge Lourie *helped write* that opinion. *Group One* test omission analysis.

Like

Clerk of Court Jan Horbaly, U.S. Court of Appeals for the Federal Circuit, clerk who signed all the opinions in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Clerk Horbaly and his staff obfuscated when the court's ruling was challenged by an *amicus curiae* brief revealing clear mistakes of law and new evidence. See analysis of the misconduct and misrepresentations within the Federal Circuit Clerk of Court in *Leader v. Facebook*. Mr. Horbaly failed to disclose his conflicts of interest and close associations with numerous Facebook attorneys and law firms, as well as his close association with one of Facebook's largest shareholders, Microsoft, who is a Director of The Federal Circuit Bar Association where Mr. Horbaly is an ex officio officer. Additionally, the DC Bar revealed in a written statement

Like

blackmail. Those that choose to buck the system, are humiliated and sent back to the matrix.

Those who play along, become “useful” tools. They sell themselves like prostitutes to the highest bidder, and are then disposed of when finished. Generally, they have heart attacks, poisonings, suicides or remotely triggered car crashes—all using the same “wet-ware” technology.

The “Senior Executive Services” or “SES” was created to emulate the control structures developed under the “Third Reich.” Within the federal bureaucracy, they are over 8,000+ strong, with an annual overhead exceeding $800K/year. They move in and out of private companies and the government at will with no vetting or challenges from the House or Senate.

In most cases, they are “invisible” to any control mechanisms, oversight, or challenges, and by default, become the “controllers” within the embedded bureaucratic structures themselves.

They are the “Third Reich Waffen SS.”’ It appears that Robert Mueller is the “neo-Himmler,” hidden in plane sight.

COMMENT

Click "*N* comments:" on the line just below this instruction to comment on this post. Alternatively, send an email with your comment to afi@leader.com and we'll post it for you. We welcome and *encourage* anonymous comments, especially from whisteblowers.

Posted by K. Craine at 3:30 PM

75 comments:

K. Craine March 16, 2018 at 7:38 PM

Email comment by GH:

Brooke Singman. (Mar. 16, 2016). Former FBI Deputy Director Andrew McCabe fired. Fox News.

FBI's Andrew McCabe fired, DOJ releases statement
The Justice Department dealt a stunning blow to former Acting FBI Director Andrew McCabe on Friday night, firing him just days before he would have been eligible for a lifetime pension after determining that he lied to investigators reviewing the bureau’s probe of Hillary Clinton’s email server.

"Pursuant to Department Order 1202, and based on the report of the Inspector General, the findings of the FBI Office of Professional Responsibility, and the recommendation of the Department’s senior career official, I have terminated the employment of Andrew McCabe effective immediately," Attorney General Jeff Sessions said in a statement.

"After an extensive and fair investigation and according to Department of Justice procedure, the Department’s Office of the Inspector General (OIG) provided its report on allegations of misconduct by Andrew McCabe to the FBI’s Office of Professional Responsibility (OPR)," Sessions said.

Full atory:

that Clerk Horbaly is not licensed to practice law in the District of Columbia. [Editorial: What does that make the Federal Circuit with its location within in a stone's throw of the White House? A self-governing state?]

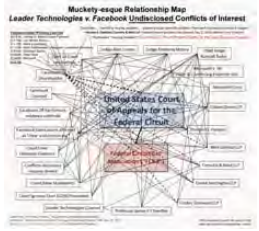
Judge Randall R. Rader, U.S. Court of Appeals for the Federal Circuit, chief judge responsible for the (mis)conduct of his judges and Clerk of Court in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Rader failed to manage his court resulting in a likely situation where his judges never even received briefs that they allegedly ruled on in favor of Facebook. Judge Rader also failed to disclose his conflicting relationships with a Leader principle with whom he may have had deep professional differences during his time at the Senate Judiciary Committee—his former professor of law at George Washington University Law Center, former Leader director Professor James P. Chandler. See analysis of Judge Rader's undisclosed conflicts of interest in *Leader v. Facebook*. Judge Rader also did not stop his judges from creating new arguments and evidence for Facebook in the secrecy of chambers—after they had debunked all of Facebook's evidence on appeal, which is a clear breach of constitutional due process.

Like

Like

Updated May 22, 2015

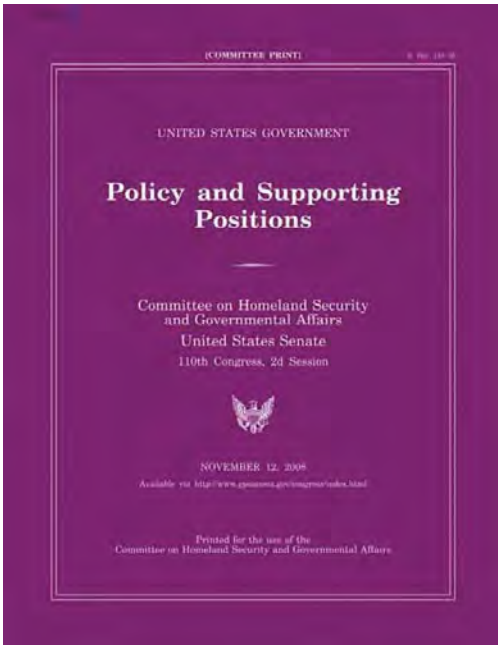
Click here to view a Federal Circuit *Leader v. Facebook* **Conflicts of Interest** Map.



See "Cover-up In Process At The Federal Circuit?" *Donna Kline Now!* Sep. 17, 2012.

Leader v. Facebook Legal Research Links

Plum Books *hide* SES employees in a blizzard of bad math and contradictory, nonsensical categories



Then, besides *hiding* their identities from *We The People*, they say their SES benefits and privileges are not accountable to the President of the United States.[1] See footnote below on "independent regulatory commission."[2]

By Anonymous Patriots

> By law, the appointment to or removal from any SES position in an independent regulatory commission shall not be subject, directly or indirectly, to review or approval by an officer or entity within the Executive Office of the President.

Apr. 04, 2018—Kudos to the American Intelligence Media reader who noticed that the tables in the Plum Books use a confusing array of notations for "Type of Appointment."

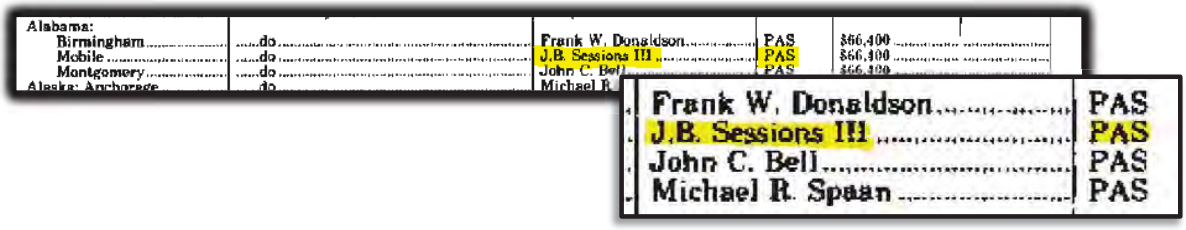
[1] S. Prt. 114-26. (Dec. 01, 2016). Plum Book, Policy and Supporting Positions. Committee on Homeland Security and Governmental Affairs. U.S. Senate, 114th Congress, 2d Session, PDF p. 228. GPO.

[2] Shockingly, the phrase "independent regulatory commission" is *undefined* in the Plum Books. Generally, when lawyers loosely define a term, it is *intentional* so that in the future it can mean whatever their buddies want it to mean. This phrase is only used here— in their claim that these positions are not accountable to the President. "Independent" is undefined. The related concept of "impartiality" is used in this same section to imply that SES positions "ensure impartiality."

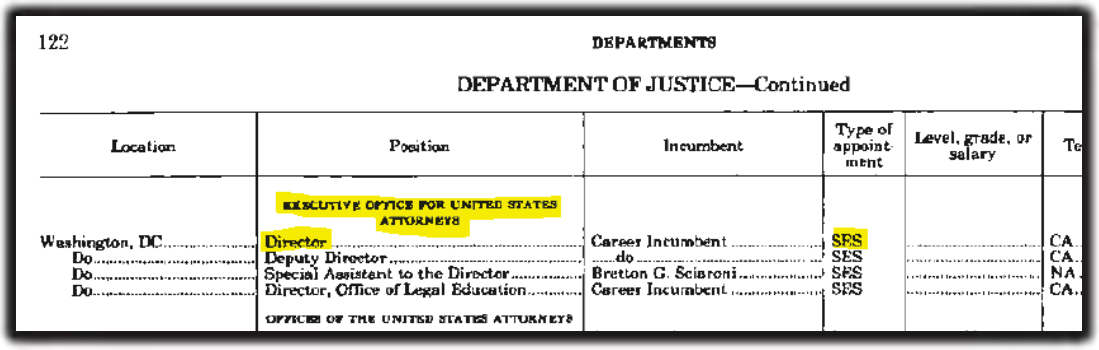
> SES positions are designated Career Reserved when the need to ensure impartiality, or the public's confidence in the impartiality of the Government, requires that they be filled only by career employees (e.g., law enforcement and audit positions).

Therefore, this could apply to all SES positions, if they want it to mean that (which they obviously do—it appears that they punish SES alums that become whistleblowers, like Dinesh D'Souza, SES 1988). *See* H. Prt. 100-NN. (Nov. 09, 1988). Dinesh D'Souza, Plum Book, Policy and Supporting Positions. Committee on Post Office and Civil Service House of Representatives, 100th Congress, 2d Session. Y 4.G 74/7 :P 75/6/988. GPO.
"Regulatory" can mean anything since government agencies are all regulatory in function. "Commission" is not defined either, and if broadly defined, encompasses the activities of all agencies in their overall missions.

This person noticed that in the 1984 Plum Book J.B. Sessions III (Jefferson "Jeff" Beauregard Sessions III, PDF p. 134) had a "PAS" designation, while others in the chart, their superiors, had "SES" designations.



On the surface, it would appear that the PAS "Type of Appointment" is different than SES. In fact, just above Sessions' name is the following list of DOJ directors who ran the U.S. Attorneys' office—all designated SES.


122 DEPARTMENTS

DEPARTMENT OF JUSTICE—Continued

Location	Position	Incumbent	Type of appointment	Level, grade, or salary	Te
	EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS				
Washington, DC	Director	Career Incumbent	SES		CA
Do	Deputy Director	do	SES		CA
Do	Special Assistant to the Director	Bretton G. Sciaroni	SES		NA
Do	Director, Office of Legal Education	Career Incumbent	SES		CA
	OFFICES OF THE UNITED STATES ATTORNEYS				

To make the disclosure even more convoluted, the summary in Appendix No. 2 about SES positions states:[3]

Number and types of SES positions

Currently there are approximately 8,000 SES positions allocated

However, investigators actually counted the records in the 1984 Plum Book (see Table below). It discloses approximately 9,872 positions in its 137 pages. If we use that number *instead* of the 8,000 number, that would mean that only 1,872 of those positions are ***not*** SES positions.

Still more discombobulated is the fact that there are, in fact, approximately 1,264 "PAS" positions and 3,728 "SES" positions in the 1984 Plum Book. So which is it? 8,000 SES positions or 3,728 SES? **The Book says both!**

[3] S. Prt. 98-286. (Nov. 22, 1984). Plum Book, Policy and Supporting Positions. Committee on Governmental Affairs. U.S. Senate, 98th Congress, 2d Session. Y 4.G 74/7:P 75/6/984, PDF p. 84. GPO.

A reader can only conclude that most of the other designations, like PAS, PA, PL, NEA, A, B, C, GS, GG, GM, NE, p.d., p.h., W.c.,(I) and WG are surreptitiously SES.

This conclusion is reinforced by looking at what changes were made in the Types of Appointments between the 1988 and 1992 Plum Books.

In 1992, the SES "Type of Appointment" was removed completely. SES became a "Pay Plan" accompanied by a hopelessly vague explanation:

Original Text:

"Note that several categories of positions can be filled by more than one type of appointment e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency or limited term appointment authorities."

Commentary with Text:

"Note that several [*open-ended*] categories of positions can be filled by more than one type of appointment [*open-ended*], e.g., SES positions listed in this publication may be filled [*open-ended*] by using career, noncareer, limited emergency or limited term appointment authorities."

This one paragraph permits the SES positions to be hidden. Following this change, only some of the names were designated as an SES (or ES) pay grade, while the total number of disclosures, in aggregate, matched the total number of SES positions disclosed. The entire disclosure is nonsensical bureaucratic jibberish . *See* Table below.

> In other words, *any type* of Plum Book appointment can be SES, the SES pay plan can be added to *any type* of appointment, the totals disclosed *roughly match* the total number of SES appointments summarized in Appendix No. 2 in the back of each Plum Book.

Plum Book Analysis:

Year	Pages total	Pages with position tables	SES positions allocated	Positions per page	Positions disclosed	Non-SES reported
1980	178	137	8,590	39.33	5,388	(3,202)
1984	280	251	8,000	39.33	9,872	1,872
1988	248	218	8,000	39.33	8,574	574
1992	216	205	8,800	39.33	8,063	(737)
1996	495	450	7,876	24	10,800	2,924
2000	349	330	7,815	28.5	9,405	1,590
2004	234	212	7,815	39.33	8,338	523
2008	217	195	8,328	39.33	7,669	(659)
2012	220	194	8,328	39.33	7,630	(698)
2016	236	211	9,936	39.33	8,299	(1,637)
Cumulative Total:			**83,488**		**84,038**	550

Conclusion:

This analysis shows that the positions disclosed in the 10 Plum Books from 1980-2016 are essentially all SES.

If this is not the correct interpretation, then it is the government's responsibility to *explain the SES in clear terms*, rather than forcing citizens to consume almost 100 hours of creative time just to try and figure out what the government SES reports are saying, and not saying.

Appendix:

Summary of the Legends from the Plum Books

1980

LEGEND

Type of appointment:

PAS	Presidential appointment, by and with the advice and consent of the Senate.
PA	Presidential appointment.
PL	Positions excepted from civil service rules and regulations by statutes.
NEA	Positions at GS–16, 17, and 18 authorized to be filled by noncareer executive assignment under Executive Order 11315 of November 17, 1966.
A	Positions excepted from civil service rules and regulations, not of a confidential or policy determining character for which it is not practical to hold any kind of examination.
B	Positions excepted from civil service rules and regulations, not of a confidential or policy determining character, for which it is not practical to hold a competitive examination.
C	Positions of a confidential or policy determining character which are excepted from the competitive service to which appointments may be made without examination by the Office of Personnel Management.

Grade:

GS	General Schedule of the Classification Act of 1949.
GG	Administrative grades similar to GS grades.
WG (WB), (WS)	Blue-collar positions where the pay is established at the local prevailing rate in the community.
FO, FR, FI,[1]	Foreign Service Officer Schedule.

1984

Type of appointment:

PAS	Presidential appointment, by and with the advice and consent of the Senate.
PA	Presidential appointment.
PL	Position excepted from the competitive civil service by statute.
SES	Position in the Senior Executive Service.
NEA	Position at GS–16, 17, or 18 which the Office of Personnel Management has authorized to be filled by Noncareer Executive Assignment.
A	Position excepted from the competitive civil service by the Office of Personnel Management which is not of a confidential or policy determining character and for which it is not practicable to hold an examination.
B	Position excepted from the competitive civil service by the Office of Personnel Management which is not of a confidential or policy determining character and for which it is not practicable to hold a competitive examination.
C	Position of a confidential or policy determining character which is excepted from the competitive civil service by the Office of Personnel Management and to which appointments may be made without examination by that Office.

Level, Grade, or Salary:

Level	Executive Level.
GS	General Schedule.
GG	Administrative grade similar to GS.
GM	Merit Pay.
NE	Grade not established.
p.d.	Per diem—daily rate of pay.
p.h.	Per hour—hourly rate of pay.
W.c.	Without compensation.
(I)	Intermittent, when actually employed.
WG	Blue collar position for which pay is established at the local prevailing rate in the community.

1988

Type of appointment:

PAS	Presidential appointment, by and with the advice and consent of the Senate.
PA	Presidential appointment.
PL	Position excepted from the competitive civil service by statute.
SES	Position in the Senior Executive Service.
NEA	Position at GS–16, 17, or 18 which the Office of Personnel Management has authorized to be filled by Noncareer Executive Assignment.
C	Position of a confidential or policy determining character which is excepted from the competitive civil service by the Office of Personnel Management and to which appointments may be made without examination by that Office.

Level, Grade, or Salary:

Level	Executive Level.
GS	General Schedule.
GG	Administrative grade similar to GS.
GM	Merit Pay.
NE	Grade not established.
p.d.	Per diem—daily rate of pay.
p.h.	Per hour—hourly rate of pay.
W.c.	Without compensation.
(I)	Intermittent, when actually employed.
WG	Blue collar position for which pay is established at the local prevailing rate in the community.

1992

Type of Appointment (Column 5)

Listed are letter codes that denote the type of appointment under which the position incumbent is serving. Note that several categories of positions can be filled by more than one type of appointment, e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency, or limited term appointment authorities. Therefore, no "Type of Appointment" is shown for such positions when they are vacant.

PAS	=	Presidential Appointment with Senate Confirmation
PA	=	Presidential Appointment (without Senate confirmation)
CA	=	Career Appointment
NA	=	Noncareer Appointment
EA	=	Limited Emergency Appointment
TA	=	Limited Term Appointment
SC	=	Schedule C Excepted Appointment
XS	=	Appointment Excepted by Statute

Pay Plan (Column 4)

Listed are letter codes that denote the Federal salary schedule or pay system under which position incumbents are paid. Tables showing the salary ranges for each pay system are contained in Appendix 4.

EX	=	Executive Schedule
ES	=	Senior Executive Service
SL	=	Senior Level
GM	=	Performance Management and Recognition System (Merit Pay)
GS	=	General Schedule
FE	=	Senior Foreign Service
FP	=	Foreign Service Specialist
OT	=	Other Pay Plan (all those not listed separately)
PD	=	Daily Pay Rate* (per diem)
WC	=	Without Compensation*

1996

Type of Appointment (Column 5)

Listed are letter codes that denote the type of appointment under which the position incumbent is serving. Note that several categories of positions can be filled by more than one type of appointment, e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency, or limited term appointment authorities. Therefore, no "Type of Appointment" is shown for such positions when they are vacant. Note also that some part-time Presidential Appointments are not included in this listing such as those serving on temporary commissions or those boards and commissions which are governed by the Federal Advisory Committee Act.

PAS = Presidential Appointment with Senate Confirmation

PA = Presidential Appointment (without Senate confirmation)

CA = Career Appointment

NA = Noncareer Appointment

EA = Limited Emergency Appointment

TA = Limited Term Appointment

SC = Schedule C Excepted Appointment

XS = Appointment Excepted by Statute

Pay Plan (Column 4)

Listed are letter codes that denote the Federal salary schedule or pay system under which position incumbents are paid. Tables showing the salary ranges for each pay system are contained in Appendix 4.

EX = Executive Schedule

ES = Senior Executive Service

SL = Senior Level

AD= Administratively Determined

GS = General Schedule

FE = Senior Foreign Service

FP = Foreign Service Specialist

OT = Other Pay Plan (all those not listed separately)

PD = Daily Pay Rate* (per diem)

WC = Without Compensation*

2000

Type of Appointment (Column 5)

Listed are letter codes that denote the type of appointment under which the position incumbent is serving. Note that several categories of positions can be filled by more than one type of appointment (e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency, or limited term appointment authorities). Therefore, no "Type of Appointment" is shown for such positions when they are vacant. Note also that some part-time Presidential Appointments are not included in this listing such as those serving on temporary commissions or those boards and commissions which are governed by the Federal Advisory Committee Act.

PAS	=	Presidential Appointment with Senate Confirmation
PA	=	Presidential Appointment (without Senate confirmation)
CA	=	Career Appointment
NA	=	Noncareer Appointment
EA	=	Limited Emergency Appointment
TA	=	Limited Term Appointment
SC	=	Schedule C Excepted Appointment
XS	=	Appointment Excepted by Statute

Pay Plan (Column 4)

Listed are letter codes that denote the Federal salary schedule or pay system under which position incumbents are paid. Tables showing the salary ranges for each pay system are contained in Appendix 4.

EX	=	Executive Schedule
ES	=	Senior Executive Service
SL	=	Senior Level
AD	=	Administratively Determined
GS	=	General Schedule
FE	=	Senior Foreign Service
FP	=	Foreign Service Specialist
VH	=	Farm Credit Administration Pay Plan
TM	=	Federal Housing Finance Board Merit Pay
CG	=	Corporate Graded at Federal Deposit Insurance Corporation
OT	=	Other Pay Plan (all those not listed separately)
PD	=	Daily Pay Rate* (per diem)
WC	=	Without Compensation*

2004

Type of Appointment (Column 4)

Listed are letter codes that denote the type of appointment under which the position incumbent is serving. Note that several categories of positions can be filled by more than one type of appointment, e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency, or limited term appointment authorities. Therefore, no "Type of Appointment" is shown for such positions when they are vacant.

PAS	=	Presidential Appointment with Senate Confirmation
PA	=	Presidential Appointment (without Senate confirmation)
CA	=	Career Appointment
NA	=	Noncareer Appointment
EA	=	Limited Emergency Appointment
TA	=	Limited Term Appointment
SC	=	Schedule C Excepted Appointment
XS	=	Appointment Excepted by Statute

Pay Plan (Column 5)

Listed are letter codes that denote the Federal salary schedule or pay system under which position incumbents are paid. Tables showing the salary ranges for each pay system are contained in Appendix 4.

EX	=	Executive Schedule
ES	=	Senior Executive Service
SL	=	Senior Level
GM	=	Performance Management and Recognition System (Merit Pay)
GS	=	General Schedule
FE	=	Senior Foreign Service
FP	=	Foreign Service Specialist
OT	=	Other Pay Plan (all those not listed separately)
PD	=	Daily Pay Rate* (per diem)
WC	=	Without Compensation*

2008

Type of Appointment (Column 4)

Listed are letter codes that denote the type of appointment under which the position incumbent is serving. Note that several categories of positions can be filled by more than one type of appointment, e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency, or limited term appointment authorities. Therefore, no "Type of Appointment" is shown for such positions when they are vacant.

PAS	=	Presidential Appointment with Senate Confirmation
PA	=	Presidential Appointment (without Senate Confirmation)
CA	=	Career Appointment
NA	=	Noncareer Appointment
TA	=	Limited Term Appointment
SC	=	Schedule C Excepted Appointment
XS	=	Appointment Excepted by Statute

Pay Plan (Column 5)

Listed are letter codes that denote the Federal salary schedule or pay system under which the position incumbents are going to be paid. Tables showing the salary ranges for major pay systems are contained in Appendix 4.

AD	=	Administratively Determined Rates
ES	=	Senior Executive Service
EX	=	Executive Schedule
FA	=	Foreign Service Chiefs of Mission
FE	=	Senior Foreign Service
FP	=	Foreign Service Specialist
GS	=	General Schedule
PD	=	Daily Pay Rate* (per diem)
SL	=	Senior Level
TM	=	Federal Housing Finance Board Merit Pay
VH	=	Farm Credit Administration Pay Plan
WC	=	Without Compensation*
OT	=	Other Pay Plan* (all those not listed separately)

2012

Type of Appointment (Column 4)

Listed are letter codes that denote the type of appointment under which the position incumbent is serving. Note that several categories of positions can be filled by more than one type of appointment, e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency, or limited term appointment authorities. Therefore, no "Type of Appointment" is shown for such positions when they are vacant.

PAS	=	Presidential Appointment with Senate Confirmation
PA	=	Presidential Appointment (without Senate Confirmation)
CA	=	Career Appointment
NA	=	Noncareer Appointment
EA	=	Limited Emergency Appointment
TA	=	Limited Term Appointment
SC	=	Schedule C Excepted Appointment
XS	=	Appointment Excepted by Statute

Pay Plan (Column 5)

Listed are letter codes that denote the Federal salary schedule or pay system under which the position incumbents are going to be paid. Tables showing the salary ranges for major pay systems are contained in Appendix 4.

AD	=	Administratively Determined Rates
ES	=	Senior Executive Service
EX	=	Executive Schedule
FA	=	Foreign Service Chiefs of Mission
FE	=	Senior Foreign Service
FP	=	Foreign Service Specialist
GS	=	General Schedule
PD	=	Daily Pay Rate* (per diem)
SL	=	Senior Level
TM	=	Federal Housing Finance Board Merit Pay
VH	=	Farm Credit Administration Pay Plan
WC	=	Without Compensation*
OT	=	Other Pay Plan* (all those not listed separately)

2016

Type of Appointment (Column 4)

Listed are letter codes that denote the type of appointment under which the position incumbent is serving. Note that several categories of positions can be filled by more than one type of appointment, e.g., SES positions listed in this publication may be filled by using career, noncareer, limited emergency, or limited term appointment authorities. Therefore, no "Type of Appointment" is shown for such positions when they are vacant.

PAS	=	Presidential Appointment with Senate Confirmation
PA	=	Presidential Appointment (without Senate Confirmation)
CA	=	Career Appointment
NA	=	Noncareer Appointment
EA	=	Limited Emergency Appointment
TA	=	Limited Term Appointment
SC	=	Schedule C Excepted Appointment
XS	=	Appointment Excepted by Statute

Pay Plan (Column 5)

Listed are letter codes that denote the Federal salary schedule or pay system under which the position incumbents are going to be paid. Tables showing the salary range for major pay systems are contained in Appendix 4.

AD	=	Administratively Determined Rates
ES	=	Senior Executive Service
EX	=	Executive Schedule
FA	=	Foreign Service Chiefs of Mission
FE	=	Senior Foreign Service
FP	=	Foreign Service Specialist
GS	=	General Schedule
PD	=	Daily Pay Rate* (per diem)
SL	=	Senior Level
TM	=	Federal Housing Finance Board Merit Pay
VH	=	Farm Credit Administration Pay Plan
WC	=	Without Compensation*
OT	=	Other Pay Plan* (all those not listed separately)

Download Plum Books (1980-2016) and Related Research

Senior Executive Service (SES) "Plum Book" Policy and Supporting Positions published by various House and Senate Committees Updated Mar. 30,2018

President	Reporting Year	SES Plum Book Be Patient on downloads, these are large files		Positions	Depts. & Agencies	Inspectors General (Deep State shadow gov't suffers)	Agency/Dept. Summary Spreadsheet
Search Note: The versions of these documents at the Federal Register and GoogleDocs/GoogleDrive contain search blocks that prevent all the names in these documents from appearing on searches and being indexed by web search crawlers. We are unpacking these files and removing those booby traps. So, just because a name does not appear the first time you search, do not assume it is not there. It may have been intentionally rendered unsearchable. We are receiving many reports from whistleblowers that these official SES lists are not comprehensive and are only the "tip of the iceberg" of total SES federal employees. Reading between the lines of their disclosure rules, SES has dozens of ways of making people's names and salaries secret, and as they say in every document, they cannot be hired or fired by the President (that statement is usually the last paragraph of APPENDIX NO. 2).							
Jimmy Carter	1980	PDF		8,600		18	
Ronald Reagan	1984	PDF		8,000		20	
	1988	PDF		8,000		14	
George H.W. Bush	1992	PDF		8,600		12	
Bill Clinton	1996	PDF		7,303	104	30	XLSX
	2000	PDF	DOCX	7,323	115	?	XLSX
George W. Bush	2004	PDF	DOCX	9,357	119	?	XLSX
	2008	PDF	DOCX	8,221	115	?	XLSX
Barack Obama	2012	PDF	DOCX	11,392	164	25	XLSX
	2016	PDF	DOCX	9,033	166	25	XLSX
		Standing SES (DOJ) Performance Review Boards*					
		Fed. Reg. PDF	Declawed PDF	500	Office of Attorney General	DOJ SES 500 - DOJ Paymasters HTML	Declawed XLSX
Various	1979-	SITE		NSA, CIA, DTIC, DOD			
Various	Various	ZIP		SERCO British/Int'l arm of SES (has controlled the U.S. Patent Office since 2006)			

https://americans4innovation.blogspot.com/2018/03/obama-hired-them-trump-cannot-fire-them.html#ses-plum-books-1996-2016

Notices: This document may contain opinion. As with all opinion, it should not be relied upon without independent verification. Think for yourself. Fair Use is relied upon for all content. For educational purposes only. No claims are made to the properties of third parties. All documents from the Federal Register and Government Printing Office designated as "Authenticated U.S. Government Information. GPO" are presumed to be judicially-recognizable public records.

AMERICAN
INTELLIGENCE MEDIA

Citizens Addicted to Truth

ANONYMOUS PATRIOTS / APRIL 11, 2018 @ 1:06 PM

TENTACLES OF SERCO STRANGLE AMERICA

APX 037

We stand corrected. We have reported that we are fighting the Second American Revolution. But our continuing research shows us that this is not the case. It appears that the *first* American Revolutionary War was never won, and we are still under British rule, in ways more sinister than the average person is aware.

It all started in our research of the Senior Executive Service. We showed you how this unconstitutional shadow government is highly organized and well paid. Its members are positioned within our civil service bureaucracies to overthrow the Republic in plain sight and establish itself as the governing body of Marxist globalists whose SES members work daily to thwart the will of the people, ignore and bastardize the rule of law, and destroy the Republic from within.

We call Senior Executive Service Obama's Army.

SES is the shadow government.

We gave you research tools so that you could name these individuals specifically and expose their bureaucratic spider holes.

We thought the story was over until we started researching a group that lands most of the government's contracts thanks to its close relationship to Senior Executive Service. Together – SES and SERCO – operate the United States government with the purpose of destroying our nation and giving our country away to the Queen of England.

Citizens of the world, not just Americans, are still subjects of the British Monarchy.

Let us explain why.

This video below will give you an overview before diving into the article:

THE BIGGEST COMPANY YOU'VE NEVER HEARD OF

BRITISH CROWN AND BRITISH EAST INDIA COMPANY RULE AMERICA

The British Crown and the British East India Company have never left America, and in fact, they have a stranglehold on the U. S. economy that is a death grip. The Bank of England, the City of London, and ultimately the British Monarchy – Queen Elizabeth II, own and control U. S. data management, corporate banking, resources of gas, uranium, gold, and many strategic resources and systems in the United States.

This system, called SERCO, is widely known and many researchers and authors precede us in their reporting; however, it is our intent in this series of articles and videos to show the specific rat lines that make Senior Executive Services and SERCO the evilest system in the world. We will be showing you the big picture of SERCO in this series.

In subsequent articles, posts, and videos, we will show you the connections of named SES agents who make sure that SERCO controls the systems and services of the United States government.

We will show you how Serco is not only an enemy of the United States, but an enemy of countries and people around the world. In the end, we hope you conclude, as have we, that the British Monarch has no place in the United States government and any of its services. The cozy relationship that Serco has with SES must be eliminated and laws be written to prevent this quiet overthrow of the Republic by SES and Serco.

For example, did you know that the U. S. Patent Office is controlled by Serco? That's right, a BRITISH based company controls the creative efforts of American entrepreneurs and

creators. Serco was the company awarded the Obamacare data management system that cost America's over $2 billion.

SES employees in charge of selecting contracts for this lucrative data management system didn't find U.S. based companies to do the work. Instead they cherry-pick their buddies at British owned and controlled Serco to deliver Obamacare management.

lobbyists controlling Congress, corporate pay-to-play through the executive branch (such as Hillary's Department of State), and the Senior Executive Service to maintain the bureaucratic status quo, selling out to global corporatism at every turn with no bid contracts and cronyism.

SENIOR EXECUTIVE SERVICES AND SERCO ARE THE PEOPLE AND ORGANIZATIONAL SYSTEMS THAT THE BRITISH MONARCH USES TO CONTROL AMERICA.

Senior Executive Service aligns with the imperialistic intents of Serco and numerous other corporations that are listed in this report (BP, Shell, ICAP, British American Tobacco, SABMiller, American Standard Life, Rio Tinto, Ixstrata, etc.).

Here are a few highlights of what Serco does already in our government. To our friends in other parts of the world, don't be surprised when you see similar structures in your own country run by the British Monarch through Serco:

- **Serco manages all patents for the U. S. Patent and Trademark Office. Brits have the first shot at stealing American's intellectual property rights. This is shocking but true.**

- **Serco controls the most sensitive data management systems in all branches of the military, federal government, and state and local municipalities.**
- **Serco controls air traffic management, airlines security, airport management and all aspects of ticketing, visa data management, and timetable management.**
- **Serco is called, "the largest company no one has ever heard of."**
- **Serco's efficiency rating in England, Canada, and Australia is below 65% and many lawsuits have been filed against the company for egregious fraud and mismanagement.**
- **Serco was paid $1.2 billion to management the data of Obamacare — British company handling American's private medical information.**

Serco goes by many names so always look under the hood in their corporate documents to find its trail back to Queen Lizzie. In America, it operates as Serco Inc. and claims on its website that it "is a leading provider of professional, technology, and management services for the federal government". Headquartered in Reston, Virginia, Serco Inc. has approximately 10,000 employees, annual revenue of $2.5 billion, and is ranked in the top 35 of the largest federal prime contractors.

Piercing the corporate veil, we find that Serco Inc. is a wholly-owned subsidiary of Serco Group plc, a $7 billion international business that works with government and public services around the world.

Many researchers say that Serco runs the United Kingdom (UK), Canada, and Australia. Serco has over 60,000 people in 35 countries across the world. To our international readers, it is highly doubtful that they are not operating in your country.

Serco is a leading provider of public services of all types. Serco operates internationally across five sectors and four geographies: defense, justice, immigration, transportation, health and human services. Its services are delivered in UK, Europe, North America, Asia Pacific, and the Middle East.

Serco delivers records management and processing support services for many U. S. government agencies. Major programs include processing and classifying of patent applications for the U.S. Patent and Trademark Office; records management and process of applications and petitions at U.S. Citizenship and Immigration Services' Service Centers; processing visa applications at the U.S. Department of State's National Visa Center and Kentucky Consular Center; and, records management services at the U.S. Citizenship and Immigration Services' National Benefits Center, among others.

Ninety percent of Serco's business is with the federal government with 10,000 workers across 45 states. Serco's experience is in paper pushing, records management, processing applications, processing visas, handling patents with the U.S. Patent and Trademark Office. There are more than 60 million records that Serco handles for the Department of Homeland Security.

Serco Inc. is indeed part of Serco Group, an international contracting firm headquartered near London and partly owned by the UK government itself. Serco Inc. is the North America division of Serco Group, plc. In North America, **Serco Inc. serves federal, state and local governments**, along with the Canadian government and commercial customers, and over 14,000 in North Americas.

Digest that for a moment: U.S. federal records, personal medical records, patents, and visas are held by a company owned and directed by the British Monarch. Its "soldiers on the ground" are employees of SES who guarantee that Serco gets the contracts, and then manages and oversees their continued involvement.

America is not a sovereign nation with this arrangement. We are still subjects of the British Monarchy.

HOW DID THE BRITISH MONARCH GAIN CONTROL OF THE U.S. GOVERNMENT?

In 1897, Guglielmo Marconi's successful development of trans-Atlantic radio communications and his drive to expand this capability resulted in the establishment of an American communications company named Radio Corporation of America (RCA). RCA assumed all the assets of the Marconi Wireless Company in America so that all technological development of radio communications for the U.S. Armed Forces would come under the auspices of the U.S. Government via a wholly-owned American entity.

RCA's success in America soon turned to the market on the other side of the Atlantic. On September 10, 1929, RCA set up the first RCA subsidiary in the UK – this is what is traditionally considered to be the "start" of Serco. In 1959, an RCA subsidiary in Great Britain negotiated a contract to install and commission an early warning radar station at RAF Flyingdales as part of the Ballistic Missile Early Warning System project. This contract, awarded in 1960, secured the future for RCA in the UK. RCA now had evolved with demonstrable capabilities in the field of technical support for the most complex antenna and radar communication networks.

In 1969, RCA organized itself into operational divisions, one of which was focused on service, and so it came about that the RCA Service Division was formed – the part of the company that would eventually be purchased by its management and staff and renamed Serco.

Serco established its North American foothold in 1988 when it was incorporated, acquiring companies that shared a similar vision. In 2005, Serco acquired Resource Consultants Inc. (RCI), which expanded its capabilities in IT services, systems engineering, strategic consulting and HR-focused business process management. In 2008 Serco acquired SI International, further broadening its capabilities in IT and professional services in North America and gaining new federal government and DoD relationships.

Serco Inc. now employs approximately 14,000 people across the U.S. and Canada. The company delivers services to all branches of the U.S. military, federal and civilian agencies, state and local agencies, and commercial customers.

In July of 2013, Serco was awarded a contract by the U.S. Department of Health and Human Services' Centers for Medicare and Medicaid Services (CMS) to support the health benefit exchanges. The contract had a one-year base period and four one-year option periods. As posted on the Federal Business Opportunities website, the contract value was approximately $1.25 billion.

Serco manages approximately 1,500 staff in Arkansas, Alabama, and Kentucky who support CMS with the routing, automated processing, reviewing, and troubleshooting of applications submitted for enrollment into a Qualified Health Plan. Serco also provides records management, and verification support.

Serco is so deeply embedded in our governmental operations that we have concluded that its take-over of the Republic is complete. Unless the unconstitutional Senior Executive Service is totally eliminated and new laws written to prevent international companies like Serco from ever operating within the government, we might as well fly the British flag over the Capitol building.

To see more on Serco and its paper trail back to RCA Photophone see:

WHAT IS THE REAL TRUTH ABOUT SERCO?

SERCO TENTACLES ALL OVER THE WORLD

Serco's reach is not just in the UK and the US. As one of the leading providers of public sector services in the world, Serco's UK and Europe region employs more than 31,700 people across 11 countries including Belgium, France, Germany and Italy. Serco advises policy makers, designs innovative solutions, integrates systems and delivers front-line services. Within the UK and Europe, Serco works across public service sectors in justice, immigration, healthcare, defense, transport and citizen services.

After reading about how Serco is entrenched in the U.S. government, we encourage international researchers to unmask these British Monarch tentacles in their own countries. If we all work together globally in exposing Serco, we might be able break free of the Queen's rule over the world where she still believes that the sun never sets on her Empire. Then we can go after her handlers – the CityofLondon, the Knights of Malta, and the Vatican.

SERCO'S DEATH GRIP ON THE U.S. PATENT OFFICE

On March 18, 2013, Serco Inc., announced that their Pre-Grant Publication (PGPubs) Classification Services team recently processed their 2 millionth patent application for the U.S. Patent and Trademark Office (USPTO). Each application was also processed within the contractually required 28-day window.

USPTO is the government agency that grants U.S. patents and registers trademarks. In 2006, Serco was awarded the contract with USPTO to manage their Pre-Grant Publication (PGPubs) Classification Services. Serco's PGPubs team has since been responsible for analyzing the claims made in patent applications and assigning the appropriate U.S. and international classifications to key aspects of proposed inventions.

In a single day, Serco's PGPubs Patent Classifiers processed approximately 1,450 patent applications by analyzing more than 21,800 patent claims and assigning more than 7,900 U.S. and international classifications. Since 2006, the team has built a virtually paperless classification operation. The operation, they claim on their website, "includes a secure facility with IT infrastructure, procedures for recruiting and training highly skilled staff, and implementation of a set of automated tools that streamlined the classification process". The facility is located in Harrisonburg, Virginia.

On November 30, 2015, Serco was awarded a patent classification services contract with the United States Patent and Trademark Office (USPTO). The recompete contract has a one-year base period with four one-year option periods, and is valued at $95 million over the five-year period, if all options and award terms are exercised.

Serco has supported the USPTO under this program since its inception in 2006, and currently processes approximately 1,600 applications a day, and over 400,000 applications annually. Under the contract, Serco has been instrumental in assisting the USPTO as it transitioned to a new international classification standard called Cooperative Patent Classification (CPC) and will continue to provide services within CPC that enables the USPTO to align and lead within the global intellectual property environment.

Serco Patent Processing System

In reading about how Serco's patent processing system works, we peel back another layer of how **Michael McKibben and Leader Technologies were ripped off by the IBM Eclipse Foundation**, the U.S. Patent office, and all corrupt attorneys involved in this patent heist of all times.

Below is a description of how the patent process works and shows you how Serco is part of the process from start to finish. What Serco added to the process was the new key element of making all American patents fit an international format. Serco has first "choice" on what patents may be an issue of "national security" and thus confiscated and eventually weaponized by the Department of Defense or the Central Intelligence Agency.

The description below is the initial process Serco uses to "screen" all U. S. patents. It is taken from the U.S. Department of Commerce Privacy Impact Assessment called the Serco Patent Processing System (Unique Project Identifier: [1858] PTOC-016-00)

Introduction

System Description. Provide a description of the system that addresses the following elements:

- a general description of the information in the system. This system processes inbound electronic images of patent applications received by Serco Inc. from USPTO. The system consists of a variety of application review, research tools and data entry tools to facilitate the evaluation and classification of the application creating a series of US Patent Classification (USPC) system and Cooperative Patent Classification (CPC) system classification data elements that describe the application.
- a description of a typical transaction conducted on the system. Serco PPS receives patent applications directly from the United States Patent and Trademark Office (USPTO).
- any information sharing conducted by the system. Serco PPS does not share any information with other agencies, individuals, or organizations. The information provided by USPTO is used by Serco for authorized activities performed by internal personnel only.
- a citation of the legal authority to collect PII and/or BII. The PII and BII data is collected by the USPTO to enable identification of the inventory and facilitate the patent application process. It is provided to the Serco PPS so that classification activities can be performed on the collected patent application.
- the Federal Information Processing Standard (FIPS). 199 security impact categories for the system.

As you can read in the description of the initial process Serco uses to screen patents, the entire nature of the patent is provided to Serco. If Serco doesn't approve a patent, it doesn't go forward. In other words, Serco controls American innovation and has the opportunity to steal any patent that is desirable to them. America is feeding British innovation and we pay Serco to conduct this theft of intellectual property.

If you thought the theft of IP by China was bad, Serco's complete control of our patents is much worse. Below, you will read our case study of one entrepreneur who was ripped off royally by this corrupt patent system. And we happen to know many others like McKibben, especially in the energy sector, who aren't able to make theri stories public… yet.

FACEBOOK UNMASKED: HOW THE WORLD'S MOST RELEVANT ENTREPRENEUR WAS SCREWED BY ZUCKERBERG

SERCO SERVICES IN AMERICA – IN ITS OWN WORDS

It is often best to see what a corporation says about itself on its own website. Serco reveals the extensive controls they have established in all aspects of American life through bragging about their accomplishments. Once you have seen the pervasive control that Serco has on the U. S. military and all aspects of government, you may be shocked.

You can read these descriptions about Serco at: **https://www.serco-na.com/** . The descriptions are lifted from their website, in their own words:

Comprehensive Support for Mission-Critical Communications and IT Systems

Serco provides comprehensive support for mission-critical communications and IT systems used by military, intelligence and civilian government clients. From information architecture to installation and maintenance, Serco covers the full technology life cycle in some of the most demanding and secure IT environments in the world.

Serco is known for our deep domain knowledge, ability to handle large scale projects, and exceptional customer focus. We have played an important role in evolving critical C4ISR systems that continue to make information superiority a key advantage of the U.S. armed forces.

We work with a range of federal civilian agencies and every branch of the armed forces to deliver solutions that advance their missions. Our flexible, comprehensive offering covers IT modernization efforts, including software application development, database

management, systems/network engineering and administration, Information Assurance, and Help Desk services.

Engineer, Furnish, Install & Test Services – From command and control centers to sensors and antennas, Serco supports the critical communications infrastructure that underpins defense, homeland security, and intelligence capabilities. We provide design engineering, installation, testing, Operations and Maintenance (O&M) services for new, upgraded or fielded systems and equipment in a range of mission-critical environments for the U.S. Air Force, U.S. Army, U.S. Navy, DHS and other federal agencies.

Ship Modernization Services – Serco supports the ongoing modernization of the fleet to incorporate the latest technology, minimize downtime, and meet exacting budgets and timelines. Serco's support for the U.S. Navy and U.S. Coast Guard has grown quickly based on our ability to assemble high quality teams, anticipate client needs, and consistently deliver on our promises.

Serco provides systems integration, installation, repair, and testing for the systems that advance operational capabilities globally.

Hardware Production & Test Services – Serco builds and delivers "mission-ready" IT, networking and communications systems adapted to the needs of clients in defense, intelligence, and homeland security.

Application & Eligibility Support – Serco has experience processing millions of applications in a highly efficient and secure manner to achieve high levels of citizen satisfaction. We provide application processing, decision support, benefits management, case management, call centers, and fraud prevention.

Document Management – Serco provides full life-cycle support for document conversion, data entry, content management and records management required for large-scale programs and complying with all applicable regulations.

Workforce Development – Serco provides workforce management services across the entire hire-to-retire journey, including recruitment, workforce analytics and planning, benefits, training, consulting, leader development, incentives and compensation, organizational design, and change management.

Facilities Management Solutions – Serco provides full lifecycle facilities and asset management solutions, utilizing IBM TRIRIGA, to enable data driven-decisions that achieve cost savings, provide superior work places, and ensure regulatory compliance for organizations.

Cyber Architecture – We employ an Enterprise Architecture-based approach to cyber operations that provides a powerful means to integrate cyber security within the framework of your mission and critical systems, so as to promote effective governance, standardized infrastructure, and consistent execution.

Cyber Awareness – We help our clients develop the ability to effectively monitor, detect, and react to cyber intrusions before they cause significant damage. This includes maintaining global situational awareness and undertaking effective defensive and offensive countermeasures.

Cyber Education – Because the human actor often remains the most vulnerable link in the chain, Serco provides an integrated approach to training, compliance, and monitoring of cyber security policies and procedures.

IT Infrastructure, including:

- Application Development
- Cloud Migration
- Datacenter Operations
- Database Development & Maintenance
- Information Assurance

- Helpdesk & IT Support
- Virtualization
- Wireless Mobility & BYOD
- Cloud Migration
- Core Networking
- Data Center Consolidation
- LAN/WAN Networks
- Satellite Communications
- Voice & Video Networks
- Wireless Communications

Acquisition Logistics – Serco provides acquisition support to our military clients on a variety of advanced weapons systems, with a focus on maximizing operational readiness.

Emergency Response – Serco has assisted with large scale emergency response efforts, including establishing rapid deployment medical facilities in Haiti and Chile following natural disasters. We help the Navy to deploy transportable hospitals that include laboratory, radiology, pharmacy, patient wards, and operating wards.

Logistics Data Management – Serco has the expertise required to design and manage large-scale logistics data systems to provide our clients with asset visibility, controls, and analytics required for complex operations.

Logistics Planning & Engineering – Serco has helped manage the large-scale movement of equipment and assets as a trusted agent on behalf of the military, with a focus on program efficiency, cost avoidance, and repurposing of valuable property.

Supply Chain Management – Serco manages advanced IT systems and databases to provide total visibility across the military supply chain to enable real-time monitoring and forecasting of materiel needs in dynamic environment.

Warehouse & Depot Management – We provide comprehensive ISO 9001:2000 certified support for sustainment, maintenance, and repair at depots and warehouses to maintain a high degree of inventory accuracy and reduce waste at warehouses and depots.

Systems Engineering Capabilities, include:

- Aviation and ATM systems
- Complex simulation & 3D modeling
- C4I Systems
- Intelligent traffic management
- Integrated logistics support
- Missile defense
- Safety & environmental engineering
- Space-based communications
- Survivability engineering
- Tactical datalinks

Personnel Services – Serco has helped to design and run some of the most sophisticated government, military personnel, and military family support programs, including the US Army Career and Alumni Program (ACAP), VA for Vets, Army OneSource, the USA Wounded Warrior Advocate Program, and others.

Planning – Whether your work force is military or civilian, we have the analytic experience and associated models to develop a strategic plan operating within your constraints which supports your mission and readiness.

Analysis – Our Team has conducted policy, compensation, incentives, and retention consulting for the Army and Navy for decades. Incentives take many forms, but the bottom line of the analysis is to determine the optimal mix of controls to produce the highest readiness at lowest cost within the legal, policy, and budgetary constraints.

Recruitment – We understand military and government life and have the skills and experience necessary to effectively draw in top talent while communicating the rewards and benefits of military service.

Processing and Administration – From processing to benefits administration to discharging, our administrative support experts enable organizations to remain operationally efficient, reduce errors and cycle times, and improve satisfaction of military members and their families.

Military Career Transition – Serco understands the challenges of transitioning from military to civilian life. We have pioneered programs to promote employment and address common family stresses. Serco's military career transition specialists work with soldiers to help them establish a foothold in the civilian world, maximizing the skills and abilities that made them successful in the military.

Service Member and Family Counseling – Millions of family members encounter unique challenges associated with government and military life – long deployments, relocations, and related stresses. We are there for service members and their families and our people bring understanding, empathy, and ability to personally connect through supportive counseling.

Wounded Warrior Support – Warriors have the courage to overcome any challenge. We support courageous solders that have sustained serious injuries in every way we know how – through one-on-one counseling, emotional support, family counseling and related services.

Training and Learning Solutions

Serco develops training programs and learning solutions that enable our clients to improve mission readiness, incorporate lessons learned, and hone the skills that directly contribute to mission success.

Mission Command Training – We operate a state-of-the-art simulation center used by the U.S. Army for mission command training.

Warfighting Exercises – Serco supports the U.S. Marine Corps with programs covering warfighting skills, technology training, mission exercises, joint operations, and combat simulation.

Healthcare Support Services

Serco provides non-clinical support services that enable hospitals and medical centers to deliver clinical services more efficiently, while improving patient satisfaction and bottom line performance.

Environmental services – Our cleaning services provide a uniformly high standard of cleaning across the entire facility, creating the impression of a high quality, well run, and safe environment.

Switchboard & operations center – At the heart of our solution is a centralized "command center" in which all incoming calls are routed, dispatch and service requests are made, and complaints are logged and quickly resolved.

Patient transport & logistics – Using our standardized platform, transport resources are optimized across the facility to improve on-time starts, reduce wait times, and improve the patient experience.

Transportation

Serco keeps critical transportation systems operating safely and efficiently. On the ground, we integrate the latest technology with our experience in running some of the world's most advanced traffic management programs. In the air, Serco has expertise in a full range of air transportation solutions, which includes air traffic control, airport management and aviation related technology and equipment.

Smart highways. Safe skyways. Wired metros. Shared bikes. Whether you travel by airplane, car, rail, boat, or bicycle, Serco can help you get there faster, safer, smarter.

With an outstanding safety record, Serco currently manages over 192,000 square miles of airspace worldwide, more than any other private company, and controls over 7 million aircraft movements a year. We operate 63 Federal Aviation Administration (FAA) Visual Flight Rules Air Traffic Control Towers in the United States. In the United States alone, we help more than 10 million commercial passengers each year reach their destinations safely.

Intelligent Transportation Systems– Serco is a global leader in design and operation of intelligent transportation systems. This includes traffic management centers, bridge and tunnel operations, traffic signal maintenance, incident management and safety service patrols, and tolling services.

Transit Services – Serco has decades of experience providing operations, maintenance and marketing support for commuter rail, light rail, rapid transit, trams, and street cars.

Parking Management Services– Serco provides total management for parking systems including installing and operating parking meter systems, managing parking space availability, and managing parking enforcement and citations.

Aviation Operations – Serco provides air traffic control operations at en route centers, radar approach control, airport towers, and airline ramp towers. We are experts in designing and implementing Safety Management Systems (SMS) to support safety excellence across all our aviation operations.

Infrastructure Services – Serco provides engineering and support for a full range of aviation infrastructure, including ground electronics maintenance, engineering and installation of ATM systems, and related communications, navigation, surveillance and weather systems.

Flight Support Services – Serco provides a range of flight support services including weather forecasting, pilot briefings, and aeronautical information management. We offer instructional services in subjects including air traffic control, flight safety, and safety management systems. Serco is the only non-state organization authorized to issue Air Traffic Control licenses on behalf of an ICAO signatory state.

Intelligent Transportation Systems

Serco has 30 years of experience developing and operating transportation solutions for national highways, states, major cities, and local roads.

- Road, Tunnel, Bridge & Traffic Management
- System development & integration
- Operational control center development
- Incident detection & management
- Lane control signals
- CCTV control & surveillance
- Intelligent congestion management
- Manual & automated toll collection
- Road-side infrastructure

- Traffic signals & management
- Tunnel management
- Vehicle recovery & emergency services
- Equipment & vehicle maintenance
- Air pollution monitoring
- Bus tracking
- Passenger mobile information services
- Asset management systems

Transit Services

Serco is internationally recognized as one of the most experienced providers designing and managing heavy rail, light rail, metro and bus fleets.

Heavy rail – Serco manages over 7,404 miles of heavy rail services. We draw from the best practices learned from across decades of operations, on eight unique rail contracts, to help our clients achieve world-class service.

Light rail – Serco is a global leader in light rail systems with the expertise in developing and managing this important element of an integrated transportation system.

Metro – Metro systems continue to play a critical role in high-density urban areas. Serco has achieved unmatched performance in operating large-scale metro systems across the globe.

Bus Service – Our services encompass urban city buses, inter-urban express and coach buses, metro rail feeder services, emergency replacement services, bus rapid transport, and airport landside transportation.

Serco Transit Services, include*:*

- Train, metro, bus & ferry operations
- Control center operations
- Security management
- Transportation mode integration
- Rail depot facility management
- Rolling stock maintenance
- Asset planning & deployment
- Track, signaling & traction power maintenance
- Passenger real-time information
- Trip planning technology
- Station layout & design
- Ticketing information & pricing
- Car park management
- Passenger demand management
- Bus network development, scheduling & management
- Vehicle maintenance
- Bus depot, stations, and control center operations
- Driver training & education

Aviation Operations & Management

Serco offers an integrated approach to airport operators who wish to achieve highly efficient operations, improved passenger flow, and on time performance, while operating at the highest levels of safety and security.

Key Services, include*:*

- Air Traffic Control
- Airport facilities management & maintenance

- Airport security
- Airport advertising & retailing
- Training – Aviation management & security
- Ground handling
- Passenger handling
- Safety Management Systems
- Freight/cargo handling
- Ramp/apron services
- Baggage handling
- Grounds management
- Airport ground lighting management
- Fuel management
- Bird control
- Aircraft ground support equipment maintenance
- Airfield & roads management
- Vehicle fleet management
- Asset & stock management
- Logistics services
- Snow & ice removal

SERCO'S SERVICE ABILITIES ARE HIGHLY EXAGGERATED

It may come as a shock to you that SERCO seems to be able to "do anything" in all areas of business and warfare. What company can say that they have all of this "expertise" in so many diverse field of knowledge? No one can do so and still be effective and efficient. Serco is well known for being about 65% efficient. This should be expected. No company has the know-how and expertise to be efficient at "all things."

Essentially, Senior Executive Service members throughout the U. S. federal government simply grant contracts and Serco tries to "keep up." A recent example of its incompetence is in the Obamacare website rollout which was extremely costly, yet, to this day, is highly unfunctional to the average user.

Essentially, SERCO is like a monopoly of U. S. data management run by a foreign nation. This "selling out" of U. S. government contracts is corrupt cronyism that is well hidden from the public. These deals happen as no bid contracts are shuffled across SES members' desks and follow the common pattern of choosing the usual government contractor that pays-to-play.

SERCO U. S. GOVERNMENT CONTRACTS

It may be hard to imagine all of the contracts that Serco has with the U. S. government so we listed some of the most obvious ones for you. The list of U. S. contracts is on the Serco website, with additional information on Wikipedia. It is not a secret that Serco gets any contract it wants and often with no other companies bidding.

PATRIOTS MIGHT ASK, "WHY WOULD WE CONTINUALLY GIVE GOVERNMENT CONTRACTS TO FOREIGN NATIONS AND CORPORATIONS THAT HAVE A TERRIBLE TRACK RECORD OF EFFICIENCY?"

We do not know a good answer to that question. Any America would respond by saying that it is wrong, crazy, and economically unsound to pay foreigners to manage sensitive American interests. Patriots around the world do not support Queen Elizabeth and the British Monarchy in operating, managing, and financially benefitting from our countries any longer.

The list below is not comprehensive and there are many ways to hide the extensive number of Serco contracts with the U. S. military and government.

Air Force

Air Combat Command
Air Force Director of Personnel
Air Force District of Washington
Air Force Electronics Systems Center
Air Force Education and Training Command
Air Force Information Warfare Center
Air Force Institute for Advanced Distributed Learning
Air Force Materiel Command
Air Force Research Lab
Air Force Space Command
Space and Missile System Center
Tinker Air Force Base

Army

Army Communications Electronics Command
Army Defense Ammunition Center
Army Enterprise Information Systems
Army Human Resources Command
Army IMCEM
Army Materiel Command/Aberdeen Proving Ground
Army Medical Department
Army Research Labs
Army Research, Development & Engineering Center
Army Space and Missile Defense Command
Army Training & Doctrine Command
National Ground Intelligence Center
Army Family and Morale, Welfare and Recreation Command
Army Medical Command
Army Installation Management Command
Army Recruiting Command

Department of Defense

Defense Acquisition University
Defense Ammunition Center
Defense Information Systems Agency
Defense Logistics Agency
Defense Threat Reduction Agency
Missile Defense Agency
National Geospatial Intelligence Agency
National Security Agency
National Security Personnel System Program Executive Office
Office of Intelligence & Analysis
Office of the Secretary of Defense
United States Air Force
Washington Headquarters Service

Joint Central Command

J6, Joint Staff
Joint Advanced Distributed Learning Co-Laboratory
Joint Forces Warfighting Center
North American Aerospace Defense Command
Northern Command
Southern Command
Strategic Command (Space Command)

Navy

Center for Surface Combat Systems – Dahlgren
Commander Navy Installations Command
Financial Management and Comptroller
Naval Air Systems Command

Naval Education and Training Command
Naval Inventory Control Point
Naval Sea Systems Command
Naval Supply Systems Command
Naval Surface Warfare Center
Navy Office of the Chief of Human Resources
Navy Public Works Center
Navy Recruiting Command
Office of Naval Intelligence
Space and Naval Warfare Systems Command
Bureau of Medicine and Surgery
Naval Reserves

Marine Corps

Marine Corps Reserve
Marine Corps Systems Command

Department of Agriculture

Animal and Plant Health Inspection Service
Forest Service
Risk Management Agency

Department of Commerce

National Weather Service
Patent & Trademark Office
United States Census Bureau

Department of Energy

National Nuclear Security Administration

Department of Health & Human Services

Center for Medicare & Medicaid Services

National Institutes of Health

Indian Health Service

Department of Homeland Security

Customs & Border Protection
Directorate of Preparedness
Federal Emergency Management Agency
Federal Protective Service
Immigration & Customs Enforcement
Transportation Security Administration
United States Citizenship & Immigration Services
US-VISIT Office of Policy
U.S. Coast Guard

Department of Housing and Urban Development

Department of Housing and Urban Development
Public and Indian Housing

Department of Interior

National Park Service

Office of Inspector General

Department of Justice

Antitrust Division
Bureau of Prisons
Civil Rights
Criminal Division
Drug Enforcement Administration
Executive Office for the U.S. Attorneys
Federal Bureau of Investigation
Justice Management Division
Organized Crime Drug Enforcement Task Force
United States Marshals Service

Department of Labor

Occupational Safety & Health Administration
Office of the Chief Information Officer

Department of State

Bureau of Consular Affairs
Foreign Service Institute
Population, Refugees, and Migration

Department of Transportation

Federal Aviation Administration
National Highway Traffic Safety Administration

VOLPE Transportation System Center

Department of Treasury

Comptroller of the Currency
Internal Revenue Service
United States Secret Service

Department of Veterans Affairs

Board of Veterans Appeals
Veterans Benefit Administration
Veterans Health Administration

General Services Administration

Federal Supply Service
Federal Technology Service

Board of Governors of the Federal Reserve System

Central Intelligence Agency

Congressional Commission on China

Congressional Research Service

Director of National Intelligence

Federal Communications Commission

Federal Deposit Insurance Corporation

Federal Trade Commission

Government Accountability Office

Government Printing Office

International Trade Commission

Library of Congress

Nuclear Regulatory Commission

Pension Benefit Guaranty Corporation

Smithsonian Institution

U.S. Postal Service

U.S. Securities and Exchange Commission

Social Security Administration

U.S. Army

U.S. Air Force

U.S. Coast Guard

U.S. Department of Health & Human Services

U.S. Department of Homeland Security

U.S. Department of Justice

U.S. Department of State

U.S. Intelligence Agencies

U.S. Marine Corps

U.S. Navy

U.S. Patent and Trademark Office

City of Chicago

City of Colorado Springs

City of Palo Alto, CA

City of San Francisco

Georgia Department of Transportation

Louisiana Department of Transportation

Montgomery County, MD

San Francisco Municipal Transportation Agency

The list above does not include the many contracts Serco has with U. S. corporations, states, cities, or other companies. No one knows the true extent of the strangle-hold Serco has on America. If you pay attention closely you will notice that when a serious data management problem arises, it is usually Serco that has the contract to safeguard that data.

SERCO'S FUTURE IN AMERICA

It is obvious to see from the presentation above that Serco has spread its tentacles into every aspect of the U. S. government and the U. S. military. Serco has also dominated many other industries in the U. S. economy and yet their name and influence is little known or recognized. Any American, when presented with this information above, would immediately conclude that there is no good reason to let Brits do what Americans can do quite nicely, thank you.

Why would we sell out our most sensitive data to a foreign country who has, quite frankly, not really been our friend from the beginning. Indeed, it does look like the American Revolution has not really ended and that the "Crown" still taxes every American for business deals that the common citizen is not aware of. No American chooses "Britain First" when it comes to providing services for our military or government — that makes no sense at all.

Serco is simply the 'tip of the iceberg' when it comes to British "interests" in America. Many of the old English, Dutch, and German bankers have benefited greatly by institutions like the U. S. Federal Reserve, U. S. Central Banks, the World Bank, the World Trade Organization, and the International Monetary Fund. Once you consider the UK's part in these multi-national (global) organizations, you can track billions of dollars flowing out of America and into the pocket of the British Crown.

The British Crown "Agents" are indeed a long-standing set of monopolies that America has had to contend with since the founding of the British inspired Council on Foreign Relations, the chief body that creates U. S. foreign policy for the U. S. State Department. Britain is always considered to be our closest partner in all things war, military intelligence, and global domination. We share our military "intelligence" with the UK. But it might surprise some people to learn that the British-American (Anglo-American) connection reaches deep into the pockets of U. S. tax payers through companies like Serco.

Serco, and other foreign corporations are the usual "no-bid" contractors always selected by the Senior Executive Service members throughout the federal government who make sure the status quo is not disturbed and that the "old boys" get their piece of the pie. This type of selling-out of America is an erosion of the U. S. Republic and an assault on the U. S. Constitution and the U. S. Bill of Rights. Tax-payers are being sold out to foreign countries while services for U. S. soldiers decline and the data being managed by Serco and others is consistently compromised.

It is time to fire Serco and let Americans do the work and gain the benefit of receiving the hard-earned dollars of U. S. tax-payers. The Crown of England, the Bank of England, the City of London, and British owned companies "NEED NOT APPLY."

For Further Information on Serco, go to:

The American Intelligence Media is a digital resource for truth news creators all around the world. We do the deep research for you and provide you resource materials so that

you can educate and enlighten your audience with your unique talents and voice. Please repost our article in any way you feel best to spread out this intel around the world.

Also link to this post below where we keep an ongoing dump of Serco material that is difficult to find on the internet:

SERCO Intel Dump Page

Use these additional resources, including Abel Danger websites, to shine a big, bright, global light on this corruption. We are ushering in a new age of peace and prosperity. **Join our movement**.

SERCO OWNS THE WORLD, | BIG BROTHER WATCH

Serco outsources to governments all over the world

OMG SERCO WINS BID FOR OBAMACARE CONTRACT

This video was done in 2014. The YouTuber is astonished to find how many corporations are attached to Serco. Start the video at 3:12 mark. Then go to Muckety and see how different the chart looks now.

APX 074

Recommended resources:

GRETA: THE OBAMACARE SERCO DEAL SMELLS ROTTEN

CONGRESS BEGINS SCRUTINY OF OBAMACARE WEBSITE'S PROBLEMS

WHAT IS SERCO HIDING?

Electronic Tagging

APX 075

Serco Associated with The GEO Group

SERCO AND IMMIGRATION

SECURITY GIANT SERCO CHIEF RESIGNS

VICIOUS SERCO? UK PUBLIC SERVICE COMPANY ENTWINED IN MAJOR FRAUD SCANDAL

G4S AND SERCO FACE £50 MILLION FRAUD INQUIRY

G4S and Serco woes deepen with British fraud investigation

PRESS THIS TWITTER FACEBOOK 230
GOOGLE

Reblog Like

8 bloggers like this.

35 Comments ADD YOURS

APX 076

...

←Older Comments

1

christopherearlstrunk on April 23, 2018 at 2:18 pm **Reply**

Good work!

In the best of all possible worlds, this is sufficient for a beginning outline for 18 USC 1961 according to **https://www.scribd.com/document/106931000/USDOJ-RICO-Manual-of-Federal-Prosecutors-1993**. THKS!

Still Cogitating!

★ Like

2

Ri-chard on April 23, 2018 at 2:30 pm **Reply**

Please consider 3i and Blackrock are the giants not SERCO and SES.

★ Like

3

R Seymour on May 18, 2018 at 9:50 am **Reply**

Good work!
After you completely expose the British Crown angle in the plunder of USA, you might examine the JEWISH angle. As far as I can tell, it is far more destructive…..

http://republicbroadcasting.org/news/homeland-security-another-jewish-racket/

★ Like

4

Ri-chard on May 18, 2018 at 12:34 pm **Reply**

Who feeds the Crown/i believe it those who control movement of money and land ownership. always follow the money and you will connects the dots to the Jewish Zionist Khazarian money changers.
There is much info out there from those that chase SERCO and SES. they are small

fry ans way too far away from the head of the snake. consider exploring 3i or Blackstone. As the feeder bags for the Crown – Note the in your face message of the 3i logo> **https://www.3i.com/** and there list of friendlie$ Jews and Zionist **https://ir.blackstone.com/investors/events/default.aspx**

★ Like

5

Our Spirit on May 18, 2018 at 12:36 pm

Send us YOUR research. Make sure to include actual documents and indictable evidence that proves these claims. We have our hands full right now with other trails.

★ Like

6

sorgfelt on May 18, 2018 at 11:59 am **Reply**

Please don't equate SES with SERCO. SES is to civil service as officers are to enlisted. SES are appointed by the President to manage the government and can be fired at will. Deep State members can be SES, but the reverse is not true.

★ Like

7

Our Spirit on May 18, 2018 at 12:29 pm **Reply**

If you have been following our research, this comment would not have been necessary. Your assessment is naive and doesn't capture the true purpose and intent of SES or Serco. SES has infiltrated our government as a separate unit. We have posted the Plum Books and you can check out the names yourself – Mueller, Rosenstein, Freidrich, Page, Strzok, McCabe, Podesta….and soooo many more. They award no-bid contracts to foreign aligned and owned Serco – which all tracks back to the Crown Agents, the Golden Share, and the Brits. The good patriots of both countries are being controlled by evil forces of the Queen to the Pope. Put any name in our search bar and see what we have uncovered so far. And for those of you that scream "the Queen is being controlled-it's not her fault" then tell her that she needs to step up and reveal her handlers.

★ Like

APX 078

8

sorgfelt on May 18, 2018 at 12:45 pm

I know some SES members. They basically got themselves promoted into those positions from civil service by making formal applications and being accepted by the Department for which they work. I am quite sure they have nothing to do with either SERCO or royalty.

★ Like

9

Our Spirit on May 18, 2018 at 12:53 pm **Reply**

You are so wrong. SES is an enemy of We the People. They are a unit of government outside of the rule of law, the constitution…they are obstructionists. They receive clandestine training at Senior Executive Institute and they most certainly don't tell YOU what they are up to. They are: Robert Mueller, Rod Rosenstein, Jeff Sessions, Lisa Page, Dabney Friedrich, Peter Strzok, Christopher Wray, Trey Gowdy, Andrew McCabe, John Podesta….and we could go on. The list is long. But if you had been doing your homework and research for yourself in the Plum Books, you would see that they are the 'stink of the swamp'….all the while giving no-bid contracts to Serco which is tied to the British Crown. They are more than Obama's army; they are the hidden army of the British Crown.

We do our homework here at AIM4Truth. If you want to leave comments in the future, don't be ignorant. Know what you are talking about.

★ Like

…

←Older Comments

Leave a Reply

Enter your comment here...

APX 079

REMARKS

Remarks by Vice President Pence on the Administration's Policy Toward China

FOREIGN POLICY

Issued on: **October 4, 2018**

★ ★ ★

The Hudson Institute
Washington, D.C.

11:07 A.M. EDT

THE VICE PRESIDENT: Thank you, Ken, for that kind introduction. To the Members of the Board of Trustees, to Dr. Michael Pillsbury, to our distinguished guests, and to all of you who, true to your mission in this place, "think about the future in unconventional ways" –- it is an honor to be back at the Hudson Institute.

For more than a half a century, this Institute has dedicated itself to "advancing global security, prosperity, and freedom." And while Hudson's hometowns have changed over the years, one thing has been constant: You have always advanced that vital truth, that American leadership lights the way.

And today, speaking of leadership, allow me to begin by bringing greetings from a great champion of American leadership at home and abroad –- I bring greetings from the 45th President of the United States of America, President Donald Trump. (Applause.)

From early in this administration, President Trump has made our relationship with China and President Xi a priority. On April 6th of last year, President Trump welcomed President Xi to Mar-a-

Lago. On November 8th of last year, President Trump traveled to Beijing, where China's leader welcomed him warmly.

Over the course of the past two years, our President has forged a strong personal relationship with the President of the People's Republic of China, and they've worked closely on issues of common interest, most importantly the denuclearization of the Korean Peninsula.

But I come before you today because the American people deserve to know that, as we speak, Beijing is employing a whole-of-government approach, using political, economic, and military tools, as well as propaganda, to advance its influence and benefit its interests in the United States.

China is also applying this power in more proactive ways than ever before, to exert influence and interfere in the domestic policy and politics of this country.

Under President Trump's leadership, the United States has taken decisive action to respond to China with American action, applying the principles and the policies long advocated in these halls.

In our National Security Strategy that the President Trump released last December, he described a new era of "great power competition." Foreign nations have begun to, as we wrote, "reassert their influence regionally and globally," and they are "contesting [America's] geopolitical advantages and trying [in essence] to change the international order in their favor."

In this strategy, President Trump made clear that the United States of America has adopted a new approach to China. We seek a relationship grounded in fairness, reciprocity, and respect for sovereignty, and we have taken strong and swift action to achieve that goal.

As the President said last year on his visit to China, in his words, "we have an opportunity to strengthen the relationship between our two countries and improve the lives of our citizens." Our vision of the future is built on the best parts of our past, when America and China reached out to one another in a spirit of openness and friendship.

When our young nation went searching in the wake of the Revolutionary War for new markets for our exports, the Chinese people welcomed American traders laden with ginseng and fur.

When China suffered through indignities and exploitations during her so-called “Century of Humiliation,” America refused to join in, and advocated the “Open Door” policy, so that we could have freer trade with China, and preserve their sovereignty.

When American missionaries brought the good news to China’s shores, they were moved by the rich culture of an ancient and vibrant people. And not only did they spread their faith, but those same missionaries founded some of China’s first and finest universities.

When the Second World War arose, we stood together as allies in the fight against imperialism. And in that war’s aftermath, America ensured that China became a charter member of the United Nations, and a great shaper of the post-war world.

But soon after it took power in 1949, the Chinese Communist Party began to pursue authoritarian expansionism. It is remarkable to think that only five years after our nations had fought together, we fought each other in the mountains and valleys of the Korean Peninsula. My own father saw combat on that frontier of freedom.

But not even the brutal Korean War could diminish our mutual desire to restore the ties that for so long had bound our peoples together. China’s estrangement from the United States ended in 1972, and, soon after, we re-established diplomatic relations and began to open our economies to one another, and American universities began training a new generation of Chinese engineers, business leaders, scholars, and officials.

After the fall of the Soviet Union, we assumed that a free China was inevitable. Heady with optimism at the turn of the 21st Century, America agreed to give Beijing open access to our economy, and we brought China into the World Trade Organization.

Previous administrations made this choice in the hope that freedom in China would expand in all of its forms -– not just economically, but politically, with a newfound respect for classical liberal principles, private property, personal liberty, religious freedom — the entire family of human rights. But that hope has gone unfulfilled.

The dream of freedom remains distant for the Chinese people. And while Beijing still pays lip service to “reform and opening,” Deng Xiaoping’s famous policy now rings hollow.

Over the past 17 years, China's GDP has grown nine-fold; it's become the second-largest economy in the world. Much of this success was driven by American investment in China. And the Chinese Communist Party has also used an arsenal of policies inconsistent with free and fair trade, including tariffs, quotas, currency manipulation, forced technology transfer, intellectual property theft, and industrial subsidies that are handed out like candy to foreign investment. These policies have built Beijing's manufacturing base, at the expense of its competitors -– especially the United States of America.

China's actions have contributed to a trade deficit with the United States that last year ran to $375 billion –- nearly half of our global trade deficit. As President Trump said just this week, in his words, "We rebuilt China" over the last 25 years.

Now, through the "Made in China 2025" plan, the Communist Party has set its sights on controlling 90 percent of the world's most advanced industries, including robotics, biotechnology, and artificial intelligence. To win the commanding heights of the 21st century economy, Beijing has directed its bureaucrats and businesses to obtain American intellectual property –- the foundation of our economic leadership -– by any means necessary.

Beijing now requires many American businesses to hand over their trade secrets as the cost of doing business in China. It also coordinates and sponsors the acquisition of American firms to gain ownership of their creations. Worst of all, Chinese security agencies have masterminded the wholesale theft of American technology –- including cutting-edge military blueprints. And using that stolen technology, the Chinese Communist Party is turning plowshares into swords on a massive scale.

China now spends as much on its military as the rest of Asia combined, and Beijing has prioritized capabilities to erode America's military advantages on land, at sea, in the air, and in space. China wants nothing less than to push the United States of America from the Western Pacific and attempt to prevent us from coming to the aid of our allies. But they will fail.

Beijing is also using its power like never before. Chinese ships routinely patrol around the Senkaku Islands, which are administered by Japan. And while China's leader stood in the Rose Garden at the White House in 2015 and said that his country had, and I quote, "no intention to militarize" the South China Sea, today, Beijing has deployed advanced anti-ship and anti-air missiles atop an archipelago of military bases constructed on artificial islands.

China's aggression was on display this week, when a Chinese naval vessel came within 45 yards of the USS Decatur as it conducted freedom-of-navigation operations in the South China Sea, forcing our ship to quickly maneuver to avoid collision. Despite such reckless harassment, the United States Navy will continue to fly, sail, and operate wherever international law allows and our national interests demand. We will not be intimidated and we will not stand down. (Applause.)

America had hoped that economic liberalization would bring China into a greater partnership with us and with the world. Instead, China has chosen economic aggression, which has in turn emboldened its growing military.

Nor, as we had hoped, has Beijing moved toward greater freedom for its own people. For a time, Beijing inched toward greater liberty and respect for human rights. But in recent years, China has taken a sharp U-turn toward control and oppression of its own people.

Today, China has built an unparalleled surveillance state, and it's growing more expansive and intrusive – often with the help of U.S. technology. What they call the "Great Firewall of China" likewise grows higher, drastically restricting the free flow of information to the Chinese people.

And by 2020, China's rulers aim to implement an Orwellian system premised on controlling virtually every facet of human life — the so-called "Social Credit Score." In the words of that program's official blueprint, it will "allow the trustworthy to roam everywhere under heaven, while making it hard for the discredited to take a single step."

And when it comes to religious freedom, a new wave of persecution is crashing down on Chinese Christians, Buddhists, and Muslims.

Last month, Beijing shut down one of China's largest underground churches. Across the country, authorities are tearing down crosses, burning bibles, and imprisoning believers. And Beijing has now reached a deal with the Vatican that gives the avowedly atheist Communist Party a direct role in appointing Catholic bishops. For China's Christians, these are desperate times.

Beijing is also cracking down on Buddhism. Over the past decade, more than 150 Tibetan Buddhist monks have lit themselves on fire to protest China's repression of their beliefs and their culture. And in Xinjiang, the Communist Party has imprisoned as many as one million Muslim Uyghurs in government camps where they endure around-the-clock brainwashing. Survivors of the camps

have described their experiences as a deliberate attempt by Beijing to strangle Uyghur culture and stamp out the Muslim faith.

As history attests though, a country that oppresses its own people rarely stops there. And Beijing also aims to extend its reach across the wider world. As Hudson's own Dr. Michael Pillsbury has written, "China has opposed the actions and goals of the U.S. government. Indeed, China is building its own relationships with America's allies and enemies that contradict any peaceful or productive intentions of Beijing."

In fact, China uses so-called "debt diplomacy" to expand its influence. Today, that country is offering hundreds of billions of dollars in infrastructure loans to governments from Asia to Africa to Europe and even Latin America. Yet the terms of those loans are opaque at best, and the benefits invariably flow overwhelmingly to Beijing.

Just ask Sri Lanka, which took on massive debt to let Chinese state companies build a port of questionable commercial value. Two years ago, that country could no longer afford its payments, so Beijing pressured Sri Lanka to deliver the new port directly into Chinese hands. It may soon become a forward military base for China's growing blue-water navy.

Within our own hemisphere, Beijing has extended a lifeline to the corrupt and incompetent Maduro regime in Venezuela that's been oppressing its own people. They pledged $5 billion in questionable loans to be repaid with oil. China is also that country's single largest creditor, saddling the Venezuelan people with more than $50 billion in debt, even as their democracy vanishes. Beijing is also impacting some nations' politics by providing direct support to parties and candidates who promise to accommodate China's strategic objectives.

And since last year alone, the Chinese Communist Party has convinced three Latin American nations to sever ties with Taipei and recognize Beijing. These actions threaten the stability of the Taiwan Strait, and the United States of America condemns these actions. And while our administration will continue to respect our One China Policy, as reflected in the three joint communiqués and the Taiwan Relations Act, America will always believe that Taiwan's embrace of democracy shows a better path for all the Chinese people. (Applause.)

Now these are only a few of the ways that China has sought to advance its strategic interests across the world, with growing intensity and sophistication. Yet previous administrations all but ignored

China's actions. And in many cases, they abetted them. But those days are over.

Under President Trump's leadership, the United States of America has been defending our interests with renewed American strength.

We've been making the strongest military in the history of the world stronger still. Earlier this year, President Trump signed into law the largest increase in our national defense since the days of Ronald Reagan -- $716 billion to extend the strength of the American military to every domain.

We're modernizing our nuclear arsenal. We're fielding and developing new cutting-edge fighters and bombers. We're building a new generation of aircraft carriers and warships. We're investing as never before in our armed forces. And this includes initiating the process to establish the United States Space Force to ensure our continued dominance in space, and we've taken action to authorize increased capability in the cyber world to build deterrence against our adversaries.

At President Trump's direction, we're also implementing tariffs on $250 billion in Chinese goods, with the highest tariffs specifically targeting the advanced industries that Beijing is trying to capture and control. And as the President has also made clear, we will levy even more tariffs, with the possibility of substantially more than doubling that number, unless a fair and reciprocal deal is made. (Applause.)

These actions — exercises in American strength — have had a major impact. China's largest stock exchange fell by 25 percent in the first nine months of this year, in large part because our administration has been standing strong against Beijing's trade practices.

As President Trump has made clear, we don't want China's markets to suffer. In fact, we want them to thrive. But the United States wants Beijing to pursue trade policies that are free, fair, and reciprocal. And we will continue to stand and demand that they do. (Applause.)

Sadly, China's rulers, thus far, have refused to take that path. The American people deserve to know: In response to the strong stand that President Trump has taken, Beijing is pursuing a comprehensive and coordinated campaign to undermine support for the President, our agenda, and our nation's most cherished ideals.

I want to tell you today what we know about China's actions here at home — some of which we've gleaned from intelligence assessments, some of which are publicly available. But all of which are fact.

As I said before, as we speak, Beijing is employing a whole-of-government approach to advance its influence and benefit its interests. It's employing this power in more proactive and coercive ways to interfere in the domestic policies of this country and to interfere in the politics of the United States.

The Chinese Communist Party is rewarding or coercing American businesses, movie studios, universities, think tanks, scholars, journalists, and local, state, and federal officials.

And worst of all, China has initiated an unprecedented effort to influence American public opinion, the 2018 elections, and the environment leading into the 2020 presidential elections. To put it bluntly, President Trump's leadership is working; and China wants a different American President.

There can be no doubt: China is meddling in America's democracy. As President Trump said just last week, we have, in his words, "found that China has been attempting to interfere in our upcoming [midterm] election[s]."

Our intelligence community says that "China is targeting U.S. state and local governments and officials to exploit any divisions between federal and local levels on policy. It's using wedge issues, like trade tariffs, to advance Beijing's political influence."

In June, Beijing itself circulated a sensitive document, entitled "Propaganda and Censorship Notice." It laid out its strategy. It stated that China must, in their words, "strike accurately and carefully, splitting apart different domestic groups" in the United States of America.

To that end, Beijing has mobilized covert actors, front groups, and propaganda outlets to shift Americans' perception of Chinese policy. As a senior career member of our intelligence community told me just this week, what the Russians are doing pales in comparison to what China is doing across this country. And the American people deserve to know it.

Senior Chinese officials have also tried to influence business leaders to encourage them to condemn our trade actions, leveraging their desire to maintain their operations in China. In one

recent example, China threatened to deny a business license for a major U.S. corporation if they refused to speak out against our administration's policies.

And when it comes to influencing the midterms, you need only look at Beijing's tariffs in response to ours. The tariffs imposed by China to date specifically targeted industries and states that would play an important role in the 2018 election. By one estimate, more than 80 percent of U.S. counties targeted by China voted for President Trump and I in 2016; now China wants to turn these voters against our administration.

And China is also directly appealing to the American voters. Last week, the Chinese government paid to have a multipage supplement inserted into the Des Moines Register –- the paper of record of the home state of our Ambassador to China, and a pivotal state in 2018 and 2020. The supplement, designed to look like the news articles, cast our trade policies as reckless and harmful to Iowans.

Fortunately, Americans aren't buying it. For example, American farmers are standing with this President and are seeing real results from the strong stands that he's taken, including this week's U.S.-Mexico-Canada Agreement, where we've substantially opened North American markets to U.S. products. The USMCA is a great win for American farmers and American manufacturers. (Applause.)

But China's actions aren't focused solely on influencing our policies and politics. Beijing is also taking steps to exploit its economic leverage, and the allure of their large marketplace, to advance its influence over American businesses.

Beijing now requires American joint ventures that operate in China to establish what they call "party organizations" within their company, giving the Communist Party a voice –- and perhaps a veto -– in hiring and investment decisions.

Chinese authorities have also threatened U.S. companies that depict Taiwan as a distinct geographic entity, or that stray from Chinese policy on Tibet. Beijing compelled Delta Airlines to publicly apologize for not calling Taiwan a "province of China" on its website. And it pressured Marriott to fire a U.S. employee who merely liked a tweet about Tibet.

And Beijing routinely demands that Hollywood portray China in a strictly positive light. It punishes studios and producers that don't. Beijing's censors are quick to edit or outlaw movies that criticize China, even in minor ways. For the movie, "World War Z," they had to cut the script's mention of a

virus because it originated in China. The movie, “Red Dawn” was digitally edited to make the villains North Korean, not Chinese.

But beyond business and entertainment, the Chinese Communist Party is also spending billions of dollars on propaganda outlets in the United States and, frankly, around the world.

China Radio International now broadcasts Beijing-friendly programs on over 30 U.S. outlets, many in major American cities. The China Global Television Network reaches more than 75 million Americans, and it gets its marching orders directly from its Communist Party masters. As China’s top leader put it during a visit to the network’s headquarters, and I quote, “The media run by the Party and the government are propaganda fronts and must have the Party as their surname.”

It’s for those reasons and that reality that, last month, the Department of Justice ordered that network to register as a foreign agent.

The Communist Party has also threatened and detained the Chinese family members of American journalists who pry too deep. And it’s blocked the websites of U.S. media organizations and made it harder for our journalists to get visas. This happened after the New York Times published investigative reports about the wealth of some of China’s leaders.

But the media isn’t the only place where the Chinese Communist Party seeks to foster a culture of censorship. The same is true across academia.

I mean, look no further than the Chinese Students and Scholars Association, of which there are more than 150 branches across America’s campuses. These groups help organize social events for some of the more than 430,000 Chinese nationals studying in the United States. They also alert Chinese consulates and embassies when Chinese students, and American schools, stray from the Communist Party line.

At the University of Maryland, a Chinese student recently spoke at her graduation of what she called, and I quote, the “fresh air of free speech” in America. The Communist Party’s official newspaper swiftly chastised her. She became the victim of a firestorm of criticism on China’s tightly-controlled social media, and her family back home was harassed. As for the university itself, its exchange program with China — one of the nation’s most extensive — suddenly turned from a flood to a trickle.

China exerts academic pressure in other ways, as well. Beijing provides generous funding to universities, think tanks, and scholars, with the understanding that they will avoid ideas that the Communist Party finds dangerous or offensive. China experts in particular know that their visas will be delayed or denied if their research contradicts Beijing's talking points.

And even scholars and groups who avoid Chinese funding are targeted by that country, as the Hudson Institute found out firsthand. After you offered to host a speaker Beijing didn't like, your website suffered a major cyberattack, originating from Shanghai. The Hudson Institute knows better than most that the Chinese Communist Party is trying to undermine academic freedom and the freedom of speech in America today.

These and other actions, taken as a whole, constitute an intensifying effort to shift American public opinion and policy away from the "America First" leadership of President Donald Trump.

But our message to China's rulers is this: This President will not back down. (Applause.) The American people will not be swayed. And we will continue to stand strong for our security and our economy, even as we hope for improved relations with Beijing.

Our administration is going to continue to act decisively to protect America's interests, American jobs, and American security.

As we rebuild our military, we will continue to assert American interests across the Indo-Pacific.

As we respond to China's trade practices, we will continue to demand an economic relationship with China that is free, fair, and reciprocal. We will demand that Beijing break down its trade barriers, fulfill its obligations, fully open its economy — just as we have opened ours.

We'll continue to take action against Beijing until the theft of American intellectual property ends once and for all. And we will continue to stand strong until Beijing stops the predatory practice of forced technology transfer. We will protect the private property interests of American enterprise. (Applause.)

And to advance our vision of a free and open Indo-Pacific, we're building new and stronger bonds with nations that share our values across the region, from India to Samoa. Our relationships will flow from a spirit of respect built on partnership, not domination.

We're forging new trade deals on a bilateral basis, just as last week President Trump signed an improved trade deal with South Korea. And we will soon begin historic negotiations for a bilateral free-trade deal with Japan. (Applause.)

I'm also pleased to report that we're streamlining international development and finance programs. We'll be giving foreign nations a just and transparent alternative to China's debt-trap diplomacy. In fact, this week, President Trump will sign the BUILD Act into law.

Next month, it will be my privilege to represent the United States in Singapore and Papua New Guinea, at ASEAN and APEC. There, we will unveil new measures and programs to support a free and open Indo-Pacific. And on behalf of the President, I will deliver the message that America's commitment to the Indo-Pacific has never been stronger. (Applause.)

Closer to home, to protect our interests, we've recently strengthened CFIUS — the Committee on Foreign Investment — heightening our scrutiny of Chinese investment in America to protect our national security from Beijing's predatory actions.

And when it comes to Beijing's malign influence and interference in American politics and policy, we will continue to expose it, no matter the form it takes. We will work with leaders at every level of society to defend our national interests and most cherished ideals. The American people will play the decisive role — and, in fact, they already are.

As we gather here, a new consensus is rising across America. More business leaders are thinking beyond the next quarter, and thinking twice before diving into the Chinese market if it means turning over their intellectual property or abetting Beijing's oppression. But more must follow suit. For example, Google should immediately end development of the "Dragonfly" app that will strengthen Communist Party censorship and compromise the privacy of Chinese customers. (Applause.)

It's also great to see more journalists reporting the truth without fear or favor, digging deep to find where China is interfering in our society, and why. And we hope that American and global news organizations will continue to join this effort on an increasing basis.

More scholars are also speaking out forcefully and defending academic freedom, and more universities and think tanks are mustering the courage to turn away Beijing's easy money,

recognizing that every dollar comes with a corresponding demand. And we're confident that their ranks will grow.

And across the nation, the American people are growing in vigilance, with a newfound appreciation for our administration's actions and the President's leadership to reset America's economic and strategic relationship with China. Americans stand strong behind a President that's putting America first.

And under President Trump's leadership, I can assure you, America will stay the course. China should know that the American people and their elected officials in both parties are resolved.

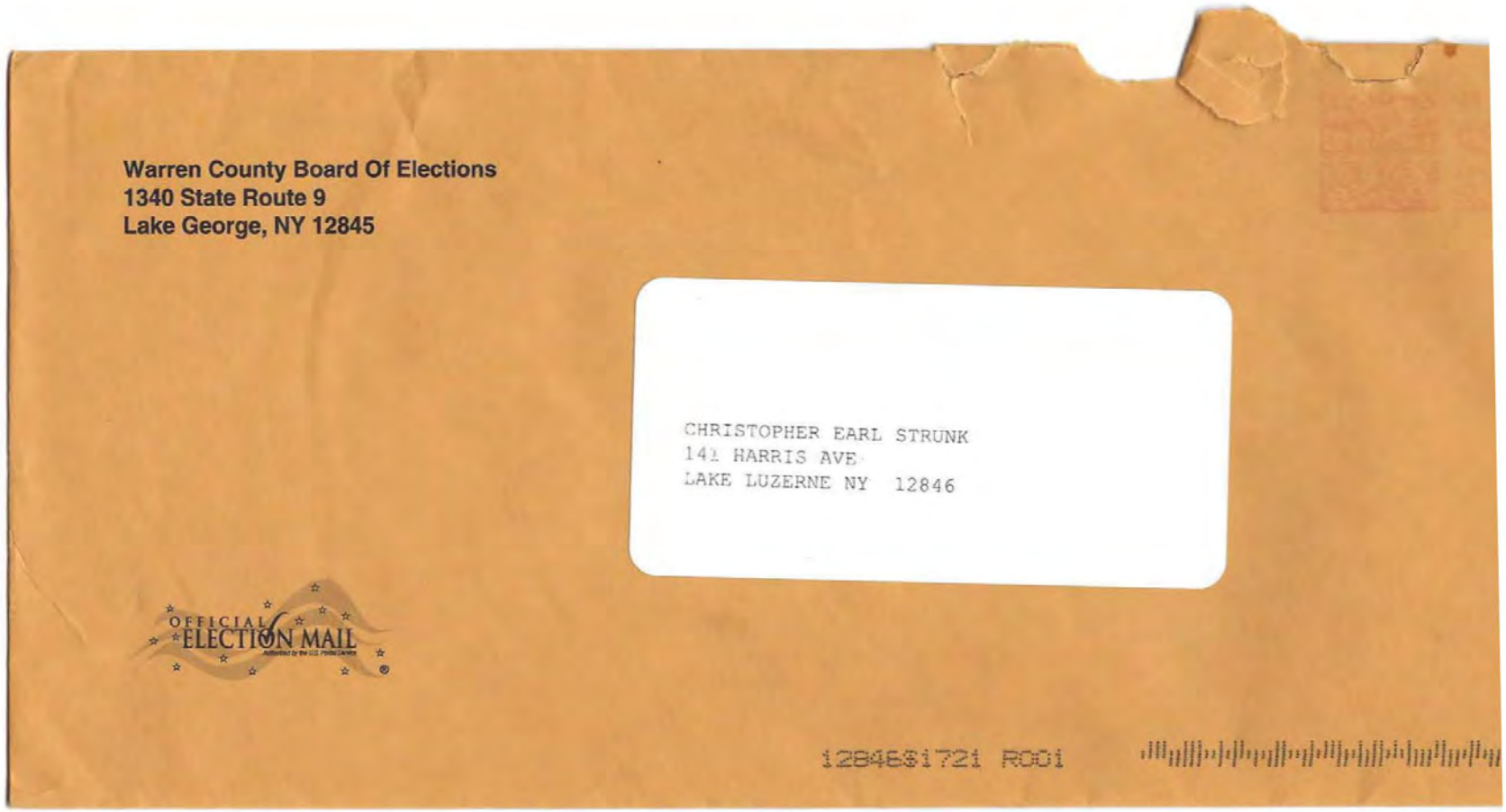
As our National Security Strategy states: We should remember that "Competition does not always mean hostility," nor does it have to. The President has made clear, we want a constructive relationship with Beijing where our prosperity and security grow together, not apart. While Beijing has been moving further away from this vision, China's rulers can still change course and return to the spirit of reform and opening that characterize the beginning of this relationship decades ago. The American people want nothing more; and the Chinese people deserve nothing less.

The great Chinese storyteller Lu Xun often lamented that his country, and he wrote, "has either looked down at foreigners as brutes, or up to them as saints," but never "as equals." Today, America is reaching out our hand to China. And we hope that soon, Beijing will reach back with deeds, not words, and with renewed respect for America. But be assured: we will not relent until our relationship with China is grounded in fairness, reciprocity, and respect for our sovereignty. (Applause.)

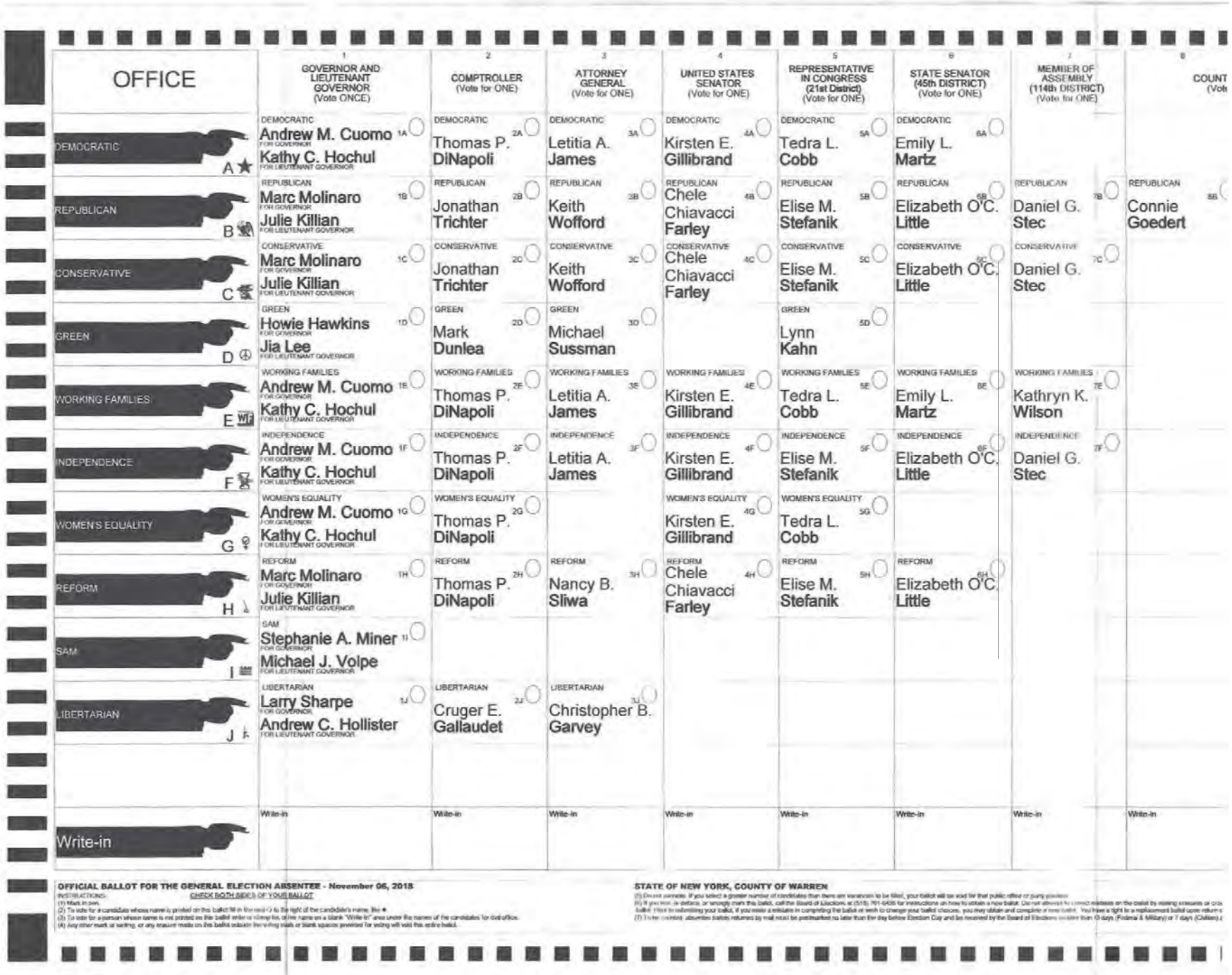
There is an ancient Chinese proverb that reads, "Men see only the present, but heaven sees the future." As we go forward, let us pursue a future of peace and prosperity with resolve and faith. Faith in President Trump's leadership and vision, and the relationship that he has forged with China's president. Faith in the enduring friendship between the American people and the Chinese people. And Faith that heaven sees the future — and by God's grace, America and China will meet that future together.

Thank you. God bless you. And God bless the United States of America. (Applause.)

END


Warren County Board Of Elections
1340 State Route 9
Lake George, NY 12845
CHRISTOPHER EARL STRUNK
141 HARRIS AVE
LAKE LUZERNE NY 12846
OFFICIAL ELECTION MAIL
12846$1721 R001

APX 093



OFFICE	1 GOVERNOR AND LIEUTENANT GOVERNOR (Vote ONCE)	2 COMPTROLLER (Vote for ONE)	3 ATTORNEY GENERAL (Vote for ONE)	4 UNITED STATES SENATOR (Vote for ONE)	5 REPRESENTATIVE IN CONGRESS (21st District) (Vote for ONE)	6 STATE SENATOR (45th DISTRICT) (Vote for ONE)	7 MEMBER OF ASSEMBLY (114th DISTRICT) (Vote for ONE)	8 COUNT (Vote
DEMOCRATIC A ★	DEMOCRATIC 1A Andrew M. Cuomo FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	DEMOCRATIC 2A Thomas P. DiNapoli	DEMOCRATIC 3A Letitia A. James	DEMOCRATIC 4A Kirsten E. Gillibrand	DEMOCRATIC 5A Tedra L. Cobb	DEMOCRATIC 6A Emily L. Martz		
REPUBLICAN B	REPUBLICAN 1B Marc Molinaro FOR GOVERNOR Julie Killian FOR LIEUTENANT GOVERNOR	REPUBLICAN 2B Jonathan Trichter	REPUBLICAN 3B Keith Wofford	REPUBLICAN 4B Chele Chiavacci Farley	REPUBLICAN 5B Elise M. Stefanik	REPUBLICAN 6B Elizabeth O'C. Little	REPUBLICAN 7B Daniel G. Stec	REPUBLICAN 8B Connie Goedert
CONSERVATIVE C	CONSERVATIVE 1C Marc Molinaro FOR GOVERNOR Julie Killian FOR LIEUTENANT GOVERNOR	CONSERVATIVE 2C Jonathan Trichter	CONSERVATIVE 3C Keith Wofford	CONSERVATIVE 4C Chele Chiavacci Farley	CONSERVATIVE 5C Elise M. Stefanik	CONSERVATIVE 6C Elizabeth O'C. Little	CONSERVATIVE 7C Daniel G. Stec	
GREEN D ☮	GREEN 1D Howie Hawkins FOR GOVERNOR Jia Lee FOR LIEUTENANT GOVERNOR	GREEN 2D Mark Dunlea	GREEN 3D Michael Sussman		GREEN 5D Lynn Kahn			
WORKING FAMILIES E WF	WORKING FAMILIES 1E Andrew M. Cuomo FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	WORKING FAMILIES 2E Thomas P. DiNapoli	WORKING FAMILIES 3E Letitia A. James	WORKING FAMILIES 4E Kirsten E. Gillibrand	WORKING FAMILIES 5E Tedra L. Cobb	WORKING FAMILIES 6E Emily L. Martz	WORKING FAMILIES 7E Kathryn K. Wilson	
INDEPENDENCE F	INDEPENDENCE 1F Andrew M. Cuomo FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	INDEPENDENCE 2F Thomas P. DiNapoli	INDEPENDENCE 3F Letitia A. James	INDEPENDENCE 4F Kirsten E. Gillibrand	INDEPENDENCE 5F Elise M. Stefanik	INDEPENDENCE 6F Elizabeth O'C. Little	INDEPENDENCE 7F Daniel G. Stec	
WOMEN'S EQUALITY G ♀	WOMEN'S EQUALITY 1G Andrew M. Cuomo FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	WOMEN'S EQUALITY 2G Thomas P. DiNapoli		WOMEN'S EQUALITY 4G Kirsten E. Gillibrand	WOMEN'S EQUALITY 5G Tedra L. Cobb			
REFORM H	REFORM 1H Marc Molinaro FOR GOVERNOR Julie Killian FOR LIEUTENANT GOVERNOR	REFORM 2H Thomas P. DiNapoli	REFORM 3H Nancy B. Sliwa	REFORM 4H Chele Chiavacci Farley	REFORM 5H Elise M. Stefanik	REFORM 6H Elizabeth O'C. Little		
SAM I	SAM 1I Stephanie A. Miner FOR GOVERNOR Michael J. Volpe FOR LIEUTENANT GOVERNOR							
LIBERTARIAN J	LIBERTARIAN 1J Larry Sharpe FOR GOVERNOR Andrew C. Hollister FOR LIEUTENANT GOVERNOR	LIBERTARIAN 2J Cruger E. Gallaudet	LIBERTARIAN 3J Christopher B. Garvey					
Write-in	Write-in	Write-in	Write-in	Write-in	Write-in	Write-in	Write-in	Write-in

OFFICIAL BALLOT FOR THE GENERAL ELECTION ABSENTEE - November 06, 2018

INSTRUCTIONS: CHECK BOTH SIDES OF YOUR BALLOT

(1) Mark in pen.
(2) To vote for a candidate whose name is printed on this ballot fill in the oval (○) to the right of the candidate's name. Like ●
(3) To vote for a person whose name is not printed on this ballot write a cleargo list of her name on a blank "Write-In" area under the names of the candidates for that office.
(4) Any other mark or writing, or any erasure made on this ballot outside the writing areas or blank spaces provided for voting will void this entire ballot.

STATE OF NEW YORK, COUNTY OF WARREN

(5) Do not overvote. If you select a greater number of candidates than there are vacancies to be filled, your ballot will be void for that public office or party position.
(6) If you tear, deface, or wrongly mark this ballot, call the Board of Elections at (518) 761-6456 for instructions on how to obtain a new ballot. Do not attempt to correct mistakes on the ballot by making erasures or cross
ballot. Prior to submitting your ballot, if you make a mistake in completing the ballot or wish to change your ballot choices, you may obtain and complete a new ballot. You have a right to a replacement ballot upon return
(7) To be counted, absentee ballots returned by mail must be postmarked no later than the day before Election Day and be received by the Board of Elections no later than 0 days (Federal & Military) or 7 days (Civilian)

APX 095

FROM: (Complete Address)

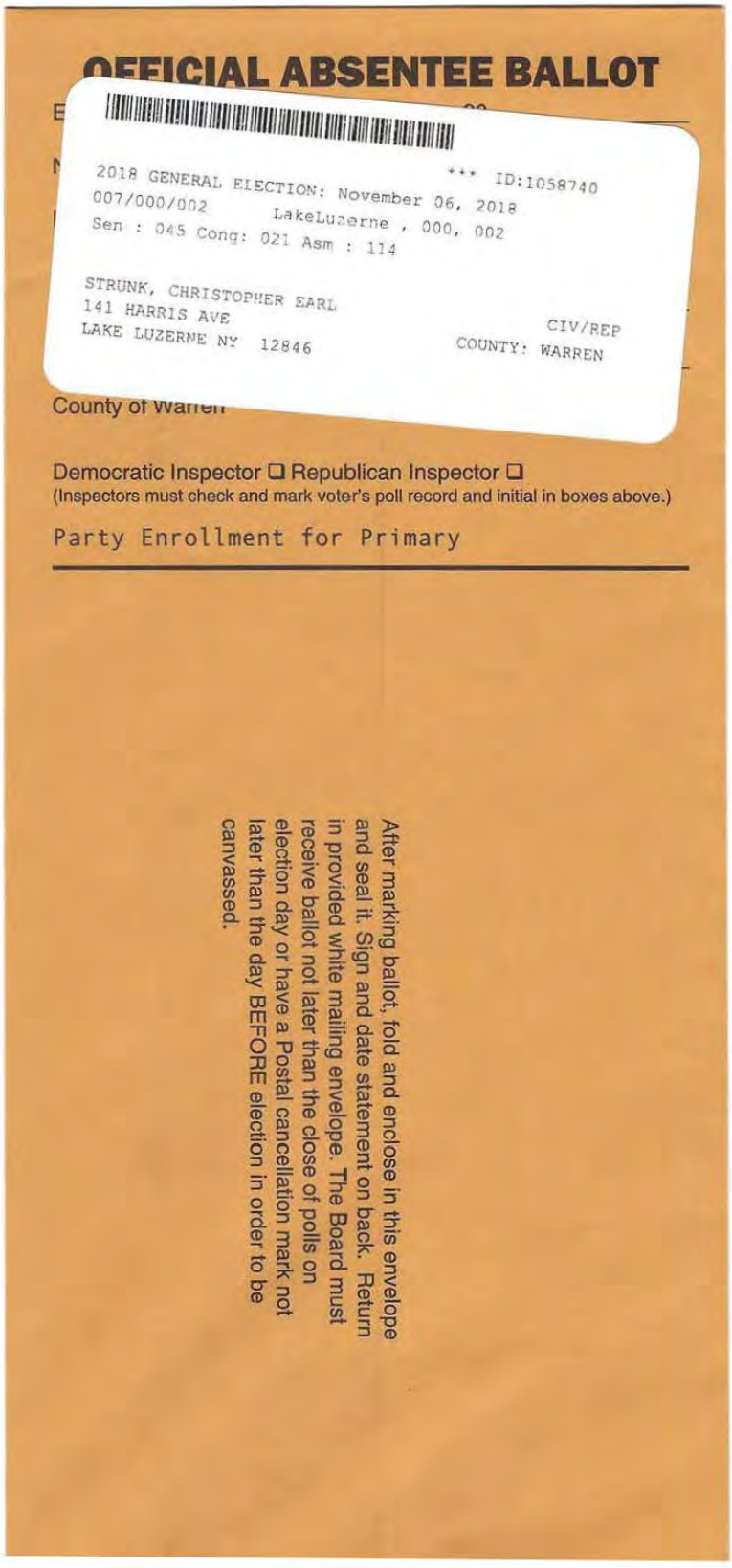
CHRISTOPHER G. STRUNK
141 HARRIS AVENUE
LAKE LUZERNE NY
12846

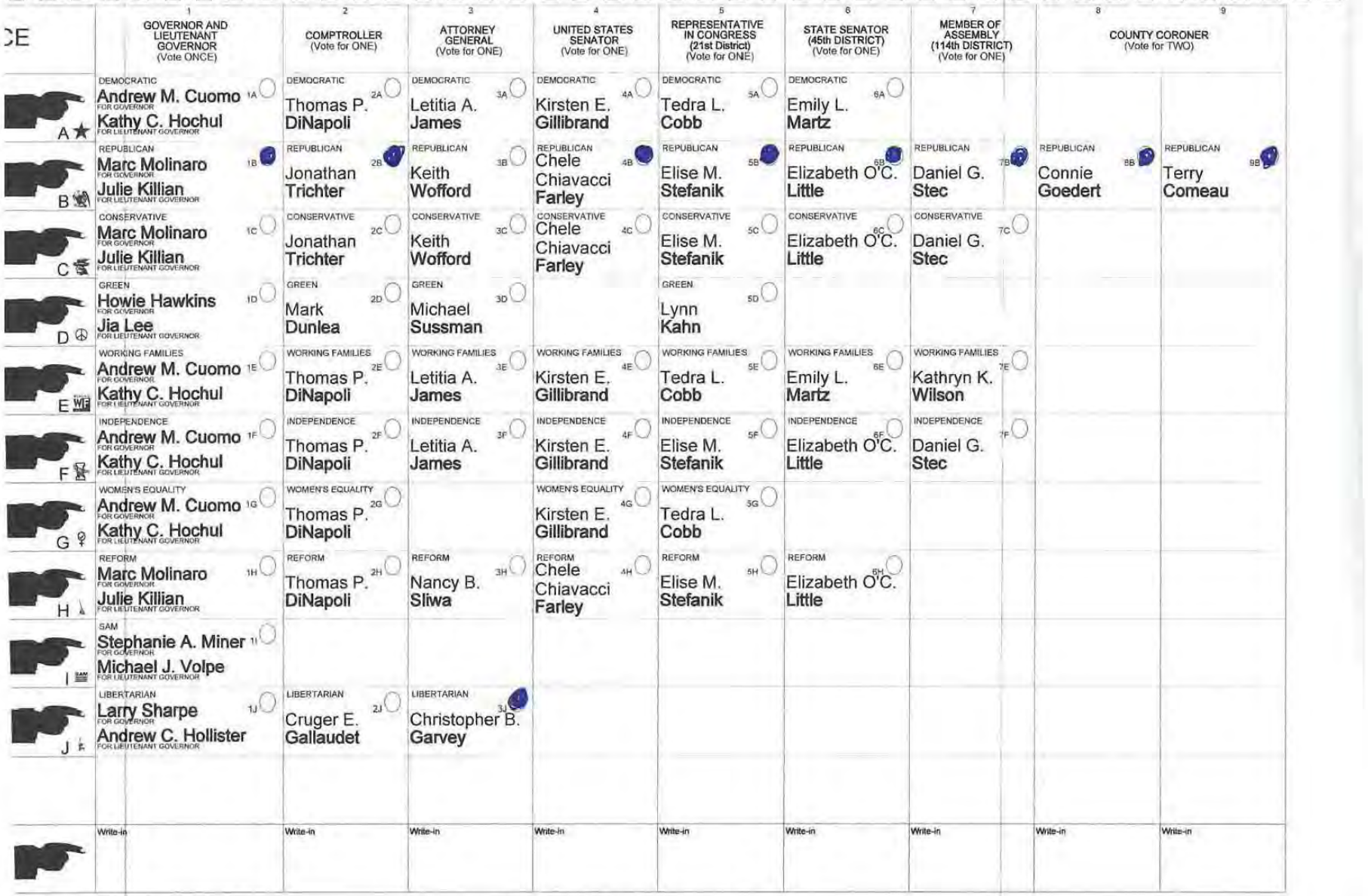
ELECTION MATERIAL – PLEASE EXPEDITE

OFFICIAL ELECTION MAIL
Authorized by the U.S. Postal Service

BOARD OF ELECTIONS
WARREN COUNTY MUNICIPAL CENTER
1340 STATE ROUTE 9
LAKE GEORGE, NY 12845

Fort Orange Press, Inc.
CR#12


OFFICIAL ABSENTEE BALLOT
*** ID:1058740
2018 GENERAL ELECTION: November 06, 2018
007/000/002 LakeLuzerne , 000, 002
Sen : 045 Cong: 021 Asm : 114
STRUNK, CHRISTOPHER EARL
141 HARRIS AVE
LAKE LUZERNE NY 12846
CIV/REP
COUNTY: WARREN
County of Warren
Democratic Inspector ❑ Republican Inspector ❑
(Inspectors must check and mark voter's poll record and initial in boxes above.)
Party Enrollment for Primary
After marking ballot, fold and enclose in this envelope and seal it. Sign and date statement on back. Return in provided white mailing envelope. The Board must receive ballot not later than the close of polls on election day or have a Postal cancellation mark not later than the day BEFORE election in order to be canvassed.



CE	1 GOVERNOR AND LIEUTENANT GOVERNOR (Vote ONCE)	2 COMPTROLLER (Vote for ONE)	3 ATTORNEY GENERAL (Vote for ONE)	4 UNITED STATES SENATOR (Vote for ONE)	5 REPRESENTATIVE IN CONGRESS (21st District) (Vote for ONE)	6 STATE SENATOR (45th DISTRICT) (Vote for ONE)	7 MEMBER OF ASSEMBLY (114th DISTRICT) (Vote for ONE)	8 COUNTY CORONER (Vote for TWO)	9
A ★	DEMOCRATIC Andrew M. Cuomo 1A FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	DEMOCRATIC Thomas P. DiNapoli 2A	DEMOCRATIC Letitia A. James 3A	DEMOCRATIC Kirsten E. Gillibrand 4A	DEMOCRATIC Tedra L. Cobb 5A	DEMOCRATIC Emily L. Martz 6A			
B	REPUBLICAN Marc Molinaro 1B FOR GOVERNOR Julie Killian FOR LIEUTENANT GOVERNOR	REPUBLICAN Jonathan Trichter 2B	REPUBLICAN Keith Wofford 3B	REPUBLICAN Chele Chiavacci Farley 4B	REPUBLICAN Elise M. Stefanik 5B	REPUBLICAN Elizabeth O'C. Little 6B	REPUBLICAN Daniel G. Stec 7B	REPUBLICAN Connie Goedert 8B	REPUBLICAN Terry Comeau 9B
C	CONSERVATIVE Marc Molinaro 1C FOR GOVERNOR Julie Killian FOR LIEUTENANT GOVERNOR	CONSERVATIVE Jonathan Trichter 2C	CONSERVATIVE Keith Wofford 3C	CONSERVATIVE Chele Chiavacci Farley 4C	CONSERVATIVE Elise M. Stefanik 5C	CONSERVATIVE Elizabeth O'C. Little 6C	CONSERVATIVE Daniel G. Stec 7C		
D	GREEN Howie Hawkins 1D FOR GOVERNOR Jia Lee FOR LIEUTENANT GOVERNOR	GREEN Mark Dunlea 2D	GREEN Michael Sussman 3D		GREEN Lynn Kahn 5D				
E WF	WORKING FAMILIES Andrew M. Cuomo 1E FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	WORKING FAMILIES Thomas P. DiNapoli 2E	WORKING FAMILIES Letitia A. James 3E	WORKING FAMILIES Kirsten E. Gillibrand 4E	WORKING FAMILIES Tedra L. Cobb 5E	WORKING FAMILIES Emily L. Martz 6E	WORKING FAMILIES Kathryn K. Wilson 7E		
F	INDEPENDENCE Andrew M. Cuomo 1F FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	INDEPENDENCE Thomas P. DiNapoli 2F	INDEPENDENCE Letitia A. James 3F	INDEPENDENCE Kirsten E. Gillibrand 4F	INDEPENDENCE Elise M. Stefanik 5F	INDEPENDENCE Elizabeth O'C. Little 6F	INDEPENDENCE Daniel G. Stec 7F		
G ♀	WOMEN'S EQUALITY Andrew M. Cuomo 1G FOR GOVERNOR Kathy C. Hochul FOR LIEUTENANT GOVERNOR	WOMEN'S EQUALITY Thomas P. DiNapoli 2G		WOMEN'S EQUALITY Kirsten E. Gillibrand 4G	WOMEN'S EQUALITY Tedra L. Cobb 5G				
H	REFORM Marc Molinaro 1H FOR GOVERNOR Julie Killian FOR LIEUTENANT GOVERNOR	REFORM Thomas P. DiNapoli 2H	REFORM Nancy B. Sliwa 3H	REFORM Chele Chiavacci Farley 4H	REFORM Elise M. Stefanik 5H	REFORM Elizabeth O'C. Little 6H			
I SAM	SAM Stephanie A. Miner 1I FOR GOVERNOR Michael J. Volpe FOR LIEUTENANT GOVERNOR								
J	LIBERTARIAN Larry Sharpe 1J FOR GOVERNOR Andrew C. Hollister FOR LIEUTENANT GOVERNOR	LIBERTARIAN Cruger E. Gallaudet 2J	LIBERTARIAN Christopher B. Garvey 3J						
	Write-in	Write-in	Write-in	Write-in	Write-in	Write-in	Write-in	Write-in	Write-in

GENERAL ELECTION ABSENTEE - November 06, 2018

CHECK BOTH SIDES OF YOUR BALLOT

ed on this ballot fill in the oval ⓘ to the right of the candidate's name, like ●
ded on this ballot write or stamp his or her name on a blank "Write-in" area under the names of the candidates for that office.
ide on this ballot outside the voting ovals or blank spaces provided for voting will void this entire ballot.

STATE OF NEW YORK, COUNTY OF WARREN

(5) Do not overvote. If you select a greater number of candidates than there are vacancies to be filled, your ballot will be void for that public office or party position.
(6) If you tear, or deface, or wrongly mark this ballot, call the Board of Elections at (518) 761-6456 for instructions on how to obtain a new ballot. Do not attempt to correct mistakes on the ballot by making erasures or cross outs. Erasures or cross outs may invalidate all or part of your ballot. Prior to submitting your ballot, if you make a mistake in completing the ballot or wish to change your ballot choices, you may obtain and complete a new ballot. You have a right to a replacement ballot upon return of the original ballot.
(7) To be counted, absentee ballots returned by mail must be postmarked no later than the day before Election Day and be received by the Board of Elections no later than 10 days (Federal & Military) or 7 days (Civilian) after Election Day.

SAMPLE BALLOT

OFFICE	1 GOVERNOR AND LIEUTENANT GOVERNOR (Vote ONCE)	3 COMPTROLLER (Vote for ONE)	4 ATTORNEY GENERAL (Vote for ONE)	5 UNITED STATES SENATOR (Vote for ONE)	6 STATE SUPREME COURT JUSTICE 3rd Judicial District (Vote for any TWO)	7	8 REPRESENTATIVE IN CONGRESS 19th District (Vote for ONE)	9 STATE SENATOR 46th District (Vote for ONE)	10 MEMBER OF ASSEMBLY 103rd District (Vote for ONE)	11 COUNTY SHERIFF (Vote for ONE)
DEMOCRATIC A ★	DEMOCRATIC Andrew M. **Cuomo** 1A / FOR GOVERNOR Kathy C. **Hochul** FOR LIEUTENANT GOVERNOR	DEMOCRATIC Thomas P. **DiNapoli** 3A	DEMOCRATIC Letitia A. **James** 4A	DEMOCRATIC Kirsten E. **Gillibrand** 5A	DEMOCRATIC Margaret T. **Walsh** 6A	DEMOCRATIC Peter A. **Lynch** 7A	DEMOCRATIC Antonio **Delgado** 8A	DEMOCRATIC Pat Courtney **Strong** 9A	DEMOCRATIC Kevin **Cahill** 10A	DEMOCRATIC Juan **Figueroa** 11A
REPUBLICAN B	REPUBLICAN Marc **Molinaro** 1B / FOR GOVERNOR Julie **Killian** FOR LIEUTENANT GOVERNOR	REPUBLICAN Jonathan **Trichter** 3B	REPUBLICAN Keith **Wofford** 4B	REPUBLICAN Chele Chiavacci **Farley** 5B		REPUBLICAN William E. **McCarthy** 7B	REPUBLICAN John J. **Faso** 8B	REPUBLICAN George A. **Amedore, Jr.** 9B		REPUBLICAN Paul J. **VanBlarcum** 11B
CONSERVATIVE C	CONSERVATIVE Marc **Molinaro** 1C / FOR GOVERNOR Julie **Killian** FOR LIEUTENANT GOVERNOR	CONSERVATIVE Jonathan **Trichter** 3C	CONSERVATIVE Keith **Wofford** 4C	CONSERVATIVE Chele Chiavacci **Farley** 5C		CONSERVATIVE William E. **McCarthy** 7C	CONSERVATIVE John J. **Faso** 8C	CONSERVATIVE George A. **Amedore, Jr.** 9C		CONSERVATIVE Paul J. **VanBlarcum** 11C
GREEN D	GREEN Howie **Hawkins** 1D / FOR GOVERNOR Jia **Lee** FOR LIEUTENANT GOVERNOR	GREEN Mark **Dunlea** 3D	GREEN Michael **Sussman** 4D				GREEN Steven **Greenfield** 8D			
WORKING FAMILIES E	WORKING FAMILIES Andrew M. **Cuomo** 1E / FOR GOVERNOR Kathy C. **Hochul** FOR LIEUTENANT GOVERNOR	WORKING FAMILIES Thomas P. **DiNapoli** 3E	WORKING FAMILIES Letitia A. **James** 4E	WORKING FAMILIES Kirsten E. **Gillibrand** 5E	WORKING FAMILIES Margaret T. **Walsh** 6E	WORKING FAMILIES Peter A. **Lynch** 7E	WORKING FAMILIES Antonio **Delgado** 8E	WORKING FAMILIES Pat Courtney **Strong** 9E	WORKING FAMILIES Kevin **Cahill** 10E	WORKING FAMILIES Juan **Figueroa** 11E
INDEPENDENCE F	INDEPENDENCE Andrew M. **Cuomo** 1F / FOR GOVERNOR Kathy C. **Hochul** FOR LIEUTENANT GOVERNOR	INDEPENDENCE Thomas P. **DiNapoli** 3F	INDEPENDENCE Letitia A. **James** 4F	INDEPENDENCE Kirsten E. **Gillibrand** 5F	INDEPENDENCE Margaret T. **Walsh** 6F	INDEPENDENCE William E. **McCarthy** 7F	INDEPENDENCE John J. **Faso** 8F	INDEPENDENCE George A. **Amedore, Jr.** 9F		INDEPENDENCE Paul J. **VanBlarcum** 11F
WOMEN'S EQUALITY G ▶	WOMEN'S EQUALITY Andrew M. **Cuomo** 1G / FOR GOVERNOR Kathy C. **Hochul** FOR LIEUTENANT GOVERNOR	WOMEN'S EQUALITY Thomas P. **DiNapoli** 3G		WOMEN'S EQUALITY Kirsten E. **Gillibrand** 5G			WOMEN'S EQUALITY Antonio **Delgado** 8G	WOMEN'S EQUALITY Pat Courtney **Strong** 9G		WOMEN'S EQUALITY Juan **Figueroa** 11G
REFORM H	REFORM Marc **Molinaro** 1H / FOR GOVERNOR Julie **Killian** FOR LIEUTENANT GOVERNOR	REFORM Thomas P. **DiNapoli** 3H	REFORM Nancy B. **Sliwa** 4H	REFORM Chele Chiavacci **Farley** 5H			REFORM John J. **Faso** 8H	REFORM George A. **Amedore, Jr.** 9H		REFORM Paul J. **VanBlarcum** 11H
SAM I	SAM Stephanie A. **Miner** 1I / FOR GOVERNOR Michael J. **Volpe** FOR LIEUTENANT GOVERNOR						FRIENDS OF DIANE NEAL Diane **Neal** 8I			
LIBERTARIAN J	LIBERTARIAN Larry **Sharpe** 1J / FOR GOVERNOR Andrew C. **Hollister** FOR LIEUTENANT GOVERNOR	LIBERTARIAN Cruger E. **Gallaudet** 3J	LIBERTARIAN Christopher B. **Garvey** 4J							
WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN	WRITE-IN

APX 098

ULSTER COUNTY
General Election
November 6, 2018

SHEET# 1

63 Election Districts
County of Ulster
19th Congressional District
46th Senatorial District
103rd Assembly District
City of: Kingston
Ward 1
E.D.(s): 1 - 3
Ward 2
E.D.(s): 1 - 3
Ward 3
E.D.(s): 1 - 3
Ward 4
E.D.(s): 1,2
Ward 5
E.D.(s): 1 - 3
Ward 6
E.D.(s): 1 - 3
Ward 7
E.D.(s): 1 - 3
Ward 8
E.D.(s): 1 - 3
Ward 9
E.D.(s): 1 - 3
Town of: Esopus
E.D.(s): 1 - 7
Town of: Hurley
E.D.(s): 1 - 8
Town of: Kingston
E.D.(s): 1
Town of: Marbletown
E.D.(s): 1 - 7
Town of: Ulster
E.D.(s): 1 - 14

INSTRUCTIONS:

(1) Mark only with a writing instrument provided by the Board of Elections.

(2) To vote for a candidate whose name is printed on this ballot fill in the oval to the right of the candidate, like: ●

(3) To vote for a person whose name is not printed on this ballot write or stamp his or her name in the designated Write-In area for that office.

(4) Any other mark or writing, or any erasure made on this ballot outside the voting ovals or blank spaces provided for voting will void this entire ballot.

(5) Do not overvote. If you select a greater number of candidates than there are vacancies to be filled, your ballot will be void for that public office or proposition.

(6) If you tear, or deface, or wrongly mark this ballot, return it and obtain another. Do not attempt to correct mistakes on the ballot by making erasures or cross outs. Erasures or cross outs may invalidate all or part of your ballot. Prior to submitting your ballot, if you make a mistake in completing the ballot or wish to change your ballot choices, you may obtain and complete a new ballot. You have a right to a replacement ballot upon return of the original ballot.

(7) Review both sides of the ballot.

(8) After completing the ballot, insert it into the ballot scanner and wait for the notice that your ballot has been successfully scanned. If no such notice appears, seek the assistance of an election inspector .

NOTE: Do not let anyone take your ballot to the scanner.

PROPOSAL NUMBER ONE, AN AMENDMENT

Allowing for the Revision of the Ulster County Charter § C-10 Commission on Reapportionment (Redistricting)

"Shall Section C-10 of the Ulster County Charter be amended to provide for the creation of an independent Redistricting Commission, designed to exclude political influence in revising county legislative districts, as proposed and unanimously approved by the Ulster County Charter Revision Committee?"

YES ○ NO ○

APX 099

WebCivil Supreme - Case Search Results

Report created on: October 24, 2018 at 01:32 PM

5 Case(s) Match Your Search. **Page 1 of 1 pages**

	Court	Index Number	Case Status	Plaintiff	Plaintiff Firm	Defendant	Defendant Firm	Appearance Date	Justice	
1	Albany Supreme Court	5888-02.	Disposed	Van Allen	H. William Van Allen	Democratic State Comm	Patricia L Murray	08/25/2003	THOMAS J. MCNAMARA	
2	Albany Supreme Court	3044-04	Disposed	Van Allen	Young Sommer	City Of Albany Zoning	Corporation Counsel	07/19/2004	LOUIS C. BENZA	
3	Albany Supreme Court	1433-12	Disposed	Van Allen	H. William Van Allen, SRL	Silver	Eric T. Schneiderman	07/26/2012	ROGER D. MCDONOUGH	M
4	Albany Supreme Court	1787-12	Disposed	Van Allen	H. William Van Allen SRL	NYS Board Of Elections	NYS Board Of Elections	08/20/2012	RICHARD M. PLATKIN	M
5	Albany Supreme Court	6418-13	Disposed	Van Allen	H. William Van Allen, SRL	NYS Secretary Of State, et al	NYS Attorney General	08/25/2016	KIMBERLY A. O'CONNOR	

[redacted]

[redacted]

Donald J. Trump
President & Chief Executive
The White House
1600 Pennsylvania Avenue NW
Washington, D.C. 20500
202-456-1414

Dear Mr. President:

Request & Win-Win Tax Reform Strategy

My fellow Leader Technologies, Inc. shareholders (Columbus, Ohio) and I ask for your help in getting paid for a great benefit that we provided to the U.S. government for which we have not been paid. I sent you my registered Miller Act Notice previously.

This unprecedented situation creates an equally unprecedented revenue opportunity for the U.S. government for which there does not appear to be a downside. Allow me to explain.

The federal government confiscated Leader's social networking invention from the very moment we met our patent attorney James P. Chandler, III in 2000. *See* Miller Act Notice, pp. 6, 15. Even though Chandler was Leader's attorney, he did not arrange for the government to license Leader's invention. Instead, the federal government silently stole Leader's invention for its use as well as for the benefit of its military-industrial complex partners.

These collaborators then created the "social networking" market out of whole cloth using Leader's invention as its foundation. This effort has been heavily financed by C.I.A. In-Q-Tel and IBM. The social networking market that emerged is valued today at over $4 trillion with 7.7 billion users.[1]

A Win-Win Tax Reform Strategy

The truth is that, Mr. President, both the federal government and the technology world have become accustomed to enjoying the benefits of social networking without paying for it. Remarkably, this historical injustice to Leader Technologies creates a *tremendous tax reform opportunity.*

[1] Social apps users now use 30 apps per month. See Sarah Perez. (May 4, 2017). Report: Smartphone owners are using 9 apps per day, 30 per month. *TechCrunch.* https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month/. However, for the purposes of this discussion we will use a 30:1 ratio and use 7.7 billion users and not 7.7x30=231 billion users.

The government has never tapped into the revenue stream potential that social networking represents.

The technology world has generated literally trillions of dollars in value from social networking, and yet has never paid a dime in fees to Leader Technologies for using their inventions.

I propose a win-win solution that generates substantial new revenues for the federal government and properly compensates Leader for the tremendous value we have provided:

1. **Forward-looking Consumer Use Fee @ $N/user/month:**

   We propose that the federal government surcharge each social networking provider ("Provider") a "Consumer Use Fee" of $N/user/month for each user worldwide. This fee shall be paid to the collecting federal agency each month by the Provider. The payment shall be comprised of:

   50% from the Provider

   50% from the Technology suppliers to Provider *pro rata* (e.g., hardware, software, firmware)

   So for example, a $2.50/month surcharge will generate $231 billion per year in revenue for the federal government.

   The surcharge shall be collected from the Providers. A precedent collection model is the Universal Service Fund (USF) (fee) collected by the Federal Communications Commission (FCC) to subsidize phone rates for rural phone companies, rural healthcare, libraries and schools. The 50% paid by the Technology suppliers shall be determined by the Provider.

2. **Forward-looking Leader Innovation Surcharge @ $2.00/user/month:**

   In addition, for the privilege of using Leader's innovations, each Provider shall collect and pay a $2/month blanket license surcharge from each user for all social apps used by that person on all devices. This annual fee of $185 billion per year will be paid to Leader for the use of its patented inventions ("Leader Innovation Surcharge").

3. **One-time Historical Fee Payment to Leader**

   Leader is prepared to accept a $40 billion one-time payment as a compromise for the historical damages, even though this is a fraction of the value.

As a supporter of the effort to reform the U.S. tax laws, I support the following statement by former President Ronald Reagan:

> "If you want more of something, subsidize it; if you want less of something, tax it."

Our current reliance on income (both personal and corporate) as a basis for taxation has led to a stagnant economy with small growth and stagnant wage rates.

I believe President Donald Trump is correct in saying that lowering the corporate tax rate to 15% and lowering personal income tax rates will unleash the U.S. economy and provide for growth of wages and Gross Domestic Product.

Unfortunately, the current prospects for passage of Tax Reform are hampered by those in Congress who are concerned that the lowering the tax rates on income will result in lowering of tax revenues and increases in the deficit and National Debt.

Lowering tax rates **increases** tax revenues in the long-run; this is the essential concept of Reaganomics.

What I propose here is a win-win strategy and could become a key part in the effort to implement Tax Reform.

You can authorize these payments pursuant to our Miller Act Notice. Leader would finally be able to enjoy a return on its investment of "social networking." It would allow Congress to impose a Consumer Use Fee *tagged to social networking instead of income.*

As everyone in public policy knows, no one likes additional taxes, and Congress will be criticized for imposing a new income tax on its own in the current Tax Reform dialogue. However, this proposal is factors better, I believe. It corrects the injustices visited upon inventor Leader Technologies while also allowing Congress to tap into a new source of revenue at the same time.

Additionally, paying Leader what Leader is due will make Leader as big as Apple. It would enable Leader to become a major job creator and perhaps the number one up and coming employer in Ohio.

This idea is a win-win-win proposition.

I would like to meet with you to discuss how you can assist us to receive the Miller Act Notice payments.

Sincerely,

Yours sincerely,

/S/ [redacted]

[redacted]

Reference:

- Miller Act Notice for Federal Works Projects 40 USC §3131 ET SEQ filed by Tier II Investor Share Class Members of Leader Technologies, Inc. including [redacted]

MILLER ACT NOTICE
FOR FEDERAL WORKS PROJECTS
40 USC §3131 ET SEQ.

July 23, 2017 ("Effective Date")

ORIGINAL CONTRACTOR:	**THE CLAIMANT:**
The United States Chief Executive Donald J. Trump, and his predecessors William J. Clinton, George W. Bush and Barack H. Obama (the "Executive") The White House 1600 Pennsylvania Avenue NW Washington, D.C. 20500	Leader Technologies, Inc. Michael T. McKibben, Founder, Chairman and Inventor (the "Claimant") P.O. Box 224 Lewis Center OH 43035 (614) 890-1986 office (614) 864-7922 fax
THE SURETY:	**HIRING PARTY:**
Surety bonds are presumed to have been provided to the Executive by the various public-private supplier-beneficiaries of Claimant's properties (the "Surety")	James P. Chandler, III, National Security Advisor, Chief Contractor Agent for the Executive, National Infrastructure Assurance/Advisory Councils (NIAC), THE CHANDLER LAW FIRM, PLLC (the "Hiring Party") 1776 K Street, NW Washington, DC 20006 Bar ID: #270686

AMOUNT AND ACCOUNTING OF CLAIM:

1. TOTAL VALUE OF ALL SERVICES PROVIDED:[1]

Historical Claim:

$40 billion (this is a substantial compromise from President Trump's recent estimated value in excess $3.5 trillion from just 22 organizations, all of whom use and benefit from Claimant's property.)[2]

Forward-Looking After-Tax Fee Claim:

Government to collect $184 billion per year Fee (*pre-tax*) from bond holders on 7.7 billion people @ $2/month who use Claimant's property as users of mobile, user-generated social, schools, federal, state and local employees. Claimant to receive *after-tax* balance of the Fee during the life of the intellectual properties, including derivative works. *Source: U.S. Census Bureau*.

[1] Notices: Any errors and omissions are inadvertent. Claimant reserves the right to amend this Notice and the Claim(s). No claims are made to third party rights. All footnotes and endnotes are incorporated as if fully written herein.

[2] *Source*: President Trump's Opening Remarks, American Technology Roundtable, WH, Jun. 19, 2017 ("We have approximately $3.5 trillion dollars of market value in this room.") *See* WH, Jun. 19, 2017 Attendees, Endnote [i].

2. PAYMENTS, CREDITS AND OFFSETS:

$ 0.00

3. BALANCE UNPAID, AND AMOUNT OF CLAIM:

- $40 billion (one-time) (as of Effective Date) (Compromise proposed. Does not reflect the full historical value of Claimant's property used.)[3]
- Net *After-Tax* Fee on $184 billion per year, collected by the government from bond holders for annual forward-looking license Fee for use of Claimant's property for the full life of the properties, incl. derivative works.

4. DATE SERVICE LAST FURNISHED:

Benefits accrue continuously to Original Contractor and bond holders.

5. THE PROPERTY AND/OR PROJECT SUBJECT TO THE CLAIM:

Claimant's property is "social networking" and related software intellectual property operating continuously on computers and servers in literally billions of locations in the United States and offshore.

America's Founders knew that a vibrant economy must protect and incentivize real inventors and writers to grow. The U.S. Constitution Article I, Section 8, Clause 8 ("[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.") protects patents and copyrights and is the only property right actually written in the Constitution.

The Founders also forbade the government in Article I, Section 9, Clause 3 from issuing a contract, then quashing it later under the color of law. These fundamental principles of property protection have been reaffirmed numerous times.

For example, James Madison said in Federalist No. 44: "Patent rights receive protection pursuant to public contracts between inventors and the federal government, acting on behalf of the people."

[3] Claimant reserves the right to reassert up to the full value of Claimant's property used without compensation.

Chief Justice John Marshall affirmed in *Fletcher v. Peck.* 10 US 87 (1810) that the government cannot rescind a contract once awarded. Subsequent Patent Office manuals reinforced this fundamental Constitutional principle: "A Patent is a Contract." *Manual of Patent Law* (1874), *A Summary of the Law of Patents* (1883).

Claimant has multiple patent contracts with the federal government that the government is using without compensating Claimant.

Claimant and his investors sought out a highly-regarded Washington, D.C. patent legal counsel in law professor James P. Chandler, III ("Chandler").[4] Claimant relied on his legal advice after sharing Claimant's innovations with him and the government. Claimant paid substantial fees to obtain patents that were eventually awarded by the government.

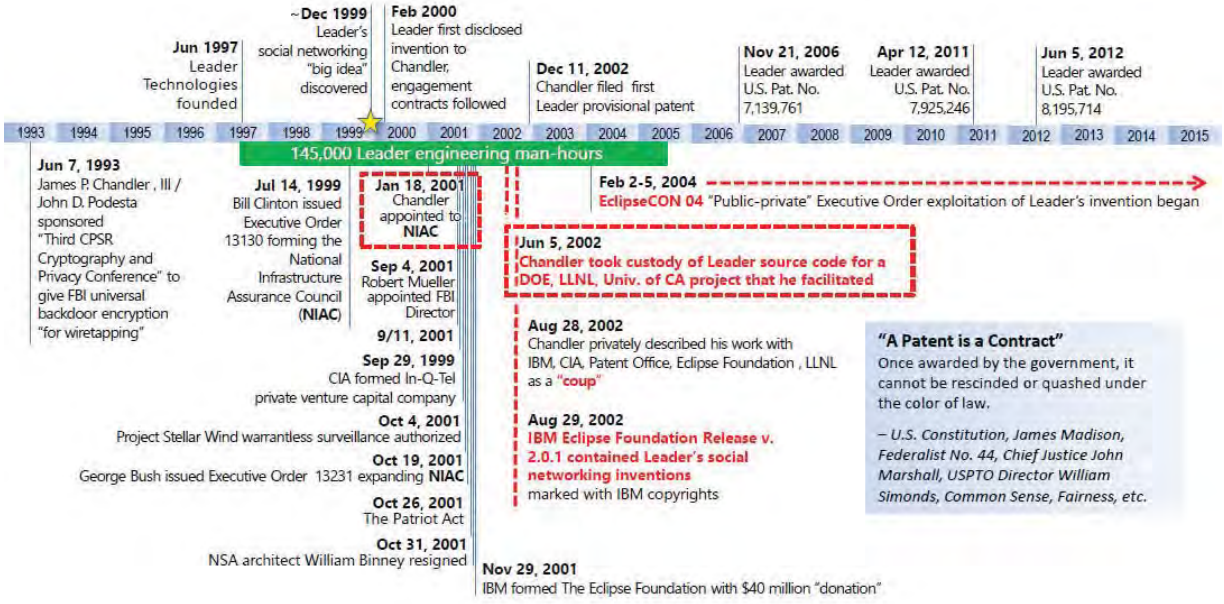


Figure 1: Timeline of events related to this Leader Technologies, Inc. claim.

However, Chandler turned over Claimant's property to a group of "public-private" collaborators with whom he was associated, without any notice or compensation to Claimant.

In February 2000, the Hiring Party, James P. Chandler, III entered into contracts with Claimant to provide legal, director and other services[5] that resulted in, among other things, the registering of

[4] Professor James P. Chandler biography, http://www.nipli.org/1/1-3-2.html.
[5] James P. Chandler, The Chandler Law Firm Chartered, Leader Technologies Director Services and Engagement Letters, Apr. 6, 2000, May 5, 2000, Mar. 01, 2001, May 25, 2001; Chandler signed a Leader Directors Services

trademarks, copyrights and the award of U.S. Patent Numbers 7,139,761,[6] 7,925,246[7] and 8,195,714.[8] Chandler was also then a senior national security advisor to the White House, Congress, Judiciary and intelligence community (e.g., FBI, NSA, CIA, DoD, DOJ, DoE, NRO, DHS, IBM), among others.

Chandler is well known or strongly believed to have collaborated with numerous members of the political, legal and intelligence communities in this work, including, but not limited to Former FBI directors Louis Freeh,[9] Robert S. Mueller, James B. Comey; Rod J. Rosenstein; Andrew D. Goldstein; Preetinder Bharara; Eric H. Holder, Jr.;[10] Loretta E. Lynch; Williams & Connolly LLP;[11] Gibson Dunn LLP,[12] Fenwick & West LLP; Weil Gotshal LLP;[13] Skadden Arps, LLP; Cooley Godward LLP; White & Case LLP; Orrick Herrington LLP; Blank Rome LLP, Perkins Coie LLP, Latham & Watkins LLP; Cravath Swaine LLP,[14] Mayer Brown LLP; Hillary & Bill Clinton; John D. Podesta;[15] Directors of the CIA, NSA. DNI and National Security Advisors since 1993 through the Obama Administration; the Federal Circuit Court of Appeals;[16] Federal Circuit Bar Association,[17] American Bar Association,[18] FISC ("The FISA Court"); In-Q-Tel principals,

---

Agreement on May 5, 2000 in which he specifically committed to the Business Judgment Rule duties of diligence, loyalty, obedience, accountability, disinterestedness, due care, good faith, abuse of discretion, e.g., "prohibited from using their position of trust and confidence to further their private interests" and "may not engage in undisclosed personal transactions of a material nature." Sec. 1(2), 1(2)(d).

[6] U.S. Pat. No. 7,139,761, Dynamic Association of Electronically Stored Information with Iterative Workflow Changes, McKibben et al, awarded by Jon W Dudas, Director, USPTO, Nov. 21, 2006.

[7] U.S. Pat. No. 7,925,246, Context Instantiated Application Protocol, McKibben et al, awarded by David J. Kappos, Director, USPTO, Jun. 5, 2012,

[8] U.S. Pat. No. 8,195,714, Radio/Telephony Interoperability System, McKibben et al, signed by David J. Kappos, Director, USPTO, Apr. 12, 2001.

[9] S. Hrg. 104-499 (Feb. 28, 1998). Economic Espionage Act Hearing, testimony of FBI Director Louis Freeh acknowledging James P. Chandler. U.S. Senate.

[10] Chandler, J. P. (Mar. 28, 2001). Trade Secrets and Enforcement of Intellectual Property Rights Conference. NIPLI (highlighted then Assistant Attorney General Eric H. Holder who was collaborating with Chandler on trade secrets and economic espionage cases, along with Robert S. Mueller, James B. Comey and Rod J. Rosenstein, among others).

[11] *United States v. James Hsu*, 155 F.3d 189 (1998) (James P. Chandler, III, for the Justice Department, and Paul Mogin, Williams & Connolly LLP, concluded the first prosecution of the Economic Espionage Act of 1996 ("EEA") drafted by Chandler for President Bill Clinton).

[12] Petition for Writ of Certiorari (Nov. 16, 2012), *Leader Technologies, Inc., v. Facebook, Inc.,* No. 12-617 (U.S. Supreme Court 2012) (Gibson Dunn LLP, White & Case LLP, Blank Rome LLP and Cooley Godward LLP represented Facebook and had personal relationships with Chief Justice John G. Roberts, Jr. who hold substantial Facebook financial interests, as do all of the lower court judges in this case).

[13] Graham, S. (May 23, 2014). Rader Steps Down as Chief, Apologies for Reines Email. *The Recorder*.

[14] Former Patent Office Director David J. Kappos's current law firm.

[15] James P. Chandler, John D. Podesta. (Jun. 07, 1993). Third CPSR Cryptography and Privacy Conference. Carnegie Endowment for International Peace ("to require [for the FBI] that telecommunications manufacturers and service providers redesign their systems to facilitate wiretapping.").

[16] Chandler bio, fn. 4.

[17] *Id*.

[18] *Id*.

their banker/underwriters and funded companies; National Venture Capital Association (NVCA); the Judicial Conference;[19] the national laboratories; and The Clinton Foundation.

At a minimum, the above-mentioned individuals, organizations and their principals should be excused from involvement in any investigations and decision making about Claimant's claim and compensation because of the appearance of impropriety. Further citations will be supplied upon request.

Chandler received detailed proprietary information about Claimant's invention properties for which he initially estimated that there were "over 60 patentable inventions." The industry now calls Claimant's inventions "social networking."

Chandler failed to disclose to Claimant his conflicts of interest and his material involvement with a "shadow government"[20] to which he was/is a key consultant.

Figure 2: On Jun. 8, 2000, James P. Chandler, III, and his legal assistant Kelley E. Clements (L/R, right rear, seated), participated, along with co-inventors Jeffrey Lamb and Michael McKibben (L/R, left rear, standing), in Leader invention design sessions in Columbus, Ohio where he learned the essences of Leader's social networking invention. *Photo: Leader Technologies, Inc.*Figure 1: On Jun. 8, 2000, James P. Chandler, III, and his legal assistant Kelley E. Clements (L/R, right rear, seated), participated, along with co-inventors Jeffrey Lamb and Michael McKibben (L/R, left rear, standing), in Leader invention design sessions in Columbus, Ohio where he learned the essences of Leader's social networking invention. *Photo: Leader Technologies, Inc.*

In 2002, under the color of attorney-client privilege and national security, Chandler obtained a custody copy of Claimant's invention engineering source code on Jun. 05, 2002.[21] Eleven (11)

[19] Report of the Secretary (Mar. 14, 2001). Report of the Proceedings of the Judicial Conference of the United States. Judicial Conference (Organizer of change to mutual fund reporting rules for federal judges and judicial employees: Jan Horbaly, Fed. Cir. Executive).
[20] National Press Office. (Sep. 2, 2016). https://vault.fbi.gov/hillary-r.clinton, Part 04 of 11, p. 56, ¶1. FBI.

weeks later, on Aug. 29, 2002, he distributed Claimant's invention to his "public-private" collaborators[22] via Version 2.0.1[23] of the IBM Eclipse Foundation source code, his client ("Eclipse"). This new Eclipse source code release contained no mention of Claimant and was marked only with IBM copyright notices.

Notably, just one day earlier, on Aug. 28, 2002, Chandler had met with Montgomery County, Maryland development officials on behalf of himself, IBM, the Patent Office and classified intelligence agencies (he specifically mentioned the CIA)[24] about acquiring a 30,000 sf. facility for their plans that his notes described as a "coup." David J. Kappos was then chief inside intellectual property counsel at IBM and an advisor to Chandler. (In 2009, Kappos was appointed director of the Patent Office by President Barack Obama.) Claimant had no knowledge of this attorney-client and directorial misconduct.

The IBM Eclipse Foundation was formed on Nov. 29, 2001 with a $40 million "donation" from IBM.[25] Through Eclipse's members, Claimant's property was distributed to and adopted widely by the bond holders under the moniker of "The Internet of Things."[26]

The Original Contractor's use of Claimant's property is ongoing and global in scope. The Hiring Party facilitated use of Claimant's property throughout a multitude of government agencies and private organizations, including but not limited to:

1. Suppliers to Executive Orders 13130 (July 14, 1999) National Infrastructure Assurance Council (NIAC), 13231 (October 16, 2001) National Infrastructure Advisor Council (NIAC) and their progeny, up to and including Executive Order 13708 (September 30, 2015) which expires on September 30, 2017 (unless renewed by the Executive), among others. **These orders give the Executive full authority to satisfy this claim.** The Hiring

---

[21] James P. Chandler. (Jun. 5, 2002). LLNL-CRADA. CRADA No. TC-2030-01. The Regents of the University of California (Lawrence Livermore National Laboratory) under its U.S. Department of Energy Contract No. W-7405-ENG-48 and Leader Technologies, LLC for RAPIDLY DEPLOYABLE SECURITY SYSTEM, signed by Jeffrey Wadsworth for Director C. Burce Tartar. The Chandler Law Firm Chartered, PDF p. 36, Sec. 5, ¶5.

[22] Executive Order 13130, Sec. 2(1); Executive Order 13231, Secs. 1(b), 10(c).

[23] Version 2.0.1 (Aug. 29, 2002). Source code release including Leader Technologies' inventions marked with IBM copyrights. IBM Eclipse Foundation.

[24] Kelley E. Clements. (Aug. 30, 2002). Chandler Executive Assistant Clements' stenographer's minutes from meetings and events surrounding meeting among James P. Chandler and Montgomery County, Maryland development officers Dave Edgerley (Director), Janis Peters and May Webster (with the knowledge of Doug Duncan, County Executive) to negotiate use of $500-1,000,000 in federal budget support for a 40,000 sf. office space facility to be used by his organization NIPLI (National Intellectual Property Law Institute), the U.S. Patent Office archives, classified material (mentions CIA) and IBM, says no involvement of Congress and even used the phrase "(kind of a 'coup' of sorts)."

[25] Eclipse.org Consortium. (Nov. 29, 2001). Eclipse.org Consortium Forms to Deliver New Era Application Development Tools [Press release]; *See* also The Eclipse Foundation (Sep. 17, 2008). The Members of Eclipse, Minutes of the Eclipse Board Meeting, Sep. 17, 2008; The Eclipse Foundation (Sep. 09, 2008). Membership Logos [Board minutes]; IBM. (2001). 2001 IBM annual report, Armonk NY, p. 21 ("We donated more than $40 million in application development tools to a new, independent, open-source software community called Eclipse.").

[26] Executive Order 13718. (Feb. 09, 2016). Commission on Enhancing National Cybersecurity, Sec. 3(a)(ii). Barack Obama ("(ii) ensuring that cybersecurity is a core element of the technologies associated with the Internet of Things and cloud computing, and that the policy and legal foundation for cybersecurity in the context of the Internet of Things is stable and adaptable.").

Party had material influence and control over the execution of these executive orders, directly and through surrogates.

In fact, the NIAC uses the "Government's procurement power to encourage information technology suppliers to develop cybersecurity framework-compliant hardware and software."[27] In other words, the Executives, namely Presidents Clinton, Bush and Obama, with the assistance of the Hiring Party, forced broad use of Claimant's property by the bond holders. *See* also Endnotes [i] and [ii] Individual and Organization beneficiaries of Claimant's property; [iii] for sources.

2. Some of the more notable federal government beneficiaries of Claimant's property include, but are not limited to, Departments of State, Justice, Treasury, Homeland Security, Defense, Energy, Interior, Education, Transportation, Commerce, Agriculture; Census Bureau, Central Intelligence Agency (CIA); National Security Agency (NSA); National Security Staff (NSS); Securities & Exchange Commission (SEC); Director of National Intelligence (DNI); Drug Enforcement Administration (DEA); National Aeronautics and Space Administration (NASA); National Archives Administration (NARA); National Reconnaissance Office (NRO); Agency for International Development (USAID); Agricultural Research Service (ARS); Bureau of Alcohol; Bureau of Indian Affairs (BIA); Centers for Disease Control and Prevention (CDCP); Consumer Product Safety Commission (CPSC); Department of Health and Human Services (HHS); Environmental Protection Agency (EPA); Executive Office of the President (EOP); Federal Aviation Agency (FAA); Federal Bureau of Investigations (FBI); Federal Election Commission (FEC); Federal Emergency Management Agency (FEMA); Federal Trade Commission (FTC); Fish and Wildlife Service (FWS); Food and Drug Administration (FDA); General Services Administration (GSA); Housing and Urban Development (HUD); Institute of Museum and Library Science (IMLS); Merit Systems Protection Board (MSPB); National Institutes of Health (NIH); National Institutes of Standards and Technology (NIST).; National Oceanic and Atmospheric Administration (NOAA); National Reconnaissance Office (NRO); National Science Foundation (NSF); Occupational Health and Safety Administration (OSHA); Office of Inspector General (OIG); Office of Personnel Management (OPM); Small Business Administration (SBA); Bureau of Alcohol, Tobacco and Firearms (BATF); US Congress; US Patent Office; US Postal Service (USPS) and US Secret Service (USSS). *See* also Endnotes [i] and [ii] Individual and Organization beneficiaries of Claimant's property, [iii] for sources.

3. Secret NGO (non-governmental organization) bond holders who use, benefit from, and provide Claimant's property to third parties, include, but are not limited to:

   Past and present agents of the Executive, members of the National Infrastructure Assurance/Advisory Council (NIAC), The IBM Eclipse Foundation, AllSeen Alliance, Brookings Institution, World Economic Forum (Davos), Freedom House, Global Network Initiatives, Bilderberg Group, Trilateral Commission, Aspen Institute, Open Society

[27] NIAC (Nov. 21, 2013). Business Meeting Agenda. Recommendations, p. 117. DHS.

Foundations (OSF), Open Society Initiatives (OSI), The Clinton Foundation (incl. more than 35 pseudonyms), Bohemian Grove, Federal Reserve, NVCA, GCHQ, ASD, CSE, GCSB, FRE and FVEY. *See* also Endnotes [i] and [ii] Individual and Organization beneficiaries of Claimant's property; [iii] for sources.

6. DESCRIPTION OF LABOR, MATERIALS, SERVICES, ETC. PROVIDED TO THE PROPERTY BY THE CLAIMANT ("SERVICES"):

Claimant invested over $10 million in five years in research and development in the property. This creative work consumed over 145,000 engineering man-hours that created over 750,000 lines of computer source code.[28] The expenses include, but are not limited to, office facilities, communications gear, multiple server centers, servers, computers, switches, hosting sites, databases, testing, debugging, documentation, patents applications, trademarks, branding, product design and development, research, legal, equipment, payroll, transportation, public relations, travel, room & board, meeting expenses, conferences, consulting, insurances, facilities management, human resources, clerical, engineering, supplies, utilities, security, copyrights, legal, accounting, fund raising, data protection, general and administrative expenses, rents, leases, systems, procedures, accounting, auditing, bookkeeping, recruiting, training, professional development, management development, strategy, Malcolm Baldrige National Quality Award state program application and award, etc.

7. CONTINGENCIES:

Claimant reserves the right to update this Notice based upon new information obtained, most especially secret, stonewalled and redacted information regarding the full scope of the Executive's use of Claimant's property.

The remainder of this page is left blank intentionally.

[28] *Leader v. Facebook*, 1:08-cv-00862-JJF-LPS (D. Del. 2008), Tr. PgID Nos. 11423:21-11424:5.

MILLER ACT NOTICE FOR FEDERAL WORKS PROJECTS
40 USC §3131 ET SEQ.

Claimant:
Leader Technologies, Inc.,
Michael T. McKibben, 07/22/2017

YOU ARE HEREBY NOTIFIED THAT THE ABOVE-IDENTIFIED AND UNDERSIGNED CLAIMANT HAS NOT BEEN PAID IN FULL, AND INTENDS TO ENFORCE ITS RIGHTS UNDER THE MILLER ACT, 40 U.S.C. §§ 3131 ET SEQ. THE UNDERSIGNED CLAIMANT HAS FURNISHED LABOR, SERVICES, EQUIPMENT, AND/OR MATERIAL OF THE GENERAL DESCRIPTION ABOVE PROVIDED AND IDENTIFIED AS "SERVICES." SERVICES WERE FURNISHED FOR THE BUILDING, STRUCTURE, OR OTHER WORK OF IMPROVEMENT LOCATED AT THE ABOVE-DESCRIBED PROPERTY. THE PERSON OR FIRM WHO REQUESTED SUCH SERVICES IS ABOVE-IDENTIFIED AS THE HIRING PARTY. THE VALUE OF THE WORK, THE PAYMENT OFFSETS AND CREDITS, AND THE UNPAID BALANCE AND AMOUNT OF THIS CLAIM IS ABOVE-IDENTIFIED AS THE AMOUNT OF CLAIM. THE DATE ON WHICH THE SERVICES WERE LAST FURNISHED IS ABOVE-IDENTIFIED AS THE DATE SERVICES LAST FURNISHED.

REQUEST FOR INFORMATION

Claimant hereby requests a copy of each payment bond of each surety provider, including their contact information, to each and every public-private beneficiary used by the subcontractors to the Original Contractor to distribute Claimant's property identified in this notice. This request is made pursuant to 40 U.S.C. §3133. Please forward a copy to the Hiring Party and the Surety Parties identified above.

Claimant: **Leader Technologies, Inc.**

/S/ Michael T. McKibben

By: Michael T. McKibben
Title: Founder, Chairman and Inventor

Claimant: **Michael T. McKibben**

/S/ Michael T. McKibben

By: Michael T. McKibben
Individually

AFFIDAVIT & REQUEST FOR BOND

State of Ohio }
} ss:
County of Delaware }

FIRST BEING DULY CAUTIONED AND SWORN, AFFIANT STATES:

PARTY PROVIDING WORK:

Leader Technologies, Inc.,
Michael T. McKibben, Founder, Chairman and Inventor (the "Claimant")

PUBLIC AUTHORITY:

The United States Chief Executive Donald J. Trump, and his predecessors William J. Clinton, George W. Bush and Barack H. Obama (the "Executive")

My name is Michael T. McKibben, and I am of legal age, sound mind and otherwise competent to make this affidavit. At all times herein, I live in Columbus, Ohio and now work in Lewis Center, Ohio. I have personal, direct knowledge of each of the facts set forth in this affidavit and believe them to be true and accurate to the best of my knowledge and ability. Errors and omissions are inadvertent.

DESCRIPTION OF LABOR, MATERIALS, SERVICES, ETC. PROVIDED TO THE PROPERTY BY THE CLAIMANT ("SERVICES"):

Claimant invested over $10 million in research and development in the property which consumed over 145,000 man-hours of cross-expertise engineering that created over 750,000 lines of computer source code. The expenses include but are not limited to office facilities, communications gear, multiple server centers, servers, computers, switches, hosting sites, databases, testing, debugging, documentation, patents applications, trademarks, branding, product design and development, research, legal, equipment, payroll, transportation, public relations, travel, room & board, meeting expenses, conferences, consulting, insurances, facilities management, human resources, clerical, engineering, supplies, utilities, security, copyrights, legal, accounting, fund raising, data protection, general and administrative expenses, rents, leases, systems, procedures, accounting, auditing, bookkeeping, recruiting, training, professional development, management development, strategy, Malcolm Baldrige National Quality Award state program application and award, etc.

Claimant's property is "social networking" and related software intellectual property operating continuously on computers and servers in literally billions of locations in the United States and offshore.

America's Founders knew that a vibrant economy must protect and incentivize real inventors and writers to grow. The U.S. Constitution Article I, Section 8, Clause 8 ("[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.") protects patents and copyrights and is the only property right actually written in the Constitution.

The Founders also forbade the government in Article I, Section 9, Clause 3 from issuing a contract, then quashing it later under the color of law. These fundamental principles of property protection have been reaffirmed numerous times.

For example, James Madison said in Federalist No. 44: "Patent rights receive protection pursuant to public contracts between inventors and the federal government, acting on behalf of the people." Chief Justice John Marshall affirmed in *Fletcher v. Peck*. 10 US 87 (1810) that the government cannot rescind a contract once awarded. Subsequent Patent Office manuals reinforced this fundamental Constitutional principle: "A Patent is a Contract." *Manual of Patent Law* (1874), *A Summary of the Law of Patents* (1883).

Claimant has multiple patent contracts with the federal government that the government is using without compensating Claimant.

Claimant and his investors sought out a highly-regarded Washington, D.C. patent legal counsel in law professor James P. Chandler, III ("Chandler").[29] Claimant relied on his legal advice after sharing Claimant's innovations with him and the government. Claimant paid substantial fees to obtain patents that were eventually awarded by the government.

The remainder of this page is left blank intentionally.

[29] Professor James P. Chandler biography, http://www.nipli.org/1/1-3-2.html.

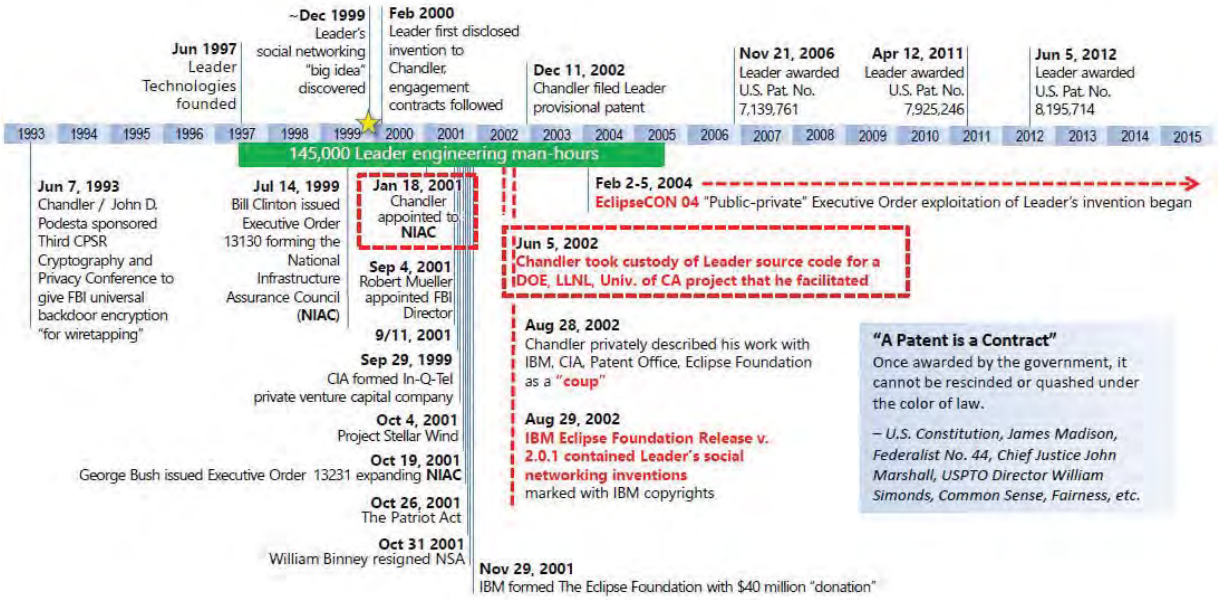


Figure 1: Timeline of events related to this Leader Technologies, Inc. claim.

However, Chandler turned over Claimant's property to a group of "public-private" collaborators with whom he was associated, without any notice or compensation to Claimant.

In February 2000, the Hiring Party, James P. Chandler, III entered into contracts with Claimant to provide legal, director and other services[30] that resulted in, among other things, the registering of trademarks, copyrights and the award of U.S. Patent Numbers 7,139,761,[31] 7,925,246[32] and 8,195,714.[33] Chandler was also then a senior national security advisor to the White House, Congress, Judiciary and intelligence community (e.g., FBI, NSA, CIA, DoD, DOJ, DoE, NRO, DHS, IBM), among others.

[30] James P. Chandler, The Chandler Law Firm Chartered, Leader Technologies Director Services and Engagement Letters, Apr. 6, 2000, May 5, 2000, Mar. 01, 2001, May 25, 2001; Chandler signed a Leader Directors Services Agreement on May 5, 2000 in which he specifically committed to the Business Judgment Rule duties of diligence, loyalty, obedience, accountability, disinterestedness, due care, good faith, abuse of discretion, e.g., "prohibited from using their position of trust and confidence to further their private interests" and "may not engage in undisclosed personal transactions of a material nature." Sec. 1(2), 1(2)(d).

[31] U.S. Pat. No. 7,139,761, Dynamic Association of Electronically Stored Information with Iterative Workflow Changes, McKibben et al, awarded by Jon W Dudas, Director, USPTO, Nov. 21, 2006.

[32] U.S. Pat. No. 7,925,246, Context Instantiated Application Protocol, McKibben et al, awarded by David J. Kappos, Director, USPTO, Jun. 5, 2012,

[33] U.S. Pat. No. 8,195,714, Radio/Telephony Interoperability System, McKibben et al, signed by David J. Kappos, Director, USPTO, Apr. 12, 2001.

Chandler is well known or strongly believed to have collaborated with numerous members of the political, legal and intelligence communities in this work, including, but not limited to Former FBI directors Louis Freeh,[34] Robert S. Mueller, James B. Comey; Rod J. Rosenstein; Andrew D. Goldstein; Preetinder Bharara; Eric H. Holder, Jr.;[35] Loretta E. Lynch; Williams & Connolly LLP;[36] Gibson Dunn LLP,[37] Fenwick & West LLP; Weil Gotshal LLP;[38] Skadden Arps, LLP; Cooley Godward LLP; White & Case LLP; Orrick Herrington LLP; Blank Rome LLP, Perkins Coie LLP, Latham & Watkins LLP; Cravath Swaine LLP,[39] Mayer Brown LLP; Hillary & Bill Clinton; John D. Podesta;[40] Directors of the CIA, NSA. DNI and National Security Advisors since 1993 through the Obama Administration; the Federal Circuit Court of Appeals;[41] Federal Circuit Bar Association,[42] American Bar Association,[43] FISC ("The FISA Court"); In-Q-Tel principals, their banker/underwriters and funded companies; National Venture Capital Association (NVCA); the Judicial Conference;[44] the national laboratories; and The Clinton Foundation.

At a minimum, the above-mentioned individuals, organizations and their principals should be excused from involvement in any investigations and decision making regarding Claimant's claim and compensation due to the appearance of impropriety. Further citations supplied upon request.

Chandler received detailed proprietary information about Claimant's invention properties for which he initially estimated that there were "over 60 patentable inventions." The industry now calls Claimant's inventions "social networking."

Chandler failed to disclose to Claimant his conflicts of interest and his material involvement with a "shadow government"[45] to which he was/is a key consultant.

---

[34] S. Hrg. 104-499 (Feb. 28, 1998). Economic Espionage Act Hearing, testimony of FBI Director Louis Freeh acknowledging James P. Chandler. U.S. Senate.

[35] Chandler, J. P. (Mar. 28, 2001). Trade Secrets and Enforcement of Intellectual Property Rights Conference. NIPLI (highlighted then Assistant Attorney General Eric H. Holder who was collaborating with Chandler on trade secrets and economic espionage cases, along with Robert S. Mueller, James B. Comey and Rod J. Rosenstein, among others).

[36] *United States v. James Hsu*, 155 F.3d 189 (1998) (James P. Chandler, III, for the Justice Department, and Paul Mogin, Williams & Connolly LLP, concluded the first prosecution of the Economic Espionage Act of 1996 ("EEA") drafted by Chandler for President Bill Clinton).

[37] Petition for Writ of Certiorari (Nov. 16, 2012), *Leader Technologies, Inc., v. Facebook, Inc.,* No. 12-617 (U.S. Supreme Court 2012) (Gibson Dunn LLP, White & Case LLP, Blank Rome LLP and Cooley Godward LLP represented Facebook and had personal relationships with Chief Justice John G. Roberts, Jr. who hold substantial Facebook financial interests, as do all of the lower court judges in this case).

[38] Graham, S. (May 23, 2014). Rader Steps Down as Chief, Apologies for Reines Email. *The Recorder*.

[39] Former Patent Office Director David J. Kappos's current law firm.

[40] James P. Chandler, John D. Podesta. (Jun. 07, 1993). Third CPSR Cryptography and Privacy Conference. Carnegie Endowment for International Peace ("to require [for the FBI] that telecommunications manufacturers and service providers redesign their systems to facilitate wiretapping.").

[41] Chandler bio, fn. 4.

[42] *Id*.

[43] *Id*.

[44] Report of the Secretary (Mar. 14, 2001). Report of the Proceedings of the Judicial Conference of the United States. Judicial Conference (Organizer of change to mutual fund reporting rules for federal judges and judicial employees: Jan Horbaly, Fed. Cir. Executive).

[45] National Press Office. (Sep. 2, 2016). https://vault.fbi.gov/hillary-r.clinton, Part 04 of 11, p. 56, ¶1. FBI.

Figure 2: On Jun. 8, 2000, James P. Chandler, III, and his legal assistant Kelley E. Clements (L/R, right rear, seated), participated, along with co-inventors Jeffrey Lamb and Michael McKibben (L/R, left rear, standing), in Leader invention design sessions in Columbus, Ohio where he learned the essences of Leader's social networking invention. *Photo: Leader Technologies, Inc.*

In 2002, under the color of attorney-client privilege and national security, Chandler obtained a custody copy of Claimant's invention engineering source code on Jun. 05, 2002.[46] Eleven (11) weeks later, on Aug. 29, 2002, he distributed Claimant's invention to his "public-private" collaborators[47] via Version 2.0.1[48] of the IBM Eclipse Foundation source code, his client ("Eclipse"). This new release contained no mention of Claimant and was marked only with IBM copyright notices.

Notably, just one day earlier, on Aug. 28, 2002, Chandler had met with Montgomery County, Maryland development officials on behalf of himself, IBM, the Patent Office and classified intelligence agencies (he specifically mentioned the CIA)[49] about acquiring a 30,000 sf. facility for plans that his notes described as a "coup." David J. Kappos was then chief inside intellectual

[46] James P. Chandler. (Jun. 5, 2002). LLNL-CRADA. CRADA No. TC-2030-01. The Regents of the University of California (Lawrence Livermore National Laboratory) under its U.S. Department of Energy Contract No. W-7405-ENG-48 and Leader Technologies, LLC for RAPIDLY DEPLOYABLE SECURITY SYSTEM, signed by Jeffrey Wadsworth for Director C. Burce Tartar. The Chandler Law Firm Chartered, PDF p. 36, Sec. 5, ¶5.

[47] Executive Order 13130, Sec. 2(1); Executive Order 13231, Secs. 1(b), 10(c).

[48] Version 2.0.1 (Aug. 29, 2002). Source code release including Leader Technologies' inventions marked with IBM copyrights. IBM Eclipse Foundation.

[49] Kelley E. Clements. (Aug. 30, 2002). Chandler Executive Assistant Clements' stenographer's minutes from meetings and events surrounding meeting among James P. Chandler and Montgomery County, Maryland development officers Dave Edgerley (Director), Janis Peters and May Webster (with the knowledge of Doug Duncan, County Executive) to negotiate use of $500-1,000,000 in federal budget support for a 40,000 sf. office space facility to be used by his organization NIPLI (National Intellectual Property Law Institute), the U.S. Patent Office archives, classified material (mentions CIA) and IBM, says no involvement of Congress and even used the phrase "(kind of a 'coup' of sorts)."

property counsel at IBM and an advisor to Chandler. (In 2009, Kappos was appointed director of the Patent Office by President Barack Obama.) Claimant had no knowledge of this attorney-client and directorial misconduct.

The IBM Eclipse Foundation was formed on Nov. 29, 2001 with a $40 million "donation" from IBM.[50] Through Eclipse's members, Claimant's property was distributed to and adopted widely by the bond holders under the moniker of "The Internet of Things."[51]

The Original Contractor's use of Claimant's property is ongoing and global in scope. The Hiring Party facilitated use of Claimant's property throughout a multitude of government agencies and private organizations, including but not limited to:

1. Suppliers to Executive Orders 13130 (July 14, 1999) National Infrastructure Assurance Council (NIAC), 13231 (October 16, 2001) National Infrastructure Advisor Council (NIAC) and their progeny, up to and including Executive Order 13708 (September 30, 2015) which expires on September 30, 2017 (unless renewed by the Executive), among others. **These orders give the Executive full authority to satisfy this claim.** The Hiring Party had material influence and control over the execution of these executive orders, directly and through surrogates.

   In fact, the NIAC uses the "Government's procurement power to encourage information technology suppliers to develop cybersecurity framework-compliant hardware and software."[52] In other words, the Executives, namely Presidents Clinton, Bush and Obama, with the assistance of the Hiring Party, forced broad use of Claimant's property by the bond holders. *See* also Endnotes [i] and [ii] Individual and Organization beneficiaries of Claimant's property; [iii] for sources.

2. Some of the more notable federal government beneficiaries of Claimant's property include, but are not limited to, Departments of State, Justice, Treasury, Homeland Security, Defense, Energy, Interior, Education, Transportation, Commerce, Agriculture; Census Bureau, Central Intelligence Agency (CIA); National Security Agency (NSA); National Security Staff (NSS); Securities & Exchange Commission (SEC); Director of National Intelligence (DNI); Drug Enforcement Administration (DEA); National Aeronautics and Space Administration (NASA); National Archives Administration (NARA); National Reconnaissance Office (NRO); Agency for International Development (USAID); Agricultural Research Service (ARS); Bureau of Alcohol; Bureau of Indian Affairs (BIA); Centers for Disease Control and Prevention (CDCP); Consumer Product

[50] Eclipse.org Consortium. (Nov. 29, 2001). Eclipse.org Consortium Forms to Deliver New Era Application Development Tools [Press release]; *See* also The Eclipse Foundation (Sep. 17, 2008). The Members of Eclipse, Minutes of the Eclipse Board Meeting, Sep. 17, 2008; The Eclipse Foundation (Sep. 09, 2008). Membership Logos [Board minutes]; IBM. (2001). 2001 IBM annual report, Armonk NY, p. 21 ("We donated more than $40 million in application development tools to a new, independent, open-source software community called Eclipse.").

[51] Executive Order 13718. (Feb. 09, 2016). Commission on Enhancing National Cybersecurity, Sec. 3(a)(ii). Barack Obama ("(ii) ensuring that cybersecurity is a core element of the technologies associated with the Internet of Things and cloud computing, and that the policy and legal foundation for cybersecurity in the context of the Internet of Things is stable and adaptable.").

[52] NIAC (Nov. 21, 2013). Business Meeting Agenda. Recommendations, p. 117. DHS.

Safety Commission (CPSC); Department of Health and Human Services (HHS); Environmental Protection Agency (EPA); Executive Office of the President (EOP); Federal Aviation Agency (FAA); Federal Bureau of Investigations (FBI); Federal Election Commission (FEC); Federal Emergency Management Agency (FEMA); Federal Trade Commission (FTC); Fish and Wildlife Service (FWS); Food and Drug Administration (FDA); General Services Administration (GSA); Housing and Urban Development (HUD); Institute of Museum and Library Science (IMLS); Merit Systems Protection Board (MSPB); National Institutes of Health (NIH); National Institutes of Standards and Technology (NIST).; National Oceanic and Atmospheric Administration (NOAA); National Reconnaissance Office (NRO); National Science Foundation (NSF); Occupational Health and Safety Administration (OSHA); Office of Inspector General (OIG); Office of Personnel Management (OPM); Small Business Administration (SBA); Bureau of Alcohol, Tobacco and Firearms (BATF); US Congress; US Patent Office; US Postal Service (USPS) and US Secret Service (USSS). *See* also Endnotes [i] and [ii] Individual and Organization beneficiaries of Claimant's property; [iii] for sources.

3. Secret NGO (non-governmental organization) bond holders who use, benefit from, and provide Claimant's property to third parties, include, but are not limited to:

   Past and present agents of the Executive, members of the National Infrastructure Assurance/Advisory Council (NIAC), The IBM Eclipse Foundation, AllSeen Alliance, Brookings Institution, World Economic Forum (Davos), Freedom House, Global Network Initiatives, Bilderberg Group, Trilateral Commission, Aspen Institute, Open Society Foundations (OSF), Open Society Initiatives (OSI), The Clinton Foundation (incl. more than 35 pseudonyms), Bohemian Grove, Federal Reserve, NVCA, GCHQ, ASD, CSE, GCSB, FRE and FVEY. *See* also Endnotes [i] and [ii] Individual and Organization beneficiaries of Claimant's property; [iii] for sources.

The remainder of this page is left blank intentionally.

BEFORE ME, undersigned authority, personally came and appeared Michael T. McKibben, who did declare under oath the following:

A. That he is an authorized and disclosed agent of the above-identified Party Providing Work, the Claimant. As the authorized and disclosed agent of the Claimant, he has been provided with the facts related to this Affidavit and Request for Bond, and to the best of his information, knowledge and belief, the facts set forth herein are true and correct. He is competent and authorized to make this Affidavit.

B. That Claimant, the Party Providing Work, has provided the above-identified Services to the above-described Project, and payment for the work provided has not been made.

Notice is hereby provided to the Public Authority to furnish to the Claimant, the Party Providing Work, a certified copy of the payment bond(s) and the contract(s) for the Project, as per any applicable statutes, or as per applicable Public Records Acts. These materials should be sent to:

Leader Technologies, Inc.
Michael T. McKibben
P.O. Box 224
Lewis Center OH 43035

FURTHER AFFIANT SAYETH NAUGHT

/S/ Michael T. McKibben

_____
Michael T. McKibben
Agent for Party Providing the Work
Claimant and Claimant Leader Technologies
Officer

SWORN AND SUBSCRIBED before me, a Notary Public, this ____ day of _____, 2017.

_____

ENDNOTES:

[i] **Attendee List at President Trump's Opening Remarks, American Technology Roundtable, WH, Jun. 19, 2017.**

President Donald J. Trump (Jun. 19, 2017):

"We have approximately $3.5 trillion dollars of market value in this room."

Surety Bond Holder Attendees: Oracle, Microsoft, IBM, CIA, Google, Alphabet, Facebook, Clarion, Palantir, Apple, Kleiner Perkins / CIA, VMWare, Dell, EMC, Palantir, NSA, In-Q-Tel, Intel, Qualcomm, Akamai, SAP, CMU, Hoover Institution, Stanford, MasterCard, Amazon, Washington Post, MIT, Accenture, Ohio State, UNC, Adobe and OpenGov.

Administration Attendees: John F. Kelley, Jared Kushner, Christopher P. Liddell, Steven T. Mnuchin, John Michael Mulvaney, David J. Shulkin, Ivanka M. Trump, Seema Verma

[ii] **Most of these organizations have used Claimant's property. received from the Hiring Party, and supplied it to third parties. They include, but are not limited to:**

(Names of responsible officials within these organizations will be supplied upon request.)[53]

18F, ABU Holding International Limited; Accel Partners LLP; AccelPath; Access; Accesso Fund LLC (Colombia, Clinton Foundation) (AFLLC); AccuRev; ACM Queue; Addison-Wesley; Adobe; Adastra Mining; Agitar; Airbnb; Aldon; ALGO; Allen & Co.; Alliance for a Healthier Generation (Clinton Foundation) (AHG); AllSeen Alliance; AMD; America Mineral Fields; American Scholars Inaugural Ball; ANCIT Consulting; Anyware Technologies; AOL; Apple; Ardoe Finance Limited; AT&T; athenahealth; Agua Caliente; Aptana; ARM; AvantSoft; AWD Holding AG; Baidu ADR; Baillie Gifford; Band Xi; Bank Menatep; Bank of America; Barclays; Barrick Gold Corporation; Battelle Memorial Institute; BEA; BEO; Bilderberg Group; Bill, Hillary & Chelsea Clinton Foundation (BHCCF); Bill & Melinda Gates Foundation; Blackberry; Blackdock; BlackRock; Boeing; Bohemian Grove; Borland; Bowles, Erskine; Bridge Masters (IOM) Limited; Brocade; Brox; BusinessObjects; BZ Media; Cape Clear; Cardew Services Ltd (DST); Carleton University; Castlight Health; Cedarville University; Chempolis; Cenit; Center for American Progress; Channel Trustees Ltd as trustee of the Yuri Milner Trust (DST); C.I.A. (Central Intelligence Agency); Cisco; Citibank; Citigroup; Ciudad Verde Amarilo Frailejon III (Clinton Foundation) (CVAF); Clarium Capital; Clinton Climate Initiative (CCI); Clinton Executive Service Corporation (CESC); Clinton Foundation (The) (TCF, CF); Clinton Foundation HIV/AIDS Initiative (CFHAI); Clinton

[53] Ref. Timeline, http://www.fbcoverup.com/docs/cyberhijack/cyber-hijack-findings.html.

Foundation Hong Kong (CFHK); Clinton Foundation Insamlingstiftelse (Sweden) (CFI); Clinton Giustra Enterprise Partnership (CGEP); Clinton Giustra Sustainable Growth Initiative (CGSGI); Clinton Global Initiative (CGI); Clinton Global Initiative - Asia (CFIA); Clinton Global Initiative University (CGIU); Clinton Health Access Initiative (CHAI); Clinton Health Matters Initiative (CHMI); Clinton Hunter Development Initiative (CHDI); Clinton Institute (CI); Clinton Small Business Initiative (CSBI); Cloud (The); Cloudera; Cloudsmith; CMA; CollabNet; Color of Change; Columbia University; Common Core; ComPeople; Computer Associates; Compuware; Cooley Godward LLP; Cooperative Research and Development Agreement (CRADA); CPSR (Computer Professionals for Social Responsibility); Council on Foreign Relations (CFR); Coupons.com; Cravath Swaine LLP; Credit Suisse; CRYPTO.com; CWI; DARPA; DC Systems; DDC-1; Dell; Deloitte & Touche; Deutsche Bank; DevZuz; DigiCash; Digital Sky Technologies (DST); Disney; Diversified Strategies Fund, L.P.; DocuSign; Dropbox; DSDM Consortium; DST (Digital Sky Technologies); DST Capital Partners Limited; DST Advisors Limited; DST Global Advisors Ltd; DST Global II, L.P.; DST Global Ltd; DST Holdings Ltd; DST Managers Ltd; DST USA II Ltd; DST USA Ltd; EADS; Eastman Chemical; eBay; Eclipse Foundation (The); EclipseCON 2004; Economic Espionage Act of 1996 (EEA); Edmundo; Embarcadero Technologies; ENEA; EOIR Technologies; Epion Holdings Limited; Ericsson; Enteraction; Etilix (USA)(Venezuela); Etish; ETRI; Eurotech, Ltd.; Eurotech, SpA; Facebook, Inc.; Fahr LLC (Steyer, Thomas F.); False Statements Accountability Act of 1996 (FSAA); Farallon Capital (Steyer, Thomas F.); FBDC Advisors Offshore, Inc. (FB=Facebook, Goldman Sachs); FBDC Investors Offshore Holdings, L.P. (FB=Facebook, Goldman Sachs); Federal Circuit Bar Association (FCBA); Fenwick & West LLP; Fidelity; Fiserv; Flickr; FOKUS; Forty Two (Clinton Foundation) (FT); Froglogic; Fujitsu; GAO (Government Accounting Office); Gates Foundation (Bill & Melinda); GDC Limited; GE; Genentech; General Dynamics; Generalitat Valenciana; Gentleware; Genuitec; Gerhardt Informatics; Ghegg; Gibson Dunn LLP; Glass-Steagall Act; Global Technology Partners; GMP Securities Ltd.; Goldman Sachs; Goldman Sachs Group Inc; Goldman Sachs & Co; Goldman Sachs Investment Partners GP, LLC; Goldman Sachs Investment Partners Private Opportunities Holdings, L.P.; Goldman Sachs Investment Partners Private Opportunities Holdings Advisors, Inc.; FBDC Investors Offshore Holdings, L.P.; FBDC Advisors Offshore, Inc.; Google; Gramm-Leach-Bliley Act of 1999; Greylock Partners; Groupon; GovTech; Harris, Jeffrey; Harvard Business School; Harvard Law School; Harvard University; Hellman & Friedman LLC (Steyer, Thomas F.); Hewlett-Packard (HP); Hitachi; Hoffman La Roche; Howcast; HSBC; IBM (International Business Machines); IBS; IDG; IDG Capital (China); IDG Technology Venture Investment III, L.P. ; IDG-Accel (China); IEEE; IMF; Ilog; Ingres; In-Q-Tel; Innoopract; Innovations Software; Inpriva; Instagram; Instantiations; Institute for Software; Intalio; Intel; International Consortium of Investigative Journalists; Intervoice; IONA; IoT; itemis; iWay Software; James LLC; Jekyll Island Club; Jiva; JNC -Opportunity Fund Ltd.; JNC Strategic Fund, Ltd.; JPMorgan Chase & Co.; Judicial Conference; Juniper Networks; Kanton Services Limited; Kanton Services (Belize) Limited; Kapino Group Holdings Limited; King & Spalding LLP; Kleiner Perkins LLP; KPMG;

KPIT Cummins Infosystems Limited; Krugle; Laszlo; Lawrence Livermore National Laboratory (LLNL); Lazare Kaplan International, Inc.; League of Nations; Lenovo; LinkedIn; Linux Foundation (The); Lockheed Martin Corporation; Lombardi; Lotus; Louisiana (Hurricane Katrina); LSI; Lucent Technologies; LynuxWorks; M.O.O.C.; Mail.ru (DST); Manchester University; Mango Software; Market LLC; Markland Technologies; Marsh & McLennan Capital, Inc.; McAfee; McManis Faulkner LLP; MDS Technologies; Media Matters; Medical Banking Policy Research (MB Project); Mentor Graphics; Meritech Management; Merrill Lynch; Metafinanz; Metallect; MexTel; Micro Focus; MicroDoc; Micron Technology; Microsoft; MicroTech; MISYS; Mitre Corp; MKS; Mobile Accord; MontaVista; Montgomery County (MD) Economic Development; Morgan Stanley; Motorola; Mozilla; mvalet; MySQL; NASA; National Economic Council (NEC); National Infrastructure Advisory Council (NIAC); National Infrastructure Assurance Council (NIAC); National Intellectual Property Law Institute (NIPLI); National Institute of Standards & Technology (NIST); National Security Agency (NSA); National Venture Capital Association (NVCA); Navigator Management LLC; NEC; NetApp; NetBridge; Netflix; New Enterprise Associates (NEA); New Media and Technology Investment; New Media Communications; New Media Technologies Capital Partners Limited; News Corporation; New York Times; Nexaweb; NexB; NextGen Climate Action (Thomas Fahr Steyer); No Ceilings: The Full Participation Project (Clinton Foundation) (NCTFPP); Nokia; Northrop Grumman; Novell; NPR; ObjectWeb; OC Systems; OCDemon Macraigor Systems; OCDemon; Ohio State University; OMG; Open Source Applications Foundation (OSAF); OpenGov; OpenMake Software; OpenMethods; Open Society Foundations (OSF); Open Society Institute (OSI); Open Source Lab; Open Systems Publishing; OPSEC; Oracle; Orland Properties Ltd (DST); Orrick Herrington LLP ; OW2 Consortium; Palamida; Palantir; Paltalk; Pandora; Parasoft; Paul Weiss LLP; PayPal; Perforce; Perkins Coie LLP ; Polcarion; Price Waterhouse; Progress Software; ProSyst; Protocode; PTAB (Patent Trial and Appeals Board); QNX; Qualcomm; QuestNet Corp.; Rational Software; Raytheon; RCP; RealNetworks; Red Hat; Redmond Media Group; Remain; Replay Solutions; Royal Bank of Canada (RBC); Renaissance Capital; RSA; RTC Group; Salesforce.com; Samsung; SAP; SAS; Serena; Siemens; SIGS Datacom; Silver Lake Partners; Skype; Skyway Software; SlickEdit; SMARTech; Software & Support Vertrag; Sony; Sony Ericsson; SpikeSource; SpringSource; Square; Squarespace; Stanford University; State Street Corp; Strandside Holdings Ltd; Stratfor; Stroz Friedberg; Sybase; Symantec; Symbian; T. Rowe Price; TARP; Task Force on National Healthcare Reform; Teamprise; Technest; Technovation Solutions; TechPresident; TEI; Telecredit, Inc.; Telelogic; Teneo Holdings; Tensilica; Texas Instruments; Thales; The Clinton Foundation (TCF, CF); The Clinton Initiatives (TCI, CI); The Clinton Museum Store (TCMS, CMS); The Eric Schmidt Project; The Full Participation Project (TFPP); The Internet of Everything; The Internet of Things; The William J. Clinton Foundation (TWJCF, WJCF); The William J. Clinton Presidential Center / Library (TWJCPC, TWJCPL); ThinkProgress; TIAA-CREF; TIBCO; TimeSys; TNI-Software; Too Small To Fail (Clinton Foundation) (TSTF); Toshiba; Trans-Pacific Partnership (TPP); TRC Group; Trident Nuclear Submarine Squadron; Trolltech; Tsinghua University; Tumblr;

Twitter; Uranium One; UrAsia Energy Ltd.; U.S. Copyright Office; U.S. Court of Appeals for the Federal Circuit (D.C.); U.S. Court of Appeals for the Ninth Circuit (CA); U.S. Department of Defense; U.S. Department of the Treasury; U.S. Digital Service; U.S. Global Investors, Inc.; U.S. Patent & Trademark Office; U.S. State Department; U.S. Senate Judiciary Committee; UBS; United Nations; United Ventures Ltd (DST); USM Internet Holdings Limited; Vanguard; Vector; Vectra Networks; Venture Strategy Partners (VSP); Verisign; VirtualLogix; Virtutech; Visa; Vista; W Software; Wal-Mart; Warburg Pincus; Washington Post; Webtide; Weil Gotshal LLP; Wells Fargo; West Wing (Clinton Foundation) (WW); Weston Presidio; White & Case LLP; White House; White Oak Group (The); Wiki; Wikipedia; Williams & Connolly LLP; William J. C. Foundation (Clinton Foundation) (WJCF); William J. Clinton Foundation (India) (WJCFI); William J. Clinton Fndn (Kenya) Char Trust (WJCFKCT); William J. Clinton Foundation UK (WJCFUK); Wilmer & Hale LLP (formerly Wilmer, Cutler & Pickering); Wind River; WininChina, Inc.; WJC Investments [William Jefferson Clinton, for profit] (WJCI); WJC, LLC [William Jefferson Clinton, for profit] (WJCLLC); Woodward LLC; Workday; World Bank; World Economic Forum (Davos); Wright-Patterson Air Force Base (WPAFB); Xbredex; Xerox Corporation; Yahoo; Yale University; YouTube; Yurie Systems; Zend; Zynga.

[iii] **Supporting Evidence.**

Archived and available from multiple sources including National Archives; Federal Register; Government Printing Office (GPO); Senate Judiciary Committee; Archive.org; Purdue University Law Archives; Judicial Conference; Department of Homeland Security (DHS); U.S. Patent Office (USPTO); Inspectors General for Departments of Commerce, State, Defense, Energy; Securities & Exchange Commission; PACER.gov; Eclipse Foundation; IBM; Federal Bureau of Investigations (FBI); Montgomery County Maryland Development Department; Leader Technologies; National Security Agency (NSA)("Collect It All"), U.S. Supreme Court; The New York Times; The Washington Post; The Wall Street Journal; The Huffington Post; Cooley Godward LLP; King & Spalding LLP; Kramer Levin LLP; White & Case LLP; Blank Rome LLP; Potter Anderson LLP; State of Ohio Department of Commerce; Office of Government Ethics (OGE); The Chandler Law Firm Chartered; Fenwick & West LLP; Harvard University; University of California; Lawrence Livermore National Laboratory (LLNL); Wright-Patterson Air Force Base (WPAFB); Defense Intelligence Agency (DIA); National Intellectual Property Law Institute (NIPLI); House Oversight Committee on Government Reform; Rep. Jim Jordan (OH-4th); Rep. Trey Gowdy (SC-4th); Mike Cernovich; Stefan Molyneux, Defense Advanced Research Projects Agency (DARPA); Swiss Leaks; WikiLeaks; DCLeaks; The Panama Papers; International Consortium of Investigative Journalists (ICIJ); Steve Piecznick; Fortune; World Bank; International Monetary Fund (IMF); Roger Stone; Reuters; ABC; CBS; NBC; Infowars; Alex Jones; Charlie Rose; PBS; FoxNews; Sean Hannity; Associated Press (AP); The Hill; AmLaw Litigation Daily; PatentlyO; The Recorder; ZDNet; Computerworld; CrunchBase; Bloomberg; The Daily Mail; The Guardian; PCWorld; IDG Financial Times; Full Measure; and Sharyl Attkisson, among others.

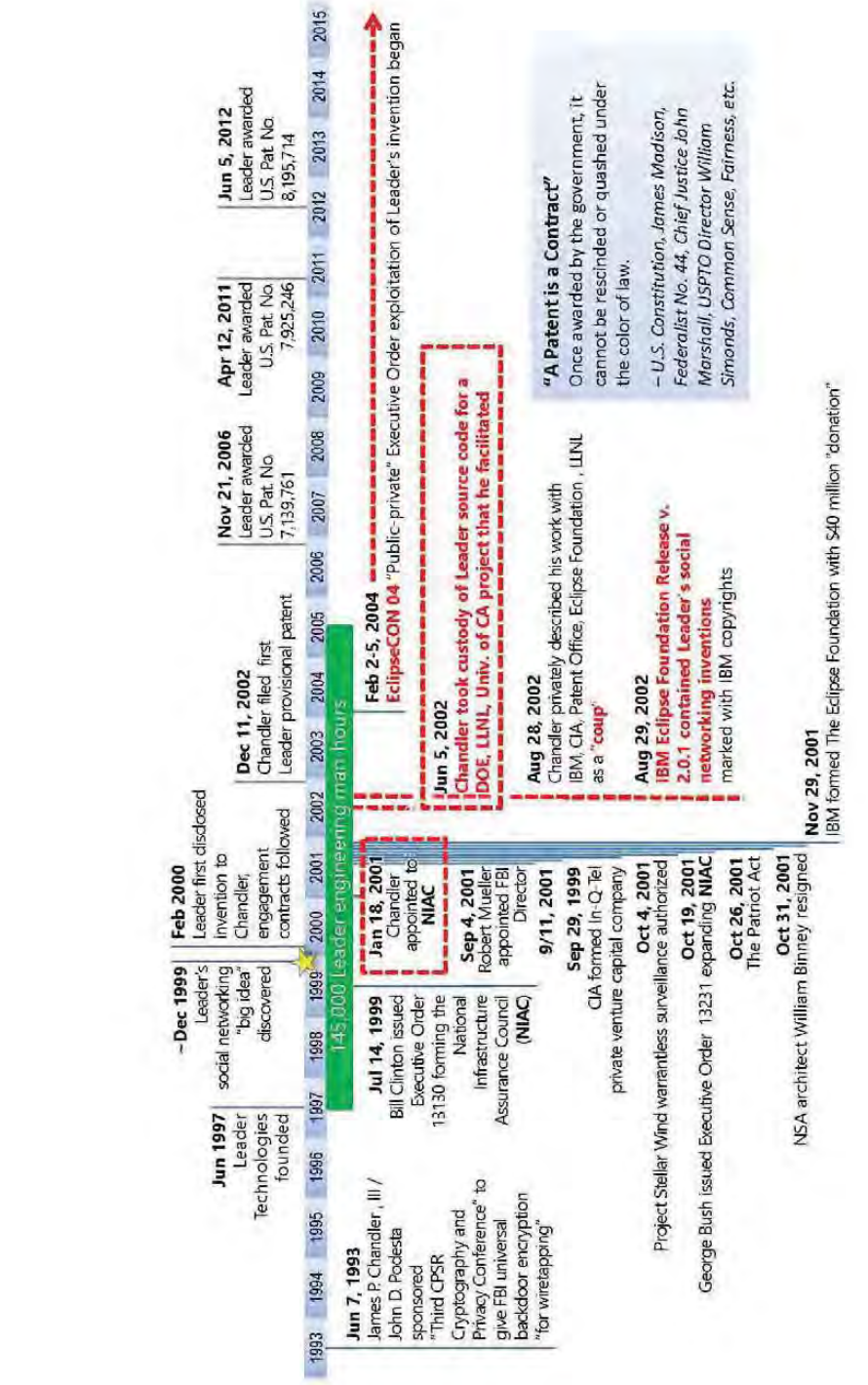


Figure 1: Timeline of events related to this Leader Technologies, Inc. claim.

PARTY PROVIDING THE WORK: Leader Technologies, Inc. / Michael T. McKibben v. PUBLIC AUTHORITY: The United States Executive Donald J. Trump and his predecessors William J. Clinton, George W. Bush and Barack H. Obama. MILLER ACT NOTICE FOR FEDERAL WORKS PROJECTS 40 USC §3131 ET SEQ., July 22, 2017.

PARTY PROVIDING WORK:

Leader Technologies, Inc.,
Michael T. McKibben, Founder, Chairman and Inventor (the "Claimant")

PUBLIC AUTHORITY:

The United States Chief Executive Donald J. Trump, and his predecessors William J. Clinton, George W. Bush and Barack H. Obama (the "Executive")

CERTIFICATE OF SERVICE

I, Michael T. McKibben, hereby certify that a copy of the MILLER ACT NOTICE FOR FEDERAL WORKS PROJECTS 40 USC §3131 ET SEQ was served on the Executive, President Donald J. Trump, at The White House, 1600 Pennsylvania Avenue NW, Washington, D.C. 20500 by Express Mail this July 22, 2017.

.

/S/ Michael T. McKibben

_____

Michael T. McKibben
Leader Technologies, Inc.
P.O. Box 224
Lewis Center, Ohio 43035
Phone: (614) 890-1986
Fax: (614) 864-7922
michael.mckibben@leader.com

Submitted July 22, 2017

Appellate Court Case Summary

Case Number: 962359
Filing Date: 08-28-2018
Supreme Court

Event Date	Event Description	Action
08-28-18	Original Action Against State Officer	Filed
08-28-18	Case Received and Pending	Status Changed
08-28-18	Other filing	Filed
08-29-18	Letter	Sent by Court
09-06-18	Filing fee	Received by Court
09-10-18	Notice of Appearance	Filed
09-11-18	Consideration on Action Against State	Filed
09-12-18	Letter	Sent by Court
09-17-18	Motion to Extend Time to File	Filed
09-18-18	Ruling on Motions	Filed
09-19-18	Motion for Reconsideration	Filed
09-20-18	Ruling on Motions	Filed
09-20-18	Letter	Sent by Court
09-20-18	Letter	Sent by Court
09-20-18	Motion - Other	Filed
10-09-18	Notice of Association of Counsel	Filed
10-12-18	Answer to motion	Filed
10-23-18	Reply to Response	Due

About Dockets

About Dockets

You are viewing the case docket or case summary. Each Court level uses different terminology for this information, but for all court levels, it is a list of activities or documents related to the case. District and municipal court dockets tend to include many case details, while superior court dockets limit themselves to official documents and orders related to the case.

If you are viewing a district municipal, or appellate court docket, you may be able to see future court appearances or calendar dates if there are any. Since superior courts generally calendar their caseloads on local systems, this search tool cannot display superior court calendaring information.

Directions

Supreme Court
Location: 415 12th Ave SW
Olympia, WA 98501-2314
Map & Directions
360-357-2077[General Information]
[Office Email]
Visit Website

Disclaimer

What is this website? It is a search engine of cases filed in the municipal, district, superior, and appellate courts of the state of Washington. The search results can point you to the official or complete court record.

How can I obtain the complete court record?
You can contact the court in which the case was filed to view the court record or to order copies of court records.

How can I contact the court?

SUPREME COURT
STATE OF WASHINGTON

James M. Miller, Citizen Petitioner, vs. SECRETARY OF STATE, KIM WYMAN Respondent	Case No. **PROVIDE AN UNBROKEN HUMAN CHAIN OF CUSTODY TO VERIFY IDENTITY, COLLECT, TALLY, CERTIFY, REPORT AND IMMEDIATELY PUBLISH THE LOCAL TALLY CARDS FOR ALL ELECTION RESULTS AND NOT USE ELECTRONIC DEVICES OF ANY KIND**

PETITION FOR WRIT OF MANDAMUS

/S/ James M. Miller

James M Miller, Citizen Petitioner
1 Blue Sky Place
Omak, WA 98841
(425) 471-8101
jimomak@leader.com

August 28, 2018

Respondent Representatives:

WASHINGTON SECRETARY OF STATE

Brenda Galarza
Records/Public Disclosure Officer
Service Designee
Kim Wyman, Secretary of State
Legislative Building
416 Sid Snyder Ave. SW
Olympia, WA 98504
(360) 704-5220
brenda.galarza@sos.wa.gov

Callie A. Castillo, Bar No. 38214
Service Designee
Robert W. Ferguson, Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
(360) 664-0869

TABLE OF CONTENTS

TABLE OF CONTENTS ii
TABLE OF AUTHORITIES iii
INTRODUCTION 1
STATEMENT OF THE CASE 12
Chain of custody in the current election process does not satisfy the Rules of Evidence, is not bipartisan, and relegates citizens to the status of mere spectators.
LAW & ARGUMENT 16
CONCLUSION & REMEDIES 20
EXHIBITS:

A. Laurie Thomas. (Jun. 8, 2018). James Miller signed response 6-8-18001. Okanogan County Auditor.
B. Brenda Galarza. (Jun. 29, 2018). PDR #18H-165 Public Records request for electronic voting procedures. Office of the WA Secretary of State, Elections Division.
C. Ron Wyden et al. (Jun. 12, 2018). Proposed Amendment to the Help America Vote Act of 2002. 115th Congress, 2d Session. U.S. Senate.
D. Jay Inslee. (Jul. 19, 2018). Letter to President Donald Trump. WA State Governor's Office.
E. Kim Wyman. (Accessed Aug. 03, 2018). Election Machine Inventory, SOS website. Washington, Secretary of State.
F. Angela Gunn. (Nov. 01, 2006). Who's building the gear that's running the show? *Computerworld*.
G. Anonymous Patriots. (Jul. 06, 2018). Scrap Electronic Voting Machines NOW! *Americans for Innovation*.
H. Phillip A. Brooks, (Sep. 18, 2015). Re. Notice of Violation, Volkswagen Software Hack To Modify Test Conditions Automatically. United States Environmental Protection Agency.
I. Ron Wyden. (Jul. 17, 2018). Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers. Ron Wyden.
J. Kim Zetter. (Jul. 17, 2018). Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States. *Motherboard*.
K. OKANOGAN County Election Procedures
L. James M. Miller. (August 5, 2018). Professional Experience and Resume.
M. Kim Wayman. (Accessed Aug. 06, 2018). System Security. Washington Secretary of State Website.
N. Don Reisinger. (Oct. 17, 2017). This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings. *Fortune*; and Staff. (Accessed Aug. 06, 2018). Our Supporters. Center for American Progress.

TABLE OF AUTHORITIES

Federal Cases

Brown v. General Motors Corp., 67 Wn.2d 278, 285, 407 P.2d 461 (1965)

Gallego v. United States, 276 F.2d 914, 917 (9th Cir.1960)

State Cases

Beggs v. City of Pasco, 93 Wash.2d 682, 689, 611 P.2d 1252 (1980)

Burson, 504 U.S. at 213 (Kennedy, J., concurring)

Cockle v. Dep't of Labor & Indus., 142 Wash.2d 801, 808, 16 P.3d 583 (2001)

Lybbert v. Grant County, 141 Wash.2d 29, 35, 1 P.3d 1124 (2000)

Port of Seattle v. Pollution Control Hearings Bd., 151 Wash.2d 568, 593, 90 P.3d 659 (2004)

Pub. Util. Dist. No. 1, 146 Wash.2d at 790, 51 P.3d 744

Port of Seattle v. PCHB, 90 P. 3d 659 - Wash: Supreme Court 2004 at 669

State v. Armendariz, 156 P. 3d 201 (Wash. SC 2007)

State v. Campbell, 691 P. 2d 929 - Wash: Supreme Court 1984

State, Dept. of Ecology v. Campbell & Gwinn, 43 P. 3d 4 - Wash: Supreme Court 2002

State ex rel. Hanson v. Wilson, 113 Wash. 49, 52 (1920)

Theodoratus, 135 Wash.2d at 599, 957 P.2d 1241

Washington State Rules of Evidence

Statutes & Rules

Washington State Constitution

RCW Section 6.17.110

RCW Section 6.17.120

RCW Section 7.16

RCW Section 7.16.170

RCW 29A.12.080

RCW 29A.12.030

RCW 29A.40.110

RCW 29A.40.020

WAC 434-250-045

WAC 434-250-110

WAC 434-260

WAC 434-261

WAC 434-261-045

WAC 434-662-060

Wash. R. Evid. 1006

Other Sources

Ramsey Touchberry. (Jul. 17, 2018). Election Hacking: Voting-Machine Supplier Admits It Used Hackable Software Despite Past Denials. *Newsweek*.

Staff. (Jun. 12, 2008). SEQUOIA VOTING SYSTEMS, INC. USES VOTE-COUNTING SOFTWARE DEVELOPED, OWNED, AND LICENSED BY FOREIGN-OWNED SMARTMATIC, A COMPANY LINKED TO THE VENEZUELAN GOVERNMENT OF HUGO CHÁVEZ. National Institute of Standards (NIST).

Lord Mark Malloch-Brown. (Jun. 04, 2018). Biography & Timeline. *Americans for Innovation*.

Senator Ron Wyden. (Jul. 11, 2018). Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers. Ron Wyden.

Kim Wayman. (Accessed Aug. 06, 2018). System Security. Washington Secretary of State Website. (Microsoft totally controls the Washington State election information technology infrastructure).

Don Reisinger. (Oct. 17, 2017). This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings. Fortune.

Staff. (Accessed Aug. 06, 2018). Our Supporters. Center for American Progress.

INTRODUCTION

Chain of custody in the current election process does not satisfy the Rules of Evidence, is not bipartisan, and relegates citizens to mere spectators.

The Constitution of the State of Washington, Article I, Declaration of Rights, Section 19, Freedom of Elections states:

> "All Elections shall be free and equal, and no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage."

Petitioner received an initial response to his inquiries into election processes. Exhibit A.

Statistical sampling of the vote cannot satisfy the rules of evidence because it cannot count all the votes, which is the only standard that can apply. State v. Campbell, 691 P. 2d 929 - Wash: Supreme Court 1984.

Petitioner has concluded that the current Washington State election process has been developed through administrative overreach that contravenes the law that says use of voting machines (instead of bipartisan human vote counters) can only be made by legislative decision. The use of electronic voting machines has *never* been the subject of a robust public debate on the most sacred of our citizen‘s rights—the right to free and fair elections. Remarkably, no unbroken bipartisan chain of custody exists in the current election process. In addition to common sense, the law says this chain of custody must satisfy the Washington Rules of Evidence, among them are WAC 434-662-060, WAC 434-250-110, WAC 434-261-050.

Worse, with our mail-in ballot process, we have no way to even determine a voter‘s identity and qualification to vote, who actually marked the ballot? Are they a citizen, do they live in the state? Are they even alive? Were they bussed in? Have they voted multiple times? Is this actually a person‘s pet named "Steve" voting? *No one knows*. Therefore, the Rules of Evidence

cannot be satisfied in any regard. The current move to do statistical sampling cannot possibly stop the onslaught of fraud that our current system invites.

No actual human counting of the mail-in ballots occurs in the current voting processes under the control of the Washington Secretary of State. Administrative authority, instead of legislative authority, has been relied upon to implement voting machines. These machines are whole *replacements* for bi-partisan chains of custody. This administrative overreach without legislative inclusion, is clearly unconstitutional; the 'will of the people' has been put in jeopardy.

Instead, citizens are merely spectators. The actual counting, tallying and reporting processes themselves are done inside computer software that is completely under the control of county supervisors and staff—who are generally partisans of the party currently in power, and therefore, not bipartisan by nature.

1. **Unseen digital bits cannot survive the Rules of Evidence regarding chain of custody.**

The vote counting function resides solely as *unseen digital bits* inside a vote-counting computer with *no human verification* performed at the time of the vote. In the current election system, while one might vote for Candidate A, the unseen software can easily change that vote to Candidate B. No bipartisan group can check for such fraud.

Brenda Galarza, Records/Public Disclosure Officer on Jun. 29, 2018 confirmed that no bipartisan chain of custody exists. **Exhibit B**.

2. **United States election assistance commission *substituted* for bipartisan chain of custody by Washington State citizens.**

Ms. Galarza says that the State has replaced a bipartisan investigation of electronic voting devices and software in our state with a *federal* break in the bipartisan chain of custody by "an independent testing authority designated by the United States election assistance commission" citing RCW 29A.12.080.

This statute violates the sovereignty of Washington State citizens‘ over our elections—and thus breaks the chain of custody. *See* RCW 29A.12.030 ("The secretary of state [not the federal government] shall inspect, evaluate, and publicly test all voting systems or components of voting systems"). The federal government has no authority to be involved in this important State‘s rights issue. This is a flagrant abuse of State‘s Rights on the Washington State vo

3. <u>"Two county auditor staff" *substitute* for bipartisan chain of custody.</u>

Ms. Galarza says "inappropriate or unauthorized access to the secured ballot materials and must be accompanied by at least two county auditor staff at all times. (WAC 434-261-045, WAC 434-250-110 & RCW 29A.40.110)."

This statement affirms that no bipartisan chain of custody is used. "Two county auditor staff" is not a bipartisan chain of custody.

Also, no procedure exists for bipartisan verification that the person or entity that mailed in the ballot is who he or she purports to be, or that he or she is qualified to vote.

4. <u>No citizen sees a "verifiable paper ballot" after the electronic scan.</u>

Ms. Galarza says that each voting device "must produce a voter verifiable paper ballot." This procedure is not followed and can only be considered willfully misleading. While she quotes the statute, this is not what happens.

All Washington citizens receive paper ballots in the mail. They do not use electronic voting machines to place their vote. See RCW 29A.40.020. Therefore, no citizen receives, or can verify, the electronic scan that occurs *after* the ballot is received back in the mail. In our state this opportunity for fraud is worse since, with mail-in ballots, we don‘t even know if the person who mailed it is real or qualified to vote. The counting is totally in the dark. This process is another break in a bipartisan chain of custody. In short, there is *no bipartisan chain of custody comparison* of the ballots whatsoever.

Article 1, Section 1 of the Washington Constitution states:

> "**All political power is inherent in the people**, and governments derive their just powers from the consent of the governed and are established to protect and maintain individual rights." (Emphasis added).

Washington citizens are being forced to rely on *pure speculation* that the electronic machinery used to verify the voter's identity, as well as scan, count and report the ballots are accurate. Bipartisan citizen counters are not part of the process.

5. **The current voting process *forces* election administrators to commit fraud since they cannot certify any vote in any county. In short, speculation of the integrity of a vote counting machine does not satisfy the Rules of Evidence regarding chain of custody.**

In the current election procedures, our state election judges are required to accept the unilateral word of private voting machine vendors who have allegedly validated a federal commission. Such outside certifications of our election devices, by nature, fail to ensure an unbroken bipartisan chain of custody required by the Washington State Constitution.

Vendor and federal statements of certification utilized by our officials should be more accurately defined as statements of faith, since they are relied upon in place of bipartisan review by citizens.

The claims made by election officials to Petitioner are largely false and thus at odds with the statutes. For example, the Washington Supreme Court stated in *Armendariz*:

> ¶ 8 Where the plain language of the statute is subject to more than one reasonable interpretation, it is ambiguous. *Cockle v. Dep't of Labor & Indus.*, 142 Wash.2d 801, 808, 16 P.3d 583 (2001). This court may attempt to discern the legislative intent underlying an ambiguous statute from its legislative history. Id. Likewise, this court may look to authoritative agency interpretations of disputed statutory language. *Port of Seattle v. Pollution Control Hearings Bd.*, 151 Wash.2d 568, 593, 90 P.3d 659 (2004). *State v. Armendariz, 156 P. 3d 201* (Wash. SC 2007).

Therefore, since the responses I received are ambiguous at best, this Court has the authority and duty to grant this writ to prevent prejudice against the citizens for a fair vote.

6. **Senator Patty Murray agrees that we must discard electronic voting, use paper ballots and insure unbroken, bipartisan chain of custody.**

Senator Patty Murray (D-WA) recently introduced "The Protecting American Votes and Elections Act" *mandating paper ballots* and *risk-limiting Audits*. She stated just weeks ago on Jun. 12, 2018:

> "With known vulnerabilities and a clear history of foreign interference, it is critical we take meaningful steps to protect the integrity of our elections and ensure the public's faith in our voting system." **Exhibit C**.

Why wait? A reasonable person will ask why Senator Murray did not first move to fix *Washington's* election system long ago? Nevertheless, this writ will remedy her delay in addressing *our* sovereign need to protect *our* elections.

According to Stuart Holmes, Voting Information System Manager, Office of the Secretary of State, fifteen percent (15%) of our electronic voting machines are provided by ES&S. Exh. C.

7. **Washington vote counting vendor ES&S *admits* a secret backdoor that can be exploited by hackers.**

ES&S just admitted to Senator Ron Wyden (D-OR)—after multiple prior denials—that they have secretly embedded the software program PCAnywhere in their voting machines, ostensibly to allow their engineers to maintain their devices remotely. This excuse rings hollow since ES&S lied about the presence of this backdoor access. The reality is that *any* programmer of normal skill in the art—not just ES&S programmers—can access these networked or standalone machines through preinstalled firmware and media voting devices if they have the

correct username and password. See *Newsweek*, July 17, 2018 [1] This fact alone shows sufficient *prima facie* risk to grant this writ. **Exhibit J**.

Further, on July 11, 2018, Senator Wyden testified to the U.S. Senate Rules Committee and published a Senate statement subtitled: Testifying at Senate Rules Committee, Wyden Blasts Voting Machine Manufacturers, Calls for Passage of His Bill Mandating Paper Ballots. [2]

8. Dubious OpTech software is contained in many Washington State voting machines.

On Jul. 23, 2018, Petitioner was told by Stuart Holmes, Voting Information Systems Manager, Office of the Secretary of State that "Smartmatic voting systems are not certified or used in the State of Washington." Exh. B.

However, the software engine inside Smartmatic is OpTech. OpTech software is also used in similar systems that *are* used in Washington, including ES&S (6 out of 39), Sequoia and Hart InterCivic (20 out of 39). **Exhibit E**

See also Angela Gunn. (Nov. 1, 2006). E-voting and voter registration: The vendors - Who's building the gear that's running the show? *Computerworld*. **Exhibit F** ("Smartmatic Corp., is privately owned, with a controlling interest held by founder and CEO Antonio Mugica. Mugica holds dual Spanish and Venezuelan citizenship. Sequoia offers AVC Edge and AVC Advantage DRE units, an AVC Edge DRE/VVPAT unit, and sells a Sequoia-branded Optech Insight optical scanner" and "Election Systems & Software also offers an Optech line").

---

[1] Ramsey Touchberry. (Jul. 17, 2018). Election Hacking: Voting-Machine Supplier Admits It Used Hackable Software Despite Past Denials. *Newsweek*. https://www.newsweek.com/election-hacking-voting-machines-software-1028948

[2] Senator Ron Wyden. (Jul. 11, 2018). Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers. Ron Wyden. https://youtu.be/XQzsoJSAtA4 ; *See* also https://www.wyden.senate.gov/news/press-releases/wyden-paper-ballots-and-audits-are-essential-to-secure-american-elections-against-foreign-hackers

9. **Proof of foreign interference in Washington State elections.**

Hart InterCivic used in the State of Washington licenses Sequoia's / Smartmatic's Optech Insight software originally developed in Venezuela.

See the National Institute of Standards (NIST) analysis which shows the real risk of foreign influence in our vote.[3]

Hart InterCivic licensee, Smartmatic is foreign-owned by SGO Corporation Limited (UK) / Smartmatic that is owned by British Privy Counselor associated with Lord Mark Malloch-Brown. Malloch-Brown is a close colleague of globalist George Soros who openly works to destabilize American elections. Malloch-Brown was a founding chairman of Soros' Open Society Foundation, vice President of Soros' Quantum Fund, and Vice Chairman of Soros' 'Soros Fund Management'. While Malloch-Brown was Deputy Secretary of the United Nations, he rented a Soros estate in upstate New York.

The involvement of Malloch-Brown and Soros in the OpTech licensing (inside ES&S and Hart InterCivic) shows an obvious threat of foreign interference in Washington State's elections. *See* Lord Mark Malloch-Brown Biography and Timeline. **Exhibit G**.

In Petitioner's FOIA questions, the state sidestepped the issue of the common OpTech software. This discrepancy begs the question as to how OpTech can be certified in ES&S and Hart InterCivic and not certified in Smartmatic. This ambiguity is deeply troubling, especially considering that ES&S's blatantly lied to Senator Wyden about their PCAnywhere backdoors. **Exhibit. I**.

---

[3] Staff. (Jun. 12, 2008). SEQUOIA VOTING SYSTEMS, INC. USES VOTE-COUNTING SOFTWARE DEVELOPED, OWNED, AND LICENSED BY FOREIGN-OWNED SMARTMATIC, A COMPANY LINKED TO THE VENEZUELAN GOVERNMENT OF HUGO CHÁVEZ. National Institute of Standards (NIST). https://www.nist.gov/sites/default/files/documents/itl/vote/SequoiaSmartmaticReport61208.pdf

10. **Incurable Uncertainty – Numerous breaks in the bipartisan chain of custody must be cured before electronic voting can be relied upon, if ever.**

The State's current election procedures create an incurable uncertainty as to the veracity of the vote count since the process has numerous breaks in the bipartisan chain of custody as discussed herein, as highlighted by Senator Ron Wyden. *Supra*.

"Trust me" affirmations by election officials alone are inadequate to trust the vote tallies. **Counting the vote is the exclusive purview of the citizens themselves.** State bureaucrats have an *inbuilt conflict of interest* to have their bosses remain in power. Washington State's election machine processes suffer from an incurable uncertainty regarding the ballot vote tally process and results. In addition, as soon as a ballot is read into the scanner, the votes are *hidden*, secret and unable to be certified. **This is a break in the bi-partisan chain of custody**.

Put more simply, on election day, no identity validation is done, and no bipartisan *human* tally of the votes is used to audit the ballot scanning machines of the mailed in ballots.

All testing of electronic voting machines is done *a priori* (before a vote). No *post priori* (after the vote) testing is done. This too is a flaw in the certification and auditing processes. Common sense says that the current system is ripe for fraud.

11. **No honest engineer could certify electronic voting machines.**

Even as advancing technology and contemporary lifestyles drive evolution in our method of voting, Washington's statutory regime manifests clear legislative intent to assure that secrecy in the method of voting in every election is absolute.

The secret ballot must not devolve into a mere 'state secret' held by officials promising not to tell. And yet, with the current technology, a state secret has occurred with the implementation of machine voting. No matter how many tests are done, the voter is dependent on speculation rather than bi-partisan, empirically observable phenomenon.

12. <u>The citizen sees nothing; the "observers" are mere spectators</u>.

The citizen cannot see the circuits, firmware, malware, or any software. The citizen sees NOTHING about how his or her vote is tallied. They are not present when the machines print a receipt, so they cannot check the scan for accuracy. The voter does not know if the software could detect when it was being tested and fool the testers—like the Volkswagen diesel fraud that hid poor emissions results from regulators for years. The software for the Volkswagen modified itself under test. **<u>Exhibit H</u>**. This very same possibility exists with all the election machines used by the State.

13. <u>Washington State voter's rights to a fair election should not be subjected to speculation as to the authenticity.</u>

Since no empirical human, bipartisan observation at all is part of this counting and reporting process, it is incurably uncertain.

The citizens of the State of Washington have no adequate remedy for this incurable uncertainty other than this Writ of Mandamus. The Secretary of State, Kim Wyman, must be compelled to:

(1) Verify the true identity and qualification of each voter to vote,

(2) Add human bipartisan counting of paper ballots where a voter submits the vote card and immediately has his or her finger dipped in suitable purple voting dye used around the world to ensure "one person, one vote,"

(3) Preparation of a tally sheet that is certified by the human bipartisan counters and immediately photographed and published on each county website,

(4) Hand delivery of that tally sheet to the state election tabulator by each group of county bipartisan election judges,

(5) Verification that the state election tabulator has entered the county's certified tabulation. This process must be done in lieu of or in addition to the use of electronic devices that can be used as an audit verification adjunct—but never again as the primary vote counting and tally processes.

The state will prevail without this injunction, as no remedy is being offered, and the will of the people is subject to the very real danger of interference in free and fair elections.

The benefit of this injunction outweighs any process utilized by the state, if that process thwarts the true and constitutional expression of the will of the people at the polling place.

The people of the State of Washington have the right of relief from this current state election process that evidently thwarts their constitutional rights.

It is the duty of the Secretary of State to provide a free election according to the Washington State Constitution without regard to any hardship such a duty imposes.

According to the Secretary of State, she recognizes the vulnerabilities in the State's elections processes that this writ addresses. This is more prima facie evidence of a problem whose solution appears to be being delayed for purely partisan political reasons.

Brenda Galarza, representing Kim Wyman, announced that voting irregularities will be addressed in 2019 using human statistical sampling of ballots. Exh. B.

First, why wait until 2019?

14. <u>Statistical sampling is easily fudged and does not replace unbroken bipartisan chain of custody sufficient to satisfy the Rules of Evidence.</u>

Second, why statistical sampling when we can just count and certify all votes in real time? Statistical sampling appears to be another euphemism for an excuse to hide rigged voting. Bipartisan human counting solves this problem.

State officials always use alleged cost savings to justify continued use of electronic machines. This argument is fallacious for several reasons.

First, the primary objective is a free and fair vote, not cost savings. **A fair vote—no matter what it costs—is the true objective.**

Second, bipartisan citizen volunteers needed to count the votes do not require payment for their services.

Third, it is very easy for bureaucrats to hide partisanship inside the cost savings argument.

Fourth, if vote counting takes a week or more, so be it. The rush to have election-night results only serves to hide and promote fraud and a rush to bogus judgment.

By the Senator Murray‘s and Secretary of State Wyman‘s admissions, the machine counts do not provide the certainty necessary to meet statutory requirements. Only a whole and complete, bi-partisan chain of custody human tally count of the ballots can overcome the incurable uncertainty of the existing processes.

Any process that is hidden and secret (like the ones currently used) is unconstitutional. In fact, the current processes force election judges in each county to certify a fraud, since they have not themselves counted the votes.

Statistical mathematics, silicon circuits, certificates of authenticity, incomplete responses to public records, protestations, and technical obfuscations are not logical or acceptable substitutes for direct human empirical observations operating under the constitutional principle of bi-partisan chain of custody.

The Petitioner also makes the claim that the decision to utilize electronic voting machines in any manner, has not been properly adopted by the state pursuant to *Ballasiotes v. Gardner, Supreme Court of Washington, March 18, 1982, No. 48295-1.* This court specifically addressed

the issue at hand. The current system is administrative by nature, and directly contradicts this opinion. The use of machines, by any county, electronic or otherwise, to replace the un-broken bi-partisan chain of custody is not supported, since electronic machines were never specifically debated and decided by the legislature.

The ignoring of *Ballasiotes* is *prima facie* evidence that no machines including electronic devices in the electoral process in counting the ballots are legal as they have not been properly adopted by the people. To be clear, the Petitioner is not contending that machines can‘t be used to transport ballots, move them around, or to publish pictures of tally sheets on the ~~–I~~nternet of Things”; the Petitioner is saying that machines can‘t be used in the bi-partisan counting and tally of the votes; the machines have not been 'properly adopted‘, and represent a *prima facie* break in the bi-partisan chain of custody; which is illegal in the State of Washington.

15. <u>Vote counting process is not bipartisan.</u>

Nowhere in WAC 434-260 ELECTION REVIEW PROCESS AND CERTIFICATION OF ELECTION ADMINISTRATORS is the vote counting process in the State of Washington bipartisan—meaning selected election administrators from each political party oversee the vote counting process. Rather, paid partisan employees of the Secretary of State do. This is yet more *prima facie* evidence that vote counting in the State of Washington is run by bureaucrats that can press their own agendas outside the electoral process. The opportunity for manipulation and fraud is evident.

It all depends on what the definition of "may" is

Instead, "observers" from parties merely watch the process like spectators at a baseball game with their beer and brats. See WAC 434-261-020. The break in the bipartisan chain of custody is quite evident in WAC 434-250-110. PROCESSING BALLOTS:

> "(6) Final processing of voted ballots, w*hich **may** include scanning ballots on an optical scan voting system*, may begin after 7:00 a.m. on the day of the election." (Emphases added).

This law implies that ballots are counted by humans. However, very evidently, the Secretary of State has relied upon the single word "may" for her overreaching authority that now counts ALL ballots electronically. A reasonable person will consider the substitution of ALL for MAY a willful misinterpretation of the statute, if not administrative abuse.

Since Petitioner has established that unseen, *unobservable* electronic bits and bytes in all electronic voting systems breaks the bipartisan chain of custody, the Washington State Statute itself proves that a break occurs at vote counting. This is more *prima facie* evidence why this writ must be granted.

Statistical sampling *implies* vote counting errors which CITIZENS DO NOT WANT!

The need for this writ is further reinforced by the most recent order by the Secretary of State to do statistical sampling of one race in three precincts in each county.[4] This process is mathematically meaningless. In mathematics, a statistical standard of deviation ***implies and***

[4] Kim Wyman. (Jul 16, 2018). Protecting Our Votes Means Strengthening Cybersecurity. The Aspen Institute. https://www.aspeninstitute.org/blog-posts/protecting-our-votes-means-strengthening-cybersecurity/; *See* also Kim Wyman. (Mar. 29, 2018). Washington to receive nearly #$8 million to upgrade elections systems. Washington Secretary of State. https://www.sos.wa.gov/office/news-releases.aspx#/news/1280

assumes errors in the vote counting! Predicative mathematical values in a statistical sampling are meaningless to a fair and accurate vote. **It assumes that it is not accurate!**

The 2004 HBO expose *Hacking Democracy* clearly shows how electronic voting machines can be tampered with *after* passing quality assurance testing.[5]

STATEMENT OF THE CASE

The previous discussion and law is fully incorporated herein. Counting votes in a bipartisan way is a founding principle of a Constitutional Republic. Unbroken chain of custody must satisfy the Washington State Rules of Evidence.

The Washington State Constitution states that that free elections without interference are a citizen‘s right. Any uncertainty in the count is unacceptable.

The burden to maintain the reliability of the vote is the highest and most solemn duty of a citizen in our Republic. It is the county auditor‘s duty to ensure that processes, as defined by the Secretary of State are properly enabled. Among these duties is the maintenance of a bipartisan chain of custody of the ballots and the counting of those ballots.

This maintenance should be by *empirical observation by humans*, who cooperate under lawful penalty to ensure that the ballots, as marked, are not compromised. Elections chain of custody refers to physical and electronic evidence controls for:

1. who can vote
2. who did vote
3. actual ballots as marked by each voter, and
4. evidence transfer and storage

The current process is highly prone to recounts and litigation because it departs dramatically from the statutory requirements.

---

[5] Hacking Democracy (2006). The Hack Trailer. *HBO*. https://youtu.be/t75xvZ3osFg

Proper accounting requires chain of custody measures, which auditors use to assess information reliability. Chain of custody is dictated by the Rules of Evidence. The current election processes do not comply at any point.

The current State of Washington process to maintain bi-partisan chain of custody fails under the current process. The reasons for the failure is very simple. First, the person‘s identity and qualification to vote cannot be verified. Then, the use of the electronic scanning machines causes the loss of bi-partisan chain of custody as soon as a ballot is scanned. While a paper receipt is created at the time of the scan, the voter is not present since the ballot was mailed in. So, the requirement for a printed receipt is nonsensical. The voter is treated more respectfully at Dairy Queen. At least they get a real receipt at DQ!

Further, in the current process no one knows if the person‘s name on the mail-in ballot is really that person. The notion that proper voters identification is somehow a burden on the citizenry is nonsensical. We show our identification every time we use a credit card, or cash a check, or sign up for Medicare or Medicaid.

In the current State of Washington voting process, no qualified voter is able to confirm that the scan of their ballot is accurate or is totaled accurately. The current system defies logic and commons sense.

There is no summation tally audit for the voting machines that scan the mailed in ballots. Further, the citizen‘s vote is not counted by bi-partisan humans.

This process is the definition of incurable uncertainty. No certificate of assurance from any entity, test, encryption, or machine language can prevent this loss of observation.

A human citizen voter cannot observe an integrated circuit, silicon chip, or the software programming embedded on the chip. Therefore, no one attests to an unbroken chain of custody.

A statistical sampling of the voting summation cannot cure this uncertainty since such samplings are based on totals that have not been prepared by bipartisan counters. On Aug. 06, 2018, Petitioner spoke with Jessica at the Okanogan County Auditor Office. She confirmed that a new statistical sampling of ballots will start occurring with the 2018 primary election on Aug. 07, 2018. However, she was unable to provide Petitioner with the bulletin from the Secretary of State that directed them to perform the new sampling.

The logic is simple . . . what the human eye cannot see, without concurrence under bi-partisan chain of control, is a fraud disguised by technology.

Evolving voting methods have produced systems that contain significant holes in chain of custody which call election legitimacy into question.

Three voting methods breach bipartisan chain of custody:

(1) vote-by-mail,

(2) electronic voting, and

(3) Internet voting.

These methods make it IMPOSSIBLE for the public to verify that:

(a) the voter is who they say they are and are qualified to vote,

(b) all ballots cast were counted;

(b) ballots counted were not altered; and

(c) unauthorized votes were not added.

Therefore, it is the duty of the Secretary of State, Kim Wyman, to provide a cure for this outrageous indiscretion regarding the expression of the will of the people. She should be compelled by this Court to direct each county: (1) to only allow counting of the mail-in ballots by bipartisan citizens groups who verify the valid identity of each voter, and (2) to post the tally

results on each county website so that the certified tally card is immediately observable by all citizens; the intent is to ensure ‗human ballot counting and tally' while maintaining observable bi-partisan chain of custody over the ballots themselves.

Remarkably, none of these public officials who responded to the Petitioner could provide evidence that the election machines themselves were safe from internal/external tampering, or that the processes surrounding the use of these machines were able to provide an unbroken, bipartisan change of custody.

It is evident that this assurance could not be provided because it cannot be verified. The petitioner's request for more information about the voting machines was denied under RCW 42.56.270, the Public Records Act.

Petitioner filed for administrative relief in court but was informed that he would be liable for all legal costs incurred by the vendor to respond, per the Okanogan County Prosecuting office.

Petitioner was provided the copious documentation about election processes and controls used by the State. **Exhibit K.** The necessity for this writ was made patently obvious after discovering the flaws in our processes that are large enough to drive a truck through.

16. Petitioner is a recognized expert in organization systems, procedures and processes

The Petitioner is a retired Boeing project manager who has been responsible for complex airplane critical and flight safety avionics software and hardware involving multiple-billion dollar projects. This makes him an expert in system processes, procedures and quality. The Petitioner hereby certifies that in his professional judgment, after studying all the information provided in this writ, the programs and processes used in the State of Washington voting processes are woefully inadequate and appear to be willfully so. Petitioner asserts that no honest process engineer could possibly certify what can best be described as a magical process that

could have only ever been intended to rig elections. Petitioner's firm conclusion is that the systems and procedures are so convoluted as to lead a process engineering expert to conclude that *mischief* is the only possible use and outcome of the current election system in the State of Washington. *See* Petitioner's expanded resume and expertise in **Exhibit L**.

17. Microsoft controls our data; Microsoft is not bipartisan

The Secretary of State's website under ~~–~~System Security" states:[6] **Exhibit M**

> "Patch Management:
>
> The Quality Assurance (QA) system is patched the day after any "patches", "hotfixes", or "cumulative" updates are received from **Microsoft**. Production (prod) servers are patched after the system updates are fully tested in QA and authorized for deployment. In most cases, the production system patched two weeks after QA to allow for testing and verification.
>
> Elections Results Site
>
> The elections results are hosted in **Microsoft's** Azure cloud, which provides server and geographic redundancy." (Emphasis added.)

It is notoriously public knowledge that Microsoft is a partisan of far left-leaning organizations. *Fortune* magazine assessed Microsoft's political leanings stating:

> "Microsoft is another supporter of the Brady Campaign, which earned it low marks on 2nd Amendment rights. The tech giant was also hit for being 'a partner' of The Nature Conservancy, a liberal and active proponent of cap-and-trade and a carbon tax."
>
> In its evaluation of Microsoft, 2ndVote also says that the company supports organizations, like Center for American Progress and the League of United Latin American Citizens, which support sanctuary cities."[7]

---

[6] Exh. M. Kim Wayman. (Accessed Aug. 06, 2018). System Security. Washington Secretary of State Website. https://www.sos.wa.gov/elections/system-security.aspx

[7] Exh. N. Don Reisinger. (Oct. 17, 2017). This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings. *Fortune*; See also Staff. (Accessed Aug. 06, 2018). Our Supporters. Center for American Progress.

The Center for American Progress is notoriously known to have been founded by Democrat operative John Podesta, who is notoriously known to have intimate political ties to George Soros, Hillary Clinton, The Clinton Foundation and other far left-leaning political organizations.

A reasonable person can easily see that the Washington State election process is completely compromised by Microsoft‘s partisan control of vital elements of our election system. **Exhibit N**.

LAW & ARGUMENT

The previous discussion and law is fully incorporated herein. The current ballot scanning process in the State of Washington cannot guarantee that the tally is correct because it is not performed by humans. Voters do not even observe the electronic scanning in the counties. Humans only enter the ballot into the machine, and no human tally occurs outside of the machine, thus breaking the bi-partisan chain of custody empirical observation.

Petitioner, and the rest of the citizenry, have a right to rely upon the truthfulness of the statements of public officials. When those statements contradict the statutes, this Court can intervene. The Washington Supreme Court stated:

> ¶ 8 Where the plain language of the statute is subject to more than one reasonable interpretation, it is ambiguous. *Cockle v. Dep't of Labor & Indus.*, 142 Wash.2d 801, 808, 16 P.3d 583 (2001). This court may attempt to discern the legislative intent underlying an ambiguous statute from its legislative history. *Id.* Likewise, this court may look to authoritative agency interpretations of disputed statutory language. *Port of Seattle v. Pollution Control Hearings Bd.*, 151 Wash.2d 568, 593, 90 P.3d 659 (2004). *State v. Armendariz*, 156 P. 3d 201 - Wash: Supreme Court 2007 at ¶ 8.

This Court may grant relief when a state agency is acting erroneously and in contradiction to the statute. The Washington Supreme Court stated in *Port of Seattle*:

> This court may grant relief if we find that the PCHB [Pollution Control Hearings Board] order is "outside the statutory authority or jurisdiction of the [PCHB]" or

> if the PCHB has "erroneously interpreted or applied the law." RCW 34.05.570(3)(b), (d). Where statutory construction is necessary, this court will interpret statutes de novo. Pub. Util. Dist. No. 1, 146 Wash.2d at 790, 51 P.3d 744. *Port of Seattle v. PCHB*, 90 P. 3d 659 - Wash: Supreme Court 2004 at 669.

While equitable estoppel is not favored, as is request here, it is needed when a manifest injustice is threatened or is occurring, as is the case here. The Washington Supreme Court affirmed this in *Ecology*:

> Equitable estoppel against the government is not favored. *Id*. Accordingly, when the doctrine is asserted against the government, it must be necessary to prevent a manifest injustice and applying estoppel must not impair the exercise of government functions. *Id*. Proof of the elements of estoppel must be by clear, cogent and convincing evidence. *Id*. *State, Dept. of Ecology v. Campbell & Gwinn*, 43 P. 3d 4 - Wash: Supreme Court 2002 at 14.

The *Ecology* opinion describes a procedure for determining if a manifest injustice is occurring:

> Equitable estoppel may apply where there has been an admission, statement or act which has been justifiably relied upon to the detriment of another party. *Lybbert v. Grant County*, 141 Wash.2d 29, 35, 1 P.3d 1124 (2000); *Beggs v. City of Pasco*, 93 Wash.2d 682, 689, 611 P.2d 1252 (1980). Establishment of equitable estoppel requires proof of (1) an admission, act or statement inconsistent with a later claim; (2) another party's reasonable reliance on the admission, act or statement; and (3) injury to the other party which would result if the first party is allowed to contradict or repudiate the earlier admission, act or statement. *Theodoratus*, 135 Wash.2d at 599, 957 P.2d 1241. *Id*.

This writ satisfies the need for this Court to equitably estop the Secretary of State from engaging in fraudulent voting practices.

(1) "*an admission, act or statement inconsistent with a later claim*" - As shown above, the admissions and statements by public election officials are inconsistent with the statute and with the election system procedures and processes.

(2) "*another party's reasonable reliance on the admission, act or statement*" - Both Petitioner and all Washington citizens have reasonably relied upon the Secretary of

State‘s election procedures and processes as the sole supplier of these public services. Therefore, the Petitioner has no choice but to rely upon these statements as truthful and in compliance with the statutes.

(3) "*injury to the other party which would result if the first party is allowed to contradict or repudiate the earlier admission, act or statement*" – A reasonable person knows that elections have direct material consequences to the administration of our Constitution. Winning candidates are given real power and authority in our State as a result of these elections. The new evidence shows that these publicly-elected officials have been empowered on the basis of flawed, if not fraudulent, voting processes that *pretend* to be compliant with the statute. As a result, any mere repudiation of prior statements and admissions only further damages the Petitioner by allowing the officials to further obfuscate the true nature of our flawed elections systems. The damages to Petitioner and our State are only exacerbated and real bipartisan fixes are only delayed.

The responses received by state public officials refused to provide substantive information about the mechanics of the voting systems currently used. **Exhibit I**. The documentation provided by the Okanogan County Auditor‘s office is too voluminous to incorporate herein. Therefore, it will be made available upon request pursuant to Wash. R. Evid. 1006.

Purity of the Ballot

The Supreme Courtin Hanson affirmed the priority for purity that should motivate this Court to grant this writ:

> Our democratic system of free and fair elections hinges on enforcement of the Constitution‘s and Legislature‘s carefully constructed array of provisions securing

> for an absolutely secret method of voting. The Constitutional requirement of an absolutely secret ballot, independently and as implemented by statute, is fundamental. "The terms of the statute are absolute, explicit and peremptory; no discretion is given. They are designed to secure the secrecy and purity of the ballot, are mandatory in their character and binding upon the electors." *State ex rel. Hanson v. Wilson*, 113 Wash. 49, 52 (1920).

Voting: A Fundamental and Cherished Liberty

> "Voting is one of the most fundamental and cherished liberties in our democratic system of government." *Burson*, 504 U.S. at 213 (Kennedy, J., concurring).

Secretary of State may not compromise the vote

This writ calls for institution of an unbroken bipartisan chain of custody immediately.

Chain of Custody in Washington State law is defined as:

> "Chain of custody" means the documentation of the succession of offices or persons who held public records, in a manner that could meet the evidentiary standards of a court of law until their proper disposition according to an approved records retention schedule.
>
> The agency must maintain chain of custody of the record, including employing sufficient security procedures to prevent additions, modifications, or deletion of a record by unauthorized parties. If there is a break in chain of custody, it must be noted in the transmittal to the archives. WAC 434-662-060. Authentication and chain of custody of electronic records.

The Washington Supreme Court in *Campbell* states regarding chain of custody and the Rules of Evidence:

> [8] Before a physical object connected with the commission of a crime may properly be admitted into evidence, it must be satisfactorily identified and shown to be in substantially the same condition as when the crime was committed. *Brown v. General Motors Corp*., 67 Wn.2d 278, 285, 407 P.2d 461 (1965); *Gallego v. United States,* 276 F.2d 914, 917 (9th Cir.1960). Factors to be considered "include the nature of the article, the circumstances surrounding the preservation and custody of it, and the **likelihood of intermeddlers tampering with it**." *Gallego*, at 917. *State v. Campbell*, 691 P. 2d 929 - Wash: Supreme Court 1984 at ¶8. (Emphasis added).

Unmistakable proof of the "likelihood of intermeddlers"

As discussed above, Petitioner has shown by substantial evidence that a "likelihood of intermeddlers" exists in the current voting system in its inability to preserve an unbroken chain of bipartisan custody.

The current election practices are markedly out of synch with the statutes. The system is highly vulnerable to "intermeddlers" and therefore does not insure an unbroken bipartisan chain of custody. Remarkably, mail-in ballots are not counted by a bipartisan group in each county, external to "any machines", or verified in any non-machine statistical bi-partisan human observable manner, which should then hand deliver the vote tallies to the State tabulator in order to maintain an unbroken chain of custody.

CONCLUSION & REMEDIES

The voting process must enable an unbroken bipartisan chain of custody.

Therefore, the citizens of the State of Washington have no adequate remedy for the incurable uncertainty that exists currently in the current voting system. Therefore, Petitioner requests that the Secretary of State immediately:

(1) Stop all involvement by Microsoft, at least until their involvement can be assessed and certified as honest by a properly constituted bipartisan group;

(2) Verify the identity and qualification of each person who presents themselves to vote through a bipartisan group;

(3) Stop using electronic voting machines immediately;

(4) Establish bipartisan groups at each location where mail-in votes are counted. (How identities are confirmed is highly suspect with mail-in. Voters need to

physically show up to vote and have their thumbs inked unless they are unable to for legitimate reasons);

(5) Implement the process by which the bipartisan group vets each voter for his or her authority to vote;

(6) Enable each bipartisan group to count each verified ballot and prepare a tally sheet that will be certified by the bipartisan group;

(7) Enable the bipartisan group to photograph and post the certified tally sheet on the county‘s website immediately upon the certification;

(8) Provide the address and directions for the bipartisan group to drive to the state tabulator to report their tally sheet; and

(9) Enable the bipartisan group to be able to verify that their tally sheet results are faithfully entered into the State tabulator.

Respectfully submitted,

/S/ James M. Miller

James M Miller, Citizen Petitioner
1 Blue Sky Place
Omak, WA 98841
(425) 471-8101
jimomak@leader.com

August 28, 2018

VERIFICATION

I, James M. Miller, being of sound mind and body do hereby affirm that information in this writ is true and accurate to the best of my knowledge and ability, including my attestations as a process control expert. *See* **Exhibit L**.

/S/ James M. Miller

_____

James M. Miller

/S/ Notary Signature & Stamp on File

SWORN AND SUBSCRIBED before me, a Notary Public, this ____ day of _____, 2018.

VERIFICATION

I, James M. Miller, being of sound mind and body do hereby affirm that information in this writ is true and accurate to the best of my knowledge and ability, including my attestations as a process control expert.

James M. Miller

James M. Miller

SWORN AND SUBSCRIBED before me, a Notary Public, this 6 day of August, 2018.

Gay L. Heindselman
8/6/2018

SUPERIOR COURT
OKANOGAN COUNTY

CERTIFICATE OF SERVICE

I, James M. Miller, hereby certify that on August 28, 2018 a true and accurate copy of the foregoing WRIT OF MANDAMUS was served upon the Washington Secretary of State's designated service officer Brenda Galarza, Records/Public Disclosure Officer, Office of the Secretary of State Kim Wyman, 801 Capital Way South, Olympia, Washington 98501, (360) 704-5220, brenda.galarza@sos.wa.gov.

/S/ James M. Miller

James M Miller, Citizen Petitioner
1 Blue Sky Place
Omak, WA 98841
(425) 471-8101
jimomak@leader.com

August 28, 2018

Respondent Representatives:

WASHINGTON SECRETARY OF STATE

Brenda Galarza
Records/Public Disclosure Officer
Service Designee
Kim Wyman, Secretary of State
Legislative Building
416 Sid Snyder Ave. SW
Olympia, WA 98504
(360) 704-5220
brenda.galarza@sos.wa.gov

Callie A. Castillo, Bar No. 38214
Service Designee
Robert W. Ferguson, Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100
(360) 664-0869

Exhibit A

Laurie Thomas. (Jun. 8, 2018). James Miller signed response 6-8-18001.
Okanogan County Auditor.

Okanogan County Auditor

Laurie Thomas, Auditor *Mila Jury, Chief Deputy Auditor*
PO Box 1010
Okanogan WA 98840
509-422-7240

June 7, 2018

James M. Miller
1 Blue Sky Pl
Omak, WA 98841

Dear Mr. Miller,

As I understand it your request was for the entire "election process manual". To fulfill this request I am attaching the "desk reference" instructions compiled and utilized by Okanogan County staff.

A few "screen shots" have been redacted from the instructions due to the inclusion of security passwords, passcodes and other security sensitive information exempt from disclosure under RCW 42.56.420(4).

We are also withholding proprietary information, including specific instruction manuals for HART and VOTEC at the instruction of the vendors we contract with because their documents are exempt from disclosure under the Public Records Act. RCW 42.56.270.
If you should disagree about the applicability of the "financial, commercial, and proprietary information" exemption, then the companies that created the records can set the matter for a court hearing and ask for a declaration from the court that the exemption applies, and an injunction preventing disclosure.

Please consider this response for records as defined in RCW 42.56.010(3) timely pursuant to the requirements of RCW 42.56. I believe this fulfills your request and will consider this matter closed. If you object to any withholding of records you must follow the administrative procedures described in Okanogan County Code 2.88.070 before seeking judicial review. Feel free to contact this office if you require further assistance in this matter.

Cordially,

Laurie Thomas

Laurie Thomas, Auditor

Exhibit B

Brenda Galarza. (Jun. 29, 2018). PDR #18H-165 Public Records request for electronic voting procedures. Office of the WA Secretary of State, Elections Division.

RE: RE: PDR #18H-165 Public Records request for electronic votingprocedures

From: Holmes, Stuart <stuart.holmes@sos.wa.gov>
Sent: Fri, Jun 29, 2018 at 3:14 pm
To: Jim Miller, Galarza, Brenda
Cc: Condotta, Rep. Cary, mike.steele@leg.wa.gov, brad.hawkins@leg.wa.gov, Kretz Joel

image001.png (30.2 KB) image002.jpg (5.3 KB) image003.jpg (7.9 KB) image004.png (10.3 KB) image005.png (10.3 KB) – **Download all**

Jim,

Happy to answer your questions. Additionally, in the State of Washington a paper ballot is required by law. Each and every voter's ballot has a voter-

1. Please provide the list of vendors of voting machines used in the state election process for each county?
   a. A list of voting equipment used by each county is available on our website here: https://www.sos.wa.gov/elections/research/voting

2. Specifically name the 3rd party testers and how they are certified, and how they maintain unbroken bipartisan chain of custody if bipartisar in person and then creating a report based on 'empirical observable phenomena? this question was not answered.
   a. According to the Election Assistance Commission (EAC) website, SLI Compliance, a Division of Gaming Laboratories International, LL
   b. For more information about how they become accredited please refer to the EAC's website: https://www.eac.gov/voting-equipmen
   c. Additionally, you can review all the testing documentation on the EAC's website here: https://www.eac.gov/voting-equipment/syste

4. Please provide the public record that states that multi-partisan chain of custody of ballots and tally totals is maintained, and is 'never secret then, by the Grace of God.
   a. As I mentioned before, it is required that counties use numbered seals and logs, or other security measures which will detect any in materials and must be accompanied by at least two county auditor staff at all times. (WAC 434-261-045, WAC 434-250-110 & RCW 2 retention schedule. (https://www.sos.wa.gov/_assets/archives/county-auditor-rrs-ver-5.0.pdf). The Secretary of State's Office doesn custody' documents. However, you could certain view or get more information about those documents from each county auditor.
   b. Ballots are also maintained according to the retention schedule. (https://www.sos.wa.gov/_assets/archives/county-auditor-rrs-ver-5
   c. Audits are observable by the public and required to be conducted prior to the certification of each election. Logic and Accuracy test 29A.60.170, WAC 434-335-240 & RCW 29A.12.130).

Stuart Holmes| Voting Information Systems Manager
Office of the Secretary of State
(360) 725-5794 | www.vote.wa.gov

Office of the Secretary of State
Elections Division

From: Jim Miller [mailto:jimomak@leader.com]
Sent: Friday, June 29, 2018 2:39 PM
To: Holmes, Stuart <stuart.holmes@sos.wa.gov>; Galarza, Brenda <brenda.galarza@sos.wa.gov>
Cc: Condotta, Rep. Cary <cary.condotta@leg.wa.gov>; mike.steele@leg.wa.gov; brad.hawkins@leg.wa.gov; Kretz Joel <kretzranch@gmail.com>
Subject: RE: RE: PDR #18H-165 Public Records request for electronic voting procedures

Public Records Request of the following:
1. Please provide the list of vendors of voting machines used in the state election process for each county?

2. Specifically name the 3rd party testers and how they are certified, and how they maintain unbroken bipartisan chain of cus present to witness such testing in person and then creating a report based on 'empirical observable phenomena? this questi

4. Please provide the public record that states that multi-partisan chain of custody of ballots and tally totals is maintained, an will go away, and not until then, by the Grace of God.

I cannot accept that multi-partisan chain of custody can be maintained in 'any computer system'. Citizens 'cannot' observe s chain of custody is not maintained, and by law...the election process is by logic invalid. We simply MUST perform elections w custody. Ballot tallies must 'never' go to 'silicon' because they are then 'hidden and secret'.

APX 162

-----Original Message-----
From: "Holmes, Stuart" <stuart.holmes@sos.wa.gov>
Sent: Friday, June 29, 2018 9:47am
To: "Jim Miller" <jimomak@leader.com>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

Jim,

First, thank you for reaching out to our office with you questions. I just want to make it clear that not Smartmatic voting system or equipment is not

1. specifically name the 3rd party tester (and the actually testers themselves) and how that company and those people are certified by a bipar
    a. Independent testing authorities (or commonly known as Voting System Testing Laboratories (VSTL)) are designated by the United St
2. When the memory stick is delivered to the county auditor by the vendor what 'proof exists', other than a 'certification piece of paper' that t
    a. County Auditors are required to do acceptance testing of their voting system prior to use as well as Logic and Accuracy Testing of th system, including hardware and software, is the certified voting system. Each voting system can produce a hash value that would cor Laboratory. This hash value would show that the software in use has not been changed. (WAC 434-335-240 & RCW 29A.12.130). Log observers.
3. Is the 'memory stick, on which the tally at each county is entered and sent to the state, tested against an encrypted part number sent to the such as certified mail to ensure that the proper 'memory stick' has been delivered to the auditor by comparison(a phone call recorded)?
    a. If the 'memory stick' is part of the voting system, then yes that can be done. However, not all voting systems have 'memory sticks' a method they'd like to transfer election results from the tabulation system. For example, some counties use one-write media like CDs formatted prior to use. In either case, they are secured before and after the election.
4. What programs exist on the memory stick?
    a. None. They are only used to transfer files in some counties depending on the voting system and procedures in place for that county
5. What circuits exist on the memory stick, and what circuits are 'blue printed' as the baseline as the 'official circuits', and how is this tested ar
    a. This would be county specific based on the 'memory sticks' in use for the voting system and procedures in place for that county.
6. Are the 'memory sticks' impounded after the election, and are they available for inspection after the election and for how long, or is the evi
    a. This is county specific depending on the voting system and procedures in place for that county because not all counties use the sam related to the election have a retention and must be retained for their entire retention period. (https://www.sos.wa.gov/_assets/arc
7. Is there a 'micro-voltage' activation 'count' embedded in the memory stick's program, so that when it is received at the county auditor's site been reprogrammed during 'transport', by a 'man in the middle'? (this would make the whole voting procedure a magic act as it exists)
    a. Election Results are verified using a paper copy of the results. When results are transported from the tabulation equipment to be u the results are appearing accurately. Additionally, that same paper copy is provided to the state to ensure that after the results were several methods and opportunities, as stated in our previous response, for auditing during the election canvassing to ensure the tab
8. Is each county auditor required to create a 'bipartisan human hand tally' as well as a PCOS/Smartmatic machine tally to audit each 'tally cou unbroken bipartisan chain of custody tallies?
    a. Smartmatic voting systems are not certified or used in the State of Washington.

Stuart Holmes| Voting Information Systems Manager
Office of the Secretary of State
(360) 725-5794 | www.vote.wa.gov

Office of the Secretary of State
Elections Division

From: Galarza, Brenda
Sent: Friday, June 29, 2018 9:39 AM
To: Jim Miller <jimomak@leader.com>
Cc: Holmes, Stuart <stuart.holmes@sos.wa.gov>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

Mr. Miller,

Washington State follows the Public Records Act RCW 42.56. FOIA is for federal records request. Your questions do not constitute a records request Stuart Holmes. He will respond to your additional questions.

Regards,

APX 163

Brenda Galarza
Records/Public Disclosure Officer
360-704-5220
SOS
Office of the Secretary of State

From: Jim Miller [mailto:jimomak@leader.com]
Sent: Friday, June 29, 2018 9:15 AM
To: Galarza, Brenda <brenda.galarza@sos.wa.gov>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

I do have additional questions, as I have not received satisfactory or conclusive evidence that bipartisan chain of custody is p electronic devices of any kind in WA state's voting process. It is the 'people's' responsibility to ensure unbroken bipartisan ch under the Federal and the WA state constitution to know that this is true. We are not stating that there is 'voter fraud', we are is in reality--not broken beyond a 'shadow of doubt'. Any action taken, whereby the 'tally' or 'counts' of any voting procedure a when it is performed and transmitted by 'electrons' in a 'digital form' fails the test of 'unbroken bipartisan chain of custody obs bipartisan chain of custody be subject to 'FAITH' , 'law', 'vendor certification', testing' or any process' that is 'hidden from emp 'certification', it by logic, and physical law fails the test. The will of the people cannot be subject 'FAITH' from government, the without failure. Electronic devices depend upon 'failure modes' or 'statistical outcomes' that depend upon 'software programs which are 'hidden from observation, and thus fail the test by default of logic of 'unbroken bipartisan chain of custody'. Thus, t the test for certification. It is open to 'man in the middle attacks', and corruption. As such, the 'will of the people' can be circur through electronic means. This is the underlying logic of my FOIA requests.

FOIA request question:
1. specifically name the 3rd party tester (and the actually testers themselves) and how that company and those people are c WA?
2. When the memory stick is delivered to the county auditor by the vendor what 'proof exists', other than a 'certification piece delivered?
3. Is the 'memory stick, on which the tally at each county is entered and sent to the state, tested against an encrypted part n communication channel such as certified mail to ensure that the proper 'memory stick' has been delivered to the auditor by c
4. What programs exist on the memory stick?
5. What circuits exist on the memory stick, and what circuits are 'blue printed' as the baseline as the 'official circuits', and how
6. Are the 'memory sticks' impounded after the election, and are they available for inspection after the election and for how lo
7. Is there a 'micro-voltage' activation 'count' embedded in the memory stick's program, so that when it is received at the cou to attest that it has not been reprogrammed during 'transport', by a 'man in the middle'? (this would make the whole voting pr
8. Is each county auditor required to create a 'bipartisan human hand tally' as well as a PCOS/Smartmatic machine tally to a preserving both tally counts as unbroken bipartisan chain of custody tallies?

Please provide the public records for these questions as a continuance of the original FOIA request as noted by your statem

----Original Message----
From: "Galarza, Brenda" <brenda.galarza@sos.wa.gov>
Sent: Thursday, June 28, 2018 11:16am
To: "jimomak@leader.com" <jimomak@leader.com>
Subject: RE: RE: PDR #18H-165 FOIA request for electronic voting procedures

Mr. Miller,

Below is information provided by our Elections Division.

1. How do you ensure bi-partisan 'chain of custody' on any electronic device that sits between the voter and the 'county/city/special district' for loca election' for federal positions?

To answer your question, I'm interpreting "electronic device" as an in-person ballot marking system that retains an electronic voting record machine, and the county's voting system that tabulates returned ballots.

Before any voting system can be used in the State of Washington it first must be tested and certified by an independent testing authority de well as inspected and tested by the Secretary of State's Office (RCW 29A.12.080). During the Secretary of State's inspection of the voting syst (WAC 434-335-040) which include "Secures to the voter secrecy in the act of voting" and "Be capable of being secured with lock and seal wh

The Secretary of State's Office requires the use of secure storage which must employ the use of numbered seals and logs, or other security n access to the secured ballot materials and must be accompanied by at least two county auditor staff at all times. (WAC 434-261-045, WAC 4: used by every county document the chain of custody for who accessed the secured ballots which includes electronic voting devices that rete certification requirements of any voting system is that the voting device must produce a voter verifiable paper ballot.

Additionally, observers may be present during the processing of ballots because the entire process is open to the public.

2. How do you ensure that the 'electronic devices' are monitored by 'bipartisan' citizens, trained to monitor the ballot tally totals?

Prior to each election, the County Auditor must request observers be appointed by the major political parties to be present during the proce requested to appoint observers. The County Auditor can train observers with respect to ballot processing procedures and the vote tallying sy

3. do you ensure the bipartisan election monitors/judges can affirmatively verify that each vote is entered, reported, and tallied without interventio be empirically observable?

Prior to certification of the election the County Auditor must audit of results of votes cast on any direct recording electronic voting devices u counting equipment, and an audit of duplicated ballots.

In 2019, Risk Limiting Audits will become an option for counties to use to audit their voting equipment. Rules for conducting a Risk Limiting A Audits provide statistical evidence and confidence that the count was accurate while keeping the resources needed by the county to as little

4. I request the 'public records' that prove the above questions regarding the usage of all 'electronic devices' used in the voting process...all stages w of the voting procedure that results in a 'summation', 'addition', 'subtraction', 'tally', 'vote count' as an 'official' record of the voting process.

If you're interested in the chain of custody logs, observer procedures, audit procedures, or specific documents about the use of the voting sy Auditor because the Secretary of State's Office does not process any ballots, conduct tabulation, or operate a voting system.

If you're interested in the Election Assistance Commission testing and certification of the voting systems, those test reports and certification: equipment/system-certification-process-s/

We also have information about the system in use in Washington on our website here: https://www.sos.wa.gov/elections/research/voting-s

I trust you will find this information useful. If you have any further questions, please let me know. Otherwise, I am closing this request today.

Regards,

Brenda Galarza
Records/Public Disclosure Officer
PO Box 40224 | Olympia, WA 98504-0224
360-704-5220 Phone | 360-704-7830 Fax
brenda.galarza@sos.wa.gov

From: Jim Miller [mailto:jlmomak@leader.com]
Sent: Friday, June 22, 2018 10:46 AM
To: Galarza, Brenda <brenda.galarza@sos.wa.gov>
Cc: bhires@omakchronicle.com; Condotta, Rep. Cary <cary.condotta@leg.wa.gov>; mike.steele@leg.wa.gov; brad.hawkins@leg.wa.gov
Subject: FW: RE: PDR #18H-165 FOIA request for electronic voting procedures

Please consider this a FOIA request with the questions as stated:

1. How do you ensure bi-partisan 'chain of custody' on any electronic device that sits between the voter and the 'county/city/t state elections, and the 'federal election' for federal positions?

2. How do you ensure that the 'electronic devices' are monitored by 'bipartisan' citizens, trained to monitor the ballot tally tot

3. do you ensure the bipartisan election monitors/judges can affirmatively verify that each vote is entered, reported, and tallie whose operations do not appear to be empirically observable?

4. I request the 'public records' that prove the above questions regarding the usage of all 'electronic devices' used in the voti any manner by non-humans, as part of the voting procedure that results in a 'summation','addition', 'subtraction', 'tally', 'vote

-----Original Message-----
From: "Public Records, House" <House.PublicRecords@leg.wa.gov>
Sent: Friday, June 22, 2018 10:19am
To: "Jim Miller" <jimomak@leader.com>
Cc: "Public Records, Senate" <Senate.PublicRecords@leg.wa.gov>, "Condotta, Rep. Cary" <Cary.Condotta@leg.wa.gov>, "
"Hawkins, Sen. Brad" <Brad.Hawkins@leg.wa.gov>
Subject: RE: PDR #18H-165

Dear Mr. Miller:

I understand you are requesting "documentation of the processes utilized statewide at each county, including confidential sof utilized in the election process". If this is correct, then you will need to direct your request to the Public Records Officer for th

If you have any questions, please let me know.

Thank you,

Samina M. Mays
Public Records Officer
Washington State House of Representatives
360.786.7227 | Samina.Mays@leg.wa.gov

From: Jim Miller <jimomak@leader.com>
Sent: Thursday, June 21, 2018 4:28 PM
To: Public Records, House <House.PublicRecords@leg.wa.gov>
Cc: Public Records, Senate <Senate.PublicRecords@leg.wa.gov>; Condotta, Rep. Cary <Cary.Condotta@leg.wa.gov>; Steele, Rep. Mike <Mike.Steele@
Subject: RE: PDR #18H-165

What we have in play is a 'catch-22'. My FOIA request is for 'information' that exists as a public record, most likely as an 'elec designation', which makes it 'hidden and secret', and thus not a 'public record' by definition. So, by definition, what the voters not available, to the voters. What a perfect legal 'black box' behind which to hide.

Therefore, I must conclude, that the 'election process', in total, has 'no bipartisan chain of custody' which can be viewed by th 'certified' when chain of custody cannot be proven, and the Secretary of State, by law cannot 'certify' that which is 'secret anc

If we cannot view that which is hidden and secret, then we have no recourse but to serve to the state an injunction to stop th can be replace with an 'open and honest' election process from registration to tally count total, such that the 'will of the peopl election. What this means, is that, in the end, no electronic machines of any type can be utilized in the voting process.

This is a FOIA request, to provide the documentation of the processes utilized statewide at each county, including confidenti utilized in the election process.

-----Original Message-----
From: "Public Records, House" <House.PublicRecords@leg.wa.gov>

Sent: Thursday, June 21, 2018 10:35am
To: "jimomak@leader.com" <jimomak@leader.com>
Cc: "Public Records, Senate" <Senate.PublicRecords@leg.wa.gov>
Subject: PDR #18H-165

Dear Mr. Miller:

As the records custodian for the House of Representatives, the Office of the Chief Clerk has received your FOIA request for Representati have assigned your request tracking number 18H-165. Please put this number on all future correspondence regarding this request.

You requested the following information:
How do you ensure bi-partisan 'chain of custody' on any electronic device that sits between the voter and the 'county/city/special district the 'federal election' for federal positions?
How do you ensure that the 'electronic devices' are monitored by 'bipartisan' citizens, trained to monitor the ballot tally totals?
How do you ensure the bipartisan election monitors/judges can affirmatively verify that each vote is entered, reported, and tallied withou do not appear to be empirically observable?

It appears that your request is for information only and not for an "identifiable record" under the Public Records Act (RCW 42.56.080, ar so I can help identify which records you wish to obtain. I will now consider this request closed. Please contact me if you have any questic

Thank you,

Samina M. Mays
Public Records Officer
Washington State House of Representatives
360.786.7227 | Samina.Mays@leg.wa.gov

Please note: A specific definition of "public records" applies to the Legislature under the Public Records Act. RCW 42.56.010 and RCW

Your email security and privacy matter.

Your email security and privacy matter.

Your email security and privacy matter.

Your email security and privacy matter.

Exhibit C

Ron Wyden et al. (Jun. 12, 2018). Proposed Amendment to the Help America Vote Act of 2002. 115th Congress, 2d Session. U.S. Senate.

115TH CONGRESS
2D SESSION

S. _____

To amend the Help America Vote Act of 2002 to require paper ballots and risk limiting audits in all Federal elections, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN (for himself, Mrs. GILLIBRAND, Ms. WARREN, Mrs. MURRAY, Mr. MARKEY, and Mr. MERKLEY) introduced the following bill; which was read twice and referred to the Committee on

---

A BILL

To amend the Help America Vote Act of 2002 to require paper ballots and risk limiting audits in all Federal elections, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Protecting American Votes and Elections Act of 2018".

SEC. 2. FINDINGS.

Congress makes the following findings:

(1) Access to the ballot, free and fair elections, and a trustworthy election process are at the core of

American Democracy. Just as the Founding Fathers signed their names to paper supporting their views for a government by and for the people, access to the paper ballot is the best way to ensure elections stay by and for the American people. Using paper provides an easily auditable, tamper proof, and simple way for citizens to access their ballot. It is for these reasons and more that using paper ballots to ensure resilient and fair elections should be the priority of this Nation.

(2) Risk-limiting audits will help to protect our elections from cyberattacks, by ensuring that if the electoral outcome is incorrect, for instance because someone tampered with the electronic counts or reporting, the audit has a large, known probability of correcting the outcome by requiring a full hand count. Paper ballots are vital to the audit process since, other than through manual inspection of a sample of paper ballots, there is currently no reliable way to determine whether an election was hacked or the outcome was miscalculated.

(3) Risk-limiting audits are a cost effective way of auditing election results. They generally require inspecting only a small percentage of the ballots cast in an election, and proceed to a full hand count only

when sampling does not provide strong evidence that the reported outcome is correct. This will ensure that Americans have confidence in their election results, without the cost of a full recount of every ballot in the country.

SEC. 3. PAPER BALLOT AND MANUAL COUNTING REQUIREMENTS.

(a) IN GENERAL.—Section 301(a)(2) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(2)) is amended to read as follows:

"(2) PAPER BALLOT REQUIREMENT.—

"(A) VOTER-VERIFIED PAPER BALLOTS.—

"(i) PAPER BALLOT REQUIREMENT.—

(I) The voting system shall require the use of an individual, durable, voter-verified, paper ballot of the voter's vote that shall be marked and made available for inspection and verification by the voter before the voter's vote is cast and counted, and which shall be counted by hand or read by an optical character recognition device or other counting device. For purposes of this subclause, the term 'individual, durable, voter-verified, paper ballot' means a paper ballot marked by the voter by hand or a

paper ballot marked through the use of a nontabulating ballot marking device or system, so long as the voter shall have the option to mark his or her ballot by hand.

"(II) The voting system shall provide the voter with an opportunity to correct any error on the paper ballot before the permanent voter-verified paper ballot is preserved in accordance with clause (ii).

"(III) The voting system shall not preserve the voter-verified paper ballots in any manner that makes it possible, at any time after the ballot has been cast, to associate a voter with the record of the voter's vote without the voter's consent.

"(ii) PRESERVATION AS OFFICIAL RECORD.—The individual, durable, voter-verified, paper ballot used in accordance with clause (i) shall constitute the official ballot and shall be preserved and used as the official ballot for purposes of any recount or audit conducted with respect to any election for Federal office in which the voting system is used.

"(iii) MANUAL COUNTING REQUIREMENTS FOR RECOUNTS AND AUDITS.—(I) Each paper ballot used pursuant to clause (i) shall be suitable for a manual audit, and shall be counted by hand in any recount or audit conducted with respect to any election for Federal office.

"(II) In the event of any inconsistencies or irregularities between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified, paper ballots used pursuant to clause (i), and subject to subparagraph (B), the individual, durable, voter-verified, paper ballots shall be the true and correct record of the votes cast.

"(iv) APPLICATION TO ALL BALLOTS.—The requirements of this subparagraph shall apply to all ballots cast in elections for Federal office, including ballots cast by absent uniformed services voters and overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act and other absentee voters.

"(B) SPECIAL RULE FOR TREATMENT OF DISPUTES WHEN PAPER BALLOTS HAVE BEEN SHOWN TO BE COMPROMISED.—

"(i) IN GENERAL.—In the event that—

"(I) there is any inconsistency between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified, paper ballots used pursuant to subparagraph (A)(i) with respect to any election for Federal office; and

"(II) it is demonstrated by clear and convincing evidence (as determined in accordance with the applicable standards in the jurisdiction involved) in any recount, audit, or contest of the result of the election that the paper ballots have been compromised (by damage or mischief or otherwise) and that a sufficient number of the ballots have been so compromised that the result of the election could be changed,

the determination of the appropriate remedy with respect to the election shall be made in accordance with applicable State law, except that the electronic tally shall not be used as the exclusive basis for determining the official certified result.

"(ii) RULE FOR CONSIDERATION OF BALLOTS ASSOCIATED WITH EACH VOTING MACHINE.—For purposes of clause (i), only the paper ballots deemed compromised, if any, shall be considered in the calculation of whether or not the result of the election could be changed due to the compromised paper ballots.".

(b) CONFORMING AMENDMENT CLARIFYING APPLICABILITY OF ALTERNATIVE LANGUAGE ACCESSIBILITY.—Section 301(a)(4) of such Act (52 U.S.C. 21081(a)(4)) is amended by inserting "(including the paper ballots required to be used under paragraph (2))" after "voting system".

(c) OTHER CONFORMING AMENDMENTS.—Section 301(a)(1) of such Act (52 U.S.C. 21081(a)(1)) is amended—

(1) in subparagraph (A)(i), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)";

(2) in subparagraph (A)(ii), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)";

(3) in subparagraph (A)(iii), by striking "counted" each place it appears and inserting "counted, in accordance with paragraphs (2) and (3)"; and

(4) in subparagraph (B)(ii), by striking "counted" and inserting "counted, in accordance with paragraphs (2) and (3)".

(d) EFFECTIVE DATE.—Notwithstanding section 301(d) of the Help America Vote Act of 2002 (52 U.S.C. 21081(d)), each State and jurisdiction shall be required to comply with the amendments made by this section for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.

SEC. 4. ACCESSIBILITY AND BALLOT VERIFICATION FOR INDIVIDUALS WITH DISABILITIES.

(a) IN GENERAL.—Section 301(a)(3)(B) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(3)(B)) is amended to read as follows:

"(B)(i) satisfy the requirement of subparagraph (A) through the use of at least 1 voting system equipped for individuals with disabilities, including nonvisual and enhanced visual accessibility for the blind and visually impaired, and nonmanual and enhanced manual accessibility for the mobility and dexterity impaired, at each polling place; and

"(ii) meet the requirements of subparagraph (A) and paragraph (2)(A) by using a system that—

"(I) allows the voter to privately and independently verify the permanent paper ballot through the presentation, in accessible form, of the printed or marked vote selections from the same printed or marked information that would be used for any vote counting or auditing; and

"(II) allows the voter to privately and independently verify and cast the permanent paper ballot without requiring the voter to manually handle the paper ballot; and".

(b) SPECIFIC REQUIREMENT OF STUDY, TESTING, AND DEVELOPMENT OF ACCESSIBLE PAPER BALLOT VERIFICATION MECHANISMS.—

(1) STUDY AND REPORTING.—Subtitle C of title II of such Act (52 U.S.C. 21081 et seq.) is amended by inserting after section 246 the following new section:

"SEC. 246A. STUDY AND REPORT ON ACCESSIBLE PAPER BALLOT VERIFICATION MECHANISMS.

"(a) STUDY AND REPORT.—The Director of the National Science Foundation shall make grants to not fewer than 3 eligible entities to study, test, and develop accessible paper ballot voting, verification, and casting mechanisms and devices and best practices to enhance the accessibility of paper ballot voting and verification mechanisms for individuals with disabilities, for voters whose primary language is not English, and for voters with difficulties in literacy, including best practices for the mechanisms themselves and the processes through which the mechanisms are used.

"(b) ELIGIBILITY.—An entity is eligible to receive a grant under this part if it submits to the Director (at such time and in such form as the Director may require) an application containing—

"(1) certifications that the entity shall specifically investigate enhanced methods or devices, including non-electronic devices, that will assist such individuals and voters in marking voter-verified paper ballots and presenting or transmitting the information printed or marked on such ballots back to such individuals and voters, and casting such ballots;

"(2) a certification that the entity shall complete the activities carried out with the grant not later than December 31, 2020; and

"(3) such other information and certifications as the Director may require.

"(c) AVAILABILITY OF TECHNOLOGY.—Any technology developed with the grants made under this section shall be treated as non-proprietary and shall be made available to the public, including to manufacturers of voting systems.

"(d) COORDINATION WITH GRANTS FOR TECHNOLOGY IMPROVEMENTS.—The Director shall carry out this section so that the activities carried out with the grants made under subsection (a) are coordinated with the research conducted under the grant program carried out by the Commission under section 271, to the extent that the Director and Commission determine necessary to provide for the advancement of accessible voting technology.

"(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out subsection (a) $10,000,000, to remain available until expended.".

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended by inserting after the item relating to section 246 the following new item:

"Sec. 246A. Study and report on accessible paper ballot verification mechanisms.".

SEC. 5. RISK-LIMITING AUDITS.

(a) IN GENERAL.—Title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.) is amended by inserting after section 303 the following new section:

"SEC. 303A. RISK-LIMITING AUDITS.

"(a) DEFINITIONS.—In this section:

"(1) RISK-LIMITING AUDIT.—

"(A) IN GENERAL.—The term 'risk-limiting audit' means a post-election process such that, if the reported outcome of the contest is incorrect, there is at least a 95 percent chance that the audit will replace the incorrect outcome with the correct outcome as determined by a full, hand-to-eye tabulation of all votes validly cast in that election contest that ascertains voter intent manually and directly from voter-verifiable paper records.

"(B) REPORTED OUTCOME.—The term 'reported outcome' means the outcome of an election contest which is determined according to the canvass and which will become the official, certified outcome unless it is revised by an audit, recount, or other legal process.

"(C) INCORRECT OUTCOME.—The term 'incorrect outcome' means an outcome that differs from the outcome that would be determined by a full tabulation of all votes validly cast in that election contest, determining voter intent manually, directly from voter-verifiable paper records.

"(D) OUTCOME.—The term 'outcome' means the winner or set of winners of an election contest, which might be candidates or positions.

"(2) BALLOT MANIFEST.—The term 'ballot manifest' means a record maintained by each county that—

"(A) is created without reliance on any part of the voting system used to tabulate votes;

"(B) functions as a sampling frame for conducting a risk-limiting audit; and

"(C) contains the following information about ballots cast and counted:

"(i) The total number of ballots cast and counted in the election (including undervotes, overvotes, and other invalid votes).

"(ii) The total number of ballots cast in each contest in the election (including undervotes, overvotes, and other invalid votes).

"(iii) A precise description of the manner in which the ballots are physically stored, including the total number of physical groups of ballots, the numbering system for each group, a unique label for each group, and the number of ballots in each such group.

"(b) REQUIREMENT.—

"(1) IN GENERAL.—

"(A) AUDITS.—Each State and jurisdiction shall administer risk-limiting audits of the results of all elections for Federal office held in the State in accordance with the requirements of paragraph (2).

"(B) FULL MANUAL TALLY.—If a risk-limiting audit conducted under subparagraph (A) leads to a full manual tally of an election contest, the State or jurisdiction shall use the results of the full manual tally as the official results of the election contest.

"(2) AUDIT REQUIREMENTS.—

"(A) RULES AND PROCEDURES.—

"(i) IN GENERAL.—Risk-limiting audits shall be conducted in accordance with the rules and procedures established by the chief State election official of the State not later than 1 year after the date of the enactment of this section.

"(ii) MATTERS INCLUDED.—The rules and procedures established under clause (i) may include the following:

"(I) Rules for ensuring the security of ballots and documenting that prescribed procedures were followed.

"(II) Rules and procedures for ensuring the accuracy of ballot manifests produced by jurisdictions.

"(III) Rules and procedures for governing the format of ballot mani-

fests, cast vote records, and other data involved in risk-limiting audits.

"(IV) Methods to ensure that any cast vote records used in a risk-limiting audit are those used by the voting system to tally the election results sent to the Secretary of State and made public.

"(V) Procedures for the random selection of ballots to be inspected manually during each audit.

"(VI) Rules for the calculations and other methods to be used in the audit and to determine whether and when the audit of each contest is complete.

"(VII) Procedures and requirements for testing any software used to conduct risk-limiting audits.

"(B) TIMING.—The risk-limiting audit shall be completed not later than the date that the result of the election is certified by the State.

"(C) PUBLIC REPORT.—After the completion of the risk-limiting audit, the State shall

publish a report on the results of the audit, together with such information as necessary to confirm that the audit was conducted properly.

"(c) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this section for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.".

(b) CONFORMING AMENDMENTS RELATED TO ENFORCEMENT.—Section 401 of such Act (52 U.S.C. 21111) is amended by striking "and 303" and inserting "303, and 303A".

(c) CLERICAL AMENDMENT.—The table of contents for such Act is amended by inserting after the item relating to section 303 the following new item:

"Sec. 303A. Risk-limiting audits.".

Exhibit D

Jay Inslee. (Jul. 19, 2018). Letter to President Donald Trump. WA State Governor's Office.

July 19, 2018

President Donald. J. Trump
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Dear President Trump:

We write with complete and total dismay and alarm over your comments at the summit with Russian President Vladimir Putin and your failure to both recognize and denounce his attacks on American democracy. Never, in the course of our nation's history, has a president sided with a foreign adversary—one responsible for a coordinated attack on our free and open elections—over our own U.S. intelligence community.

We now know, unequivocally, that—on the order of President Putin—Russian officials attacked at least 21 state systems during the 2016 election, as part of a coordinated effort to influence our elections. Last week, FBI special counsel Robert Mueller indicted twelve Russian intelligence officers accused of interfering in the 2016 election. The U.S. intelligence community confirmed these facts in no uncertain terms. Your inconsistency in accepting those facts, and your inability to confront President Putin, poses a direct threat to our national security and to our freedoms.

Our election systems remain targets of foreign interference. On February 13, 2018, Director of National Intelligence Dan Coats, testifying before the Senate Intelligence Committee, said that "persistent and disruptive cyber operations" would continue "using elections as opportunities to undermine democracy" in the United States in 2018 and beyond. In that same hearing, he affirmed that he had already seen evidence Russia was targeting U.S. elections in November 2018.

As governors, we remain committed to protecting our states' election systems. There is nothing more fundamental to the enduring success of our American democracy, and we take seriously our responsibility to protect the integrity and security of our elections. Through the National Governors Association and public-private partnerships, we have led a number of bipartisan initiatives on cybersecurity to bolster the security of our election infrastructure. States are leading the way in protecting voters, but more has to be done to send a clear message: Interference in our elections will not be tolerated.

We cannot take a passive stance while a hostile foreign government continues to undermine our democracy. And we certainly cannot defend or actively condone Russia's actions, which is what you are choosing to do. Ignoring the real threats Russia poses to our elections is, quite frankly, un-American. This is an imminent national security threat that transcends party lines. This is a matter of protecting and preserving fair elections—the underpinning of our democracy.

As governors, we are committed to ensuring that every vote is protected and counted. Americans need a president who is willing to stand-up to a foreign adversary that continues to threaten our basic rights and freedom.

We call on you to stand with the American people and lead by denouncing the Russian government's assault on the fundamental and basic right of Americans to elect their leaders without interference. We call on you to enforce and strengthen sanctions against Russia and hold them accountable for their continued attacks. Lastly, we call on you to support strong congressional action to help states secure our elections and protect our democracy from Russian cyberattacks. The American people deserve better.

Sincerely,

Jay Inslee
Governor
State of Washington

Andrew Cuomo
Governor
State of New York

Exhibit E

Kim Wyman. (Accessed Aug. 03, 2018). Election Machine Inventory, SOS website. Washington, Secretary of State.

Voting Systems by County					
County	System	Type of AVU*	Vendor	Software	Accessible Voting Unit
Adams	Optical Scan	Touchscreen	Election Systems and Software	EVS	AutoMark
Asotin	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Benton	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Chelan	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Clallam	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Clark	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Columbia	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Cowlitz	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Douglas	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Ferry	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Franklin	Digital Scan	Touchscreen	Dominion Voting Systems	Democracy Suite	AVC Edge
Garfield	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Grant	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Grays Harbor	Digital Scan	Touchsceen	ClearBallot	ClearVote	ClearAccess
Island	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Jefferson	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
King	Digital Scan	Touchscreen	ClearBallot	ClearVote	ClearAccess
Kitsap	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Kittitas	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Klickitat	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Lewis	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Lincoln	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Mason	Digital Scan	Dial	ClearBallot	ClearVote	ClearAccess
Okanogan	Digital Scan	Dial	Hart InterCivic	HVS	eSlate

Pacific	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Pend Oreille	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Pierce	Digital Scan	Touchscreen	ClearBallot	ClearVote	ClearAccess
San Juan	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Skagit	Digital Scan	Touchscreen	Hart InterCivic	Verity	Touch Writer
Skamania	Digital Scan	Touchscreen	ClearVote	ClearVote	ClearAccess
Snohomish	Digital Scan	Touchscreen	ClearVote	ClearVote	ClearAccess
Spokane	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Stevens	Digital Scan	Dial	Hart InterCivic	HVS	eSlate
Thurston	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Wahkiakum	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Walla Walla	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Whatcom	Digital Scan	Touchscreen	ClearBallot	ClearVote	ClearAccess
Whitman	Optical Scan	Touchscreen	Election Systems and Software	Unity	AutoMark
Yakima	Digital Scan	Dial	Hart InterCivic	HVS	eSlate

Exhibit F

Angela Gunn. (Nov. 01, 2006). Who's building the gear that's running the show? *Computerworld*.

E-voting and voter registration: The vendors

Who's building the gear that's running the show?

By Angela Gunn

Computerworld | NOV 1, 2006 12:00 AM PT

The biggest vendors of e-voting machinery are also among the largest vendors of voter-registration technology. Roughly speaking, there are four significant players in the e-voting market and three in the voter-registration arena. We follow our overview of those seven companies with capsule descriptions of other companies whose technology voters may encounter around the country.

E-VOTING VENDORS: THE MAJORS

Diebold Inc.

Not the largest e-voting vendor but certainly the most controversial, **Diebold** has repeatedly raised hackles with its aggressive responses to computer-security professionals who have demonstrated problems with the company's hardware and software. That's leaving out entirely the ill-advised 2003 promise by Diebold CEO and Republican fund-raiser Walden O'Dell to "[help] Ohio deliver its electoral votes to the president." (O'Dell left Diebold in 2005 amid rumors of securities-fraud litigation and insider trading.)

The company produces the AccuVote line of direct recording electronics (DRE), DRE/VVPAT (voter-verified paper audit trail) and optical scan machines. Diebold machines have figured in two high-profile tests that discovered multiple hardware and software vulnerabilities, and they compare poorly with contemporary Sequoia Voting Systems Inc. units in independent tests undertaken in Alameda, Calif.

As of October, various machines from North Canton, Ohio-based Diebold were certified for use in Alaska, Arizona, California, Colorado, Connecticut, Florida, Georgia, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Mississippi, Missouri, New Hampshire, Ohio, Pennsylvania, Tennessee, Texas, Utah, Vermont, Virginia, Washington, Wisconsin and Wyoming. Massachusetts will evaluate several Diebold machines in the commonwealth's November elections.

Diebold is also involved with voter-registration database systems, having purchased Costa Mesa, Calif.-based Data Information Management Systems in 2003. The company has been criticized for its involvement in this summer's voter-registration controversy in Alabama.

Election Systems & Software Inc.
The world's largest elections company, responsible for half of the e-voting machines in the U.S. ES&S was known as American Information Systems until 1997, when the company merged with Business Records Corp. (BRC). Until 1996, its chairman was Chuck Hagel, who quit to run for and win a U.S. Senate seat for Nebraska. Omaha-based ES&S makes a variety of machines, including DRE, DRE/VVPAT and optical-scan versions. It also offers voter-registration database development services. The company produces the iVotronic line of DRE and DRE/VVPAT machines as well as optical scan units. (As part of its purchase of BRC, ES&S ended up with service responsibility for BRC's Optech optical scan machines; for antitrust-related reasons, however, new Optechs come from Sequoia.)

As of October, various machines from **ES&S** were certified for use in Alabama, Arizona, Arkansas, California, Colorado, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Virginia, Washington, West Virginia, Wisconsin and Wyoming. Massachusetts will evaluate several of the company's machines in its November elections.

Hart InterCivic Inc.
Hart InterCivic's Web site nods at the continuing controversy over e-voting technology, promising to "guarantee the best election you've never heard of." (Presumably, that was written before the name-truncation bugs spotted in Virginia and Texas late in the election cycle.) Hart's eSlate machines, unlike most of the competition's units, function essentially as dumb terminals. The user interface is distinguished by the Select Wheel positioning device, which eliminates the use of touch screens. eSlates are available in DRE and DRE/VVPATmodels.

As of October, various machines from Austin-based Hart InterCivic were certified for use in California, Colorado, Hawaii, Illinois, Kentucky, Pennsylvania, Tennessee, Texas, Virginia and Washington. Massachusetts will evaluate several Hart machines in its November elections. Hart is also involved with voter-registration database systems in conjunction with IBM.

Sequoia Voting Systems Inc.
By late October, Oakland, Calif.-based **Sequoia Voting Systems** was once again fending off rumors that the company has connections to the **Venezuelan government**. According to information on the company's Web site, Sequoia's parent company, Smartmatic Corp., is privately owned, with a controlling interest held by founder and CEO Antonio Mugica. Mugica holds dual Spanish and Venezuelan citizenship. Sequoia offers AVC Edge and AVC Advantage DRE units, an AVC Edge DRE/VVPAT unit, and sells a Sequoia-branded Optech Insight optical scanner. (Election Systems & Software also offers an Optech line for reasons explained in the ES&S section.) Also in October, Sequoia figured at the center of tests on Alameda County, Calif., e-voting machines; results (**download PDF**) were generally positive compared with those for a contemporary Diebold unit, though the need for stronger network security and better

handling procedures was emphasized.

As of October, various machines from Sequoia were certified for use in Arizona, California, Colorado, the District of Columbia, Florida, Illinois, Louisiana, Missouri, Nevada, New Jersey, New Mexico, Pennsylvania, Virginia, Washington and Wisconsin.

VOTER REGISTRATION: THE MAJORS

Accenture Ltd.

Florida used information from Bermuda-based Accenture that led to the state's disastrous 2004 registration purge. Until 1989, it was the consulting division of former accounting firm Arthur Anderson, **Accenture** changed its name during a final split from that firm in 2001. Since then, Accenture has gained and lost statewide voter-registration system (SVRS) contracts in Colorado, Kansas and Wyoming -- in the final case, the company was forced to refund the state's money in full. Accenture is working on databases for Pennsylvania and Wisconsin. Both projects have been widely criticized, and Pennsylvania's is late. (Votingindustry.com has an **interesting overview** of Accenture's long history with e-voting technologies.)

Covansys Corp./Saber Corp.

Portland, Ore.-based **Saber** first built the Oregon registration database, then expanded to Mississippi, Montana, Maryland and Iowa. The latter states contracted with Maximus Inc. to deliver the technology for Missouri's database as well. The company acquired **Covansys**' SVRS projects when it purchased that branch of the Farmington Hills, Mich.-based company in February, though the development teams and products remain separate.

PCC Technology Group LLC

The Bloomfield, Conn.-based company that delivered the voter-registration system for Connecticut, Rhode Island and West Virginia, **PCC** has often partnered with Covansys, now part of Saber.

OTHER PLAYERS

AccuPoll Holding Corp.

This Newport Beach, Calif.-based company declared bankruptcy in January. **AccuPoll**'s e-voting technology, which lets the voter make selections on a DRE touch screen and then printed a paper ballot, has been certified for use in Texas and Missouri.

Advanced Voting Solutions Inc.

Once upon a time, Frisco, Texas-based **AVS** was known as Shoup Voting Solutions, and it built lever machines. Company founder Howard Van Pelt's previous company, Global Election Systems, grew up to be Diebold. AVS e-voting machines are or have operated in Mississippi, Pennsylvania and Virginia.

Aradyme Corp.

Orem, Utah-based **Aradyme** is subcontracted to handle data conversion on many states' voter-registration projects.

Arran Technologies Inc.
Roseville, Minn.-based **Arran**'s consultants advised Minnesota on the development of its SVRS.

Avante
Avante's Vote-Trakker 1 was the first DRE/VVPAT machine available; the latest version, Vote-Trakker 2, records votes to paper (kept behind a plastic panel, but viewable for voters to confirm before finalizing their votes) as well as to both flash memory and a hard drive. Princeton, N.J.-based Avante's machines are or have been operated in New Jersey and New York.

Automatic Voting Machine Corp.
Now defunct, Jamestown, N.Y.-based AVM built the lever machines now being phased out in New York and already retired in Louisiana and other states. It was established in 1896.

Business Records Corp. (BRC)
See **ES&S**, above.

Catalyst Computing Group Inc.
This company provides registration-database technology. Chicago-based **Catalyst** is contracted with Illinois to deliver a final version of its Help America Vote Act-compliant Illinois Voter Registration System in 2007.

Guardian Voting Systems
This is Danaher Corp.'s e-voting machines unit. States in which Gurnee, Ill.-based **Guardian Voting Systems**' machines are or have been certified are Arkansas, Delaware, Kentucky, New Mexico and Pennsylvania.

DFM Associates
As of September, Irvine, Calif.-based **DFM**'s election management software has been certified for use in California.

IVS LLC
Inspire Vote-By-Phone's e-voting technology was in wide deployment for the first time this year. Voters dial in via touch-tone phone to a computer system at a central location, monitored by election officials. The phones are situated at polling places, and a poll worker must key in his worker ID and a ballot-access ID, then hand the phone over to the voter. Louisville, Ky.-based **IVS** is certified for use in Connecticut, Maine, New Hampshire, Oklahoma, Oregon and Vermont.

MicroVote General Corp.
As of September, DRE machines from Indianapolis-based **MicroVote** were certified for use in Indiana, Kentucky and Tennessee.

Populex Corp.
This company offers e-voting technology that uses a stylus/touch-screen input to print a

bar-coded ballot card that's then scanned to record the voter's choices. As of September, Elgin, Ill.-based **Populex**'s voting technology was certified for use in Illinois and Missouri.

Quest Informations Systems Inc.
Quest sells registration-database technology. Indianapolis-based **Quest IS** developed Indiana's voter-registration database and is contracted to do the same in Virginia via an arrangement with Unisys Corp.

Saber Consulting Inc./Saber Corp.
See the registration database technology of Covansys/Saber above.

UniLect Corp.
As of September, Dublin, Calif.-based **UniLect**'s e-voting technology was certified for use in Virginia.

Vote-PAD Inc .
The Voting-on-Paper Assistive Device is a paper-based voting system geared toward use by disabled voters. As of September, **Vote-PAD**'s technology was certified in Wisconsin.

Voting Technologies International
E-voting technology. As of September, Milwaukee-based **VTI**'s DRE machines were certified in Indiana, Kansas and Wisconsin.

For more information on voter registration systems and vendors, check out **Votingindustry.com**.

See more about e-voting:

- **E-voting state by state: What you need to know**
- **Laws, lingo and technologies**
- **Review: Hacking Democracy**

Exhibit G

Anonymous Patriots. (Jul. 06, 2018). Scrap Electronic Voting Machines NOW!
Americans for Innovation.

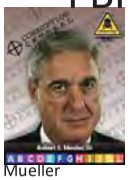
Scrap Corruption-ridden Electronic Voting – Now!

Finding: All prominent electronic voting systems in the U.S. (Smartmatic, Sequoia, Diebold, ES&S, Dominion and Hart InterCivic) are networked to the *same* software engine and controlled by the same financiers tied to George Soros and the Queen's Privy Council, thus making corrupt practices in U.S. elections a foregone conclusion. Lord Mark Malloch-Brown and Sir Geoffrey E. Pattie brag about their ability to "bend" elections , protected by the Queen.

Recommendation: In addition to the companies identified below, there are other companies trying to make voting secure with jpegs, separate validations, etc. on separate machines. However, no tech of any kind can maintain a "bipartisan chain of custody." The human eye cannot see silicon circuits, software induced voltages, and that which is hidden from empirical observation. We can only 'trust' the process and the people. Electronic voting offends the entire concept of our Republic -- which was formed on the concept that authority, being given from the "power of the people" who gain it directly from God, must be separated with jurisdictional boundaries so that the "tendency of men with too much authority to 'oppress'" can be muted by that separation. Centralizing the voting process so that the 'Fake News' can report a sensationalized and profitable result is pure idiocy. We the People should not trust government. We must insist at all times and under all circumstances that dual-Federalism is maintained. The job of the People is to ensure that the boundaries are maintained. We must all be mechanics of the Republic. The following voting machines must be scrapped immediately as the fruit of a poisoned tree called technocracy.

Chief Electronic Voting Scammers:

FBI / DOJ / C.I.A.


Mueller

Comey

Holder

State Dept / DNC / RNC

Clinton

Obama

Romney

Bush

Queen's Privy Council

Soros

Malloch-Brown

Pattie

SMARTMATIC

2000 Founded in Venezuela
2004 28% Caesar Chavez-owned; offices in London UK, Caracas VZ, Boca Raton FL, Sunnyvale CA
2005 Purchased Sequoia; acquired **OpTech**
2006 Sold Sequoia-Smartmatic (US) to Smartmatic (UK)
2012 Smartmatic (UK) operated R&D labs in US, Brazil, Venezuela, Barbados, Panama, UK, Netherlands, UAE, Phillipines, Estonia and Taiwan.
2014 SGO (**Lord Malloch-Brown**) acquired Smartmatic (UK)

SEQUOIA

1960 Mathematical Systems Corp; punch cards
1970 Diamond National Corp acquired Mathematical
1983 Sequoia Pacific; acquired Diamond
1984 Sequoia Voting Machines formed from Diamond, Automatic Voting Machine Corp, **OpTech** license from Smartmatic
1997 Licensed OpTech software from Smartmatic
2005 Sequoia purchased by Smartmatic (UK)
2010 **DOJ-triggered** sale of Smartmatic to US investors (**Mitt Romney, Bain Capital**, Booz Allen), renamed company Sequoia
2011 Sold to Dominion (Canada)
2011 Filed Chapter 11 bankruptcy in US

DIEBOLD / ES&S / DOMINION

1974 Klopp Printing, Urosevich Bros, created **OpTech**; ally with Westinghouse Corp to sell Data Mark Systems
1979 Urosevich Bros and Westinghouse start American Information Systems
1997 America Info acquired ESD; renamed to Election Systems & Software (ES&S); licensed OpTech to Diebold (later renamed Premier)
1998 ES&S acquired Votronic fully electronic voting (DRE)
2006 Diebold rebranded to Premier Election Systems
2009 ES&S acquired Premier
2010 Dominion Voting Systems acquired Premier (formerly Diebold) in a **DOJ-triggered** anti-trust divestiture

HART INTERCIVIC

2000 Hart InterCivic spun off from Hart Graphics to focus on election systems
2010 **Mitt Romney, Bain Capital**, Booz Allen purchased Smartmatic (US); acquires **OpTech** license from **DOJ-triggered** sale; renamed it Sequoia

LORD MALLOCH-BROWN

2010 Avid introduced **LeaderPlus** Election Night Newsroom management suite
2012 Investec Plc , Malloch-Brown invested in **ISIS Management Limited** (**Investec Plc**); Avid introduced **Avid Knowledge Base ISIS Management Console** - Agent Settings as complement to LeaderPlus; pushes Fake News scripts to MSM election news anchors in real time

Use freely. Anonymous Patriots. Rev. July 06, 2018

APX 199

Exhibit H

Phillip A. Brooks, (Sep. 18, 2015). Re. Notice of Violation, Volkswagen Software Hack To Modify Test Conditions Automatically. United States Environmental Protection Agency.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

SEP 18 2015

OFFICE OF
ENFORCEMENT AND
COMPLIANCE ASSURANCE

VIA CERTIFIED MAIL
RETURN RECEIPT REQUESTED

Volkswagen AG
Audi AG
Volkswagen Group of America, Inc.
Thru:

David Geanacopoulos
Executive Vice President Public Affairs and General Counsel
Volkswagen Group of America, Inc.
2200 Ferdinand Porsche Drive
Herndon, VA 20171

Stuart Johnson
General Manager
Engineering and Environmental Office
Volkswagen Group of America, Inc.
3800 Hamlin Road
Auburn Hills, MI 48326

Re: Notice of Violation

Dear Mr. Geanacopoulos and Mr. Johnson:

The United States Environmental Protection Agency (EPA) has investigated and continues to investigate Volkswagen AG, Audi AG, and Volkswagen Group of America (collectively, VW) for compliance with the Clean Air Act (CAA), 42 U.S.C. §§ 7401–7671q, and its implementing regulations. As detailed in this Notice of Violation (NOV), the EPA has determined that VW manufactured and installed defeat devices in certain model year 2009 through 2015 diesel light-duty vehicles equipped with 2.0 liter engines. These defeat devices bypass, defeat, or render inoperative elements of the vehicles' emission control system that exist to comply with CAA emission standards. Therefore, VW violated section 203(a)(3)(B) of the CAA, 42 U.S.C. § 7522(a)(3)(B). Additionally, the EPA has determined that, due to the existence of the defeat

devices in these vehicles, these vehicles do not conform in all material respects to the vehicle specifications described in the applications for the certificates of conformity that purportedly cover them. Therefore, VW also violated section 203(a)(1) of the CAA, 42 U.S.C. § 7522(a)(1), by selling, offering for sale, introducing into commerce, delivering for introduction into commerce, or importing these vehicles, or for causing any of the foregoing acts.

Law Governing Alleged Violations

This NOV arises under Part A of Title II of the CAA, 42 U.S.C. §§ 7521–7554, and the regulations promulgated thereunder. In creating the CAA, Congress found, in part, that "the increasing use of motor vehicles . . . has resulted in mounting dangers to the public health and welfare." CAA § 101(a)(2), 42 U.S.C. § 7401(a)(2). Congress' purpose in creating the CAA, in part, was "to protect and enhance the quality of the Nation's air resources so as to promote the public health and welfare and the productive capacity of its population," and "to initiate and accelerate a national research and development program to achieve the prevention and control of air pollution." CAA § 101(b)(1)–(2), 42 U.S.C. § 7401(b)(1)–(2). The CAA and the regulations promulgated thereunder aim to protect human health and the environment by reducing emissions of nitrogen oxides (NOx) and other pollutants from mobile sources of air pollution. Nitrogen oxides are a family of highly reactive gases that play a major role in the atmospheric reactions with volatile organic compounds (VOCs) that produce ozone (smog) on hot summer days. Breathing ozone can trigger a variety of health problems including chest pain, coughing, throat irritation, and congestion. Breathing ozone can also worsen bronchitis, emphysema, and asthma. Children are at greatest risk of experiencing negative health impacts from exposure to ozone.

The EPA's allegations here concern light-duty motor vehicles for which 40 C.F.R. Part 86 sets emission standards and test procedures and section 203 of the CAA, 42 U.S.C. § 7522, sets compliance provisions. Light-duty vehicles must satisfy emission standards for certain air pollutants, including NOx. 40 C.F.R. § 86.1811-04. The EPA administers a certification program to ensure that every vehicle introduced into United States commerce satisfies applicable emission standards. Under this program, the EPA issues certificates of conformity (COCs), and thereby approves the introduction of vehicles into United States commerce.

To obtain a COC, a light-duty vehicle manufacturer must submit a COC application to the EPA for each test group of vehicles that it intends to enter into United States commerce. 40 C.F.R. § 86.1843-01. The COC application must include, among other things, a list of all auxiliary emission control devices (AECDs) installed on the vehicles. 40 C.F.R. § 86.1844-01(d)(11). An AECD is "any element of design which senses temperature, vehicle speed, engine RPM, transmission gear, manifold vacuum, or any other parameter for the purpose of activating, modulating, delaying, or deactivating the operation of any part of the emission control system." 40 C.F.R. § 86.1803-01. The COC application must also include "a justification for each AECD, the parameters they sense and control, a detailed justification of each AECD that results in a reduction in effectiveness of the emission control system, and [a] rationale for why it is not a defeat device." 40 C.F.R. § 86.1844-01(d)(11).

A defeat device is an AECD "that reduces the effectiveness of the emission control system under conditions which may reasonably be expected to be encountered in normal vehicle operation and

use, unless: (1) Such conditions are substantially included in the Federal emission test procedure; (2) The need for the AECD is justified in terms of protecting the vehicle against damage or accident; (3) The AECD does not go beyond the requirements of engine starting; or (4) The AECD applies only for emergency vehicles . . . ." 40 C.F.R. § 86.1803-01.

Motor vehicles equipped with defeat devices, such as those at issue here, cannot be certified. EPA, *Advisory Circular Number 24: Prohibition on use of Emission Control Defeat Device* (Dec. 11, 1972); *see also* 40 C.F.R. §§ 86-1809-01, 86-1809-10, 86-1809-12. Electronic control systems which may receive inputs from multiple sensors and control multiple actuators that affect the emission control system's performance are AECDs. EPA, *Advisory Circular Number 24-2: Prohibition of Emission Control Defeat Devices – Optional Objective Criteria* (Dec. 6, 1978). "Such elements of design could be control system logic (i.e., computer software), and/or calibrations, and/or hardware items." *Id.*

"Vehicles are covered by a certificate of conformity only if they are in all material respects as described in the manufacturer's application for certification . . . ." 40 C.F.R. § 86.1848-10(c)(6). Similarly, a COC issued by EPA, including those issued to VW, state expressly, "[t]his certificate covers only those new motor vehicles or vehicle engines which conform, in all material respects, to the design specifications" described in the application for that COC. *See also* 40 C.F.R. §§ 86.1844-01 (listing required content for COC applications), 86.1848-01(b) (authorizing the EPA to issue COCs on any terms that are necessary or appropriate to assure that new motor vehicles satisfy the requirements of the CAA and its regulations).

The CAA makes it a violation "for any person to manufacture or sell, or offer to sell, or install, any part or component intended for use with, or as part of, any motor vehicle or motor vehicle engine, where a principal effect of the part or component is to bypass, defeat, or render inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter, and where the person knows or should know that such part or component is being offered for sale or installed for such use or put to such use." CAA § 203(a)(3)(B), 42 U.S.C. § 7522(a)(3)(B); 40 C.F.R. § 86.1854-12(a)(3)(ii). Additionally, manufacturers are prohibited from selling, offering for sale, introducing into commerce, delivering for introduction into commerce, or importing, any new motor vehicle unless that vehicle is covered by an EPA-issued COC. CAA § 203(a)(1), 42 U.S.C. § 7522(a)(1); 40 C.F.R. § 86.1854-12(a)(1). It is also a violation to cause any of the foregoing acts. CAA § 203(a), 42 U.S.C. § 7522(a); 40 C.F.R. § 86-1854-12(a).

Alleged Violations

Each VW vehicle identified by the table below has AECDs that were not described in the application for the COC that purportedly covers the vehicle. Specifically, VW manufactured and installed software in the electronic control module (ECM) of these vehicles that sensed when the vehicle was being tested for compliance with EPA emission standards. For ease of reference, the EPA is calling this the "switch." The "switch" senses whether the vehicle is being tested or not based on various inputs including the position of the steering wheel, vehicle speed, the duration of the engine's operation, and barometric pressure. These inputs precisely track the parameters of the federal test procedure used for emission testing for EPA certification purposes. During EPA

emission testing, the vehicles' ECM ran software which produced compliant emission results under an ECM calibration that VW referred to as the "dyno calibration" (referring to the equipment used in emissions testing, called a dynamometer). At all other times during normal vehicle operation, the "switch" was activated and the vehicle ECM software ran a separate "road calibration" which reduced the effectiveness of the emission control system (specifically the selective catalytic reduction or the lean NOx trap). As a result, emissions of NOx increased by a factor of 10 to 40 times above the EPA compliant levels, depending on the type of drive cycle (e.g., city, highway).

The California Air Resources Board (CARB) and the EPA were alerted to emissions problems with these vehicles in May 2014 when the West Virginia University's (WVU) Center for Alternative Fuels, Engines & Emissions published results of a study commissioned by the International Council on Clean Transportation that found significantly higher in-use emissions from two light duty diesel vehicles (a 2012 Jetta and a 2013 Passat). Over the course of the year following the publication of the WVU study, VW continued to assert to CARB and the EPA that the increased emissions from these vehicles could be attributed to various technical issues and unexpected in-use conditions. VW issued a voluntary recall in December 2014 to address the issue. CARB, in coordination with the EPA, conducted follow up testing of these vehicles both in the laboratory and during normal road operation to confirm the efficacy of the recall. When the testing showed only a limited benefit to the recall, CARB broadened the testing to pinpoint the exact technical nature of the vehicles' poor performance, and to investigate why the vehicles' onboard diagnostic system was not detecting the increased emissions. None of the potential technical issues suggested by VW explained the higher test results consistently confirmed during CARB's testing. It became clear that CARB and the EPA would not approve certificates of conformity for VW's 2016 model year diesel vehicles until VW could adequately explain the anomalous emissions and ensure the agencies that the 2016 model year vehicles would not have similar issues. Only then did VW admit it had designed and installed a defeat device in these vehicles in the form of a sophisticated software algorithm that detected when a vehicle was undergoing emissions testing.

VW knew or should have known that its "road calibration" and "switch" together bypass, defeat, or render inoperative elements of the vehicle design related to compliance with the CAA emission standards. This is apparent given the design of these defeat devices. As described above, the software was designed to track the parameters of the federal test procedure and cause emission control systems to underperform when the software determined that the vehicle was not undergoing the federal test procedure.

VW's "road calibration" and "switch" are AECDs[1] that were neither described nor justified in the applicable COC applications, and are illegal defeat devices. Therefore each vehicle identified by the table below does not conform in a material respect to the vehicle specifications described in the COC application. As such, VW violated section 203(a)(1) of the CAA, 42 U.S.C. § 7522(a)(1), each time it sold, offered for sale, introduced into commerce, delivered for introduction into commerce, or imported (or caused any of the foregoing with respect to) one of the hundreds of thousands of new motor vehicles within these test groups. Additionally, VW

[1] There may be numerous engine maps associated with VW's "road calibration" that are AECDs, and that may also be defeat devices. For ease of description, the EPA is referring to these maps collectively as the "road calibration."

APX 204

violated section 203(a)(3)(B) of the CAA, 42 U.S.C. § 7522(a)(3)(B), each time it manufactured and installed into these vehicles an ECM equipped with the "switch" and "road calibration."

The vehicles are identified by the table below. All vehicles are equipped with 2.0 liter diesel engines.

Model Year	EPA Test Group	Make and Model(s)
2009	9VWXV02.035N	VW Jetta, VW Jetta Sportwagen
2009	9VWXV02.0U5N	VW Jetta, VW Jetta Sportwagen
2010	AVWXV02.0U5N	VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2011	BVWXV02.0U5N	VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2012	CVWXV02.0U5N	VW Beetle, VW Beetle Convertible, VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2012	CVWXV02.0U4S	VW Passat
2013	DVWXV02.0U5N	VW Beetle, VW Beetle Convertible, VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2013	DVWXV02.0U4S	VW Passat
2014	EVWXV02.0U5N	VW Beetle, VW Beetle Convertible, VW Golf, VW Jetta, VW Jetta Sportwagen, Audi A3
2014	EVWXV02.0U4S	VW Passat
2015	FVGAV02.0VAL	VW Beetle, VW Beetle Convertible, VW Golf, VW Golf Sportwagen, VW Jetta, VW Passat, Audi A3

Enforcement

The EPA's investigation into this matter is continuing. The above table represents specific violations that the EPA believes, at this point, are sufficiently supported by evidence to warrant the allegations in this NOV. The EPA may find additional violations as the investigation continues.

The EPA is authorized to refer this matter to the United States Department of Justice for initiation of appropriate enforcement action. Among other things, persons who violate section 203(a)(3)(B) of the CAA, 42 U.S.C. § 7522(a)(3)(B), are subject to a civil penalty of up to $3,750 for each violation that occurred on or after January 13, 2009;[1] CAA § 205(a), 42 U.S.C. § 7524(a); 40 C.F.R. § 19.4. In addition, any manufacturer who, on or after January 13, 2009, sold, offered for sale, introduced into commerce, delivered for introduction into commerce, imported, or caused any of the foregoing acts with respect to any new motor vehicle that was not covered by an EPA-issued COC is subject, among other things, to a civil penalty of up to $37,500 for each violation.[2] CAA § 205(a), 42 U.S.C. § 7524(a); 40 C.F.R. § 19.4. The EPA may seek, and district courts may order, equitable remedies to further address these alleged violations. CAA § 204(a), 42 U.S.C. § 7523(a).

[1] $2,750 for violations occurring prior to January 13, 2009.
[2] $32,500 for violations occurring prior to January 13, 2009.

APX 205

The EPA is available to discuss this matter with you. Please contact Meetu Kaul, the EPA attorney assigned to this matter, to discuss this NOV. Ms. Kaul can be reached as follows:

Meetu Kaul
U.S. EPA, Air Enforcement Division
1200 Pennsylvania Avenue, NW
William Jefferson Clinton Federal Building
Washington, DC 20460
(202) 564-5472
kaul.meetu@epa.gov

Sincerely,

Phillip A. Brooks
Director
Air Enforcement Division
Office of Civil Enforcement

Copy:
Todd Sax, California Air Resources Board
Walter Benjamin Fisherow, United States Department of Justice
Stuart Drake, Kirkland & Ellis LLP

July 11, 2018

Wyden: Paper Ballots and Audits are Essential to Secure American Elections Against Foreign Hackers

Testifying at Senate Rules Committee, Wyden Blasts Voting Machine Manufacturers, Calls for Passage of His Bill Mandating Paper Ballots

Washington, D.C. – Sen. Ron Wyden, D-Ore., sounded the alarm about the urgent need for paper ballots to secure American elections against foreign hackers, in testimony at the Senate Rules Committee today.

Wyden called on the Senate to pass his Protecting American Votes and Elections Act, which requires paper ballots and effective audits for all federal elections, and has been endorsed by leading cybersecurity experts. View his full testimony here.

"At least 44 million Americans - and perhaps millions more - have no choice but to use insecure voting machines that have foreign hackers salivating," Wyden said. **"It is inexcusable that American democracy depends on hackable voting technology made by a handful of companies that have evaded oversight and stonewalled Congress. That must end."**

Wyden blasted voting machine companies for refusing to answer basic questions about their cybersecurity practices. ES&S continued to stonewall Wyden's questions even after the New York Times reported the company had sold voting technology with remote monitoring software installed.

"The only way to make this worse would be to leave unguarded ballot boxes in Moscow and Beijing," Wyden said. **"Americans must move to paper ballots, marked by hand. Until that system is adopted, every election that goes by is an election that Russia could hack."**

###

Exhibit J

Kim Zetter. (Jul. 17, 2018). Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States. *Motherboard*.

MOTHERBOARD VICE

PCANYWHERE

Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States

Remote-access software and modems on election equipment 'is the worst decision for security short of leaving ballot boxes on a Moscow street corner.'

By Kim Zetter | Jul 17 2018, 5:00am

UP NEXT

Solve the Internet Crossword Puzzle: August 1, 2018

APX 210

SHARE TWEET

The nation's top voting machine maker has admitted in a letter to a federal lawmaker that the company installed remote-access software on election-management systems it sold over a period of six years, raising questions about the security of those systems and the integrity of elections that were conducted with them.

In a letter sent to Sen. Ron Wyden (D-OR) in April and obtained recently by Motherboard, Election Systems and Software acknowledged that it had "provided pcAnywhere remote connection software ... to a small number of customers between 2000 and 2006," which was installed on the election-management system ES&S sold them.

ADVERTISEMENT

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

The statement contradicts what the company **told me and fact checkers for a story I wrote for the *New York Times*** in February. At that time, a spokesperson said ES&S had never installed pcAnywhere on any election system it sold. "None of the employees, ... including long-tenured employees, has any knowledge that our voting systems have ever been sold with remote-access software," the spokesperson said.

ES&S did not respond on Monday to questions from Motherboard, and it's not clear why the company changed its response between February and April. Lawmakers, however, have subpoena powers that can compel a company to hand over documents or provide sworn testimony on a matter lawmakers are investigating, and a statement made to lawmakers

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

Trump's Stupid 'Where Is the DNC Server?' Conspiracy Theory, Explained

Trump refuses to believe all the evidence that Russia hacked the DNC, because he understands nothing about how digital forensics works.

Motherboard Jason Koebler Jul 16

ES&S is the top voting machine maker in the country, a position it held in the years 2000-2006 when it was installing pcAnywhere on its systems. The company's machines were used statewide in a number of states, and

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

The company told Wyden it stopped installing pcAnywhere on systems in December 2007, after the Election Assistance Commission, which oversees the federal testing and certification of election systems used in the US, released new voting system standards. Those standards required that any election system submitted for federal testing and certification thereafter could contain only software essential for voting and tabulation. Although the standards only went into effect in 2007, they were created in 2005 in a very public process during which the security of voting machines was being discussed frequently in newspapers and on Capitol Hill.

ADVERTISEMENT

Election-management systems are not the voting terminals that voters use to cast their ballots, but are just as critical: they sit in county election

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

upgrade or alter software. But election-management systems and voting machines are supposed to be air-gapped for security reasons—that is, disconnected from the internet and from any other systems that are connected to the internet. ES&S customers who had pcAnywhere installed also had modems on their election-management systems so ES&S technicians could dial into the systems and use the software to troubleshoot, thereby creating a potential port of entry for hackers as well.

In May 2006 in Allegheny County, Pennsylvania, ES&S technicians used the pcAnywhere software installed on that county's election-management system for hours trying to reconcile vote discrepancies in a local election, according to a report filed at the time. And in a contract with Michigan, which covered 2006 to 2009, ES&S discussed its use of pcAnywhere and modems for this purpose.

"In some cases, the Technical Support representative accesses the customer's system through PCAnywhere—off-the-shelf software which allows immediate access to the customer's data and network system from a remote location—to gain insight into the issue and offer precise solutions," ES&S wrote in a June 2007 addendum to the contract. "ES&S technicians can use PCAnywhere to view a client computer, assess the exact situation that caused a software issue and to view data files."

Motherboard asked a Michigan spokesman if any officials in his state ever

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

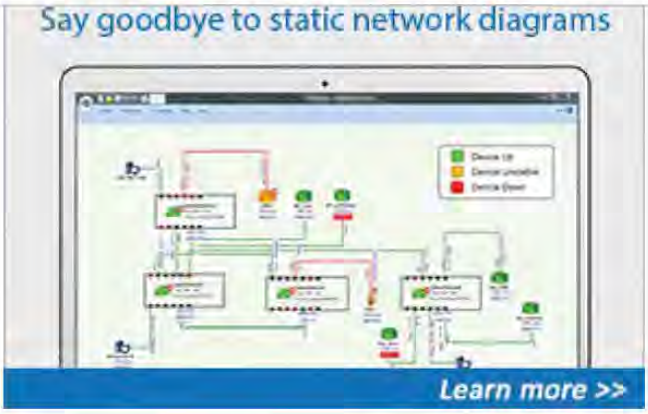
security vulnerabilities. If an attacker can gain remote access to an election-management system through the modem and take control of it using the pcAnywhere software installed on it, he can introduce malicious code that gets passed to voting machines to disrupt an election or alter results.

Wyden told Motherboard that installing remote-access software and modems on election equipment "is the worst decision for security short of leaving ballot boxes on a Moscow street corner."

In 2006, the same period when ES&S says it was still installing pcAnywhere on election systems, hackers **stole the source code for the pcAnyhere software**, though the public didn't learn of this until years later in 2012 when a hacker posted some of the source code online, forcing Symantec, the distributor of pcAnywhere, to admit that it had been stolen years earlier. Source code is invaluable to hackers because it allows them to examine the code to find security flaws they can exploit. When Symantec admitted to the theft in 2012, it took the unprecedented step of **warning users to disable or uninstall the software** until it could make sure that any security flaws in the software had been patched.

ADVERTISEMENT

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018



Around this same time, security researchers **discovered a critical vulnerability** in pcAnywhere that would allow an attacker to seize control of a system that had the software installed on it, without needing to authenticate themselves to the system with a password. And other researchers with the security firm Rapid7 scanned the internet for any computers that were online and had pcAnywhere installed on them and found nearly 150,000 were configured in a way that would allow direct access to them.

It's not clear if election officials who had pcAnywhere installed on their systems, ever patched this and other security flaws that were in the software.

"[I]t's very unlikely that jurisdictions that had to use this software ... updated it very often," says Joseph Lorenzo Hall, chief technologist for the Center for Democracy and Technology, "meaning it's likely that a non-

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

only to dial out, not receive calls, so that only election officials could initiate connections with ES&S. But when Wyden's office asked in a letter to ES&S in March what settings were used to secure the communications, whether the system used hard-coded or default passwords and whether ES&S or anyone else had conducted a security audit around the use of pcAnywhere to ensure that the communication was done in a secure manner, the company did not provide responses to any of these questions.

Even if ES&S and its customers configured their remote connections to ES&S in a secure manner, the recent **US indictments against Russian state hackers** who tried to interfere in the 2016 presidential elections, show that they targeted companies in the US that make software for the administration of elections. An attacker would only have had to hack ES&S and then use its network to slip into a county's election-management system when the two systems made a remote connection.

In its letter to Wyden, ES&S defended its installation of pcAnywhere, saying that during the time it installed the software on customer machines prior to 2006, this was "considered an accepted practice by numerous technology companies, including other voting system manufacturers."

Motherboard contacted two of the top vendors—Hart InterCivic and Dominion—to verify this, but neither responded. However, Douglas Jones,

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

their contracts with customers included the requirement of a remote-login port allowing [the company] to have remote access to the customer system in order to allow customer support."

He notes that election officials who purchased the systems likely were not aware of the potential risks they were taking in allowing this and didn't understand the threat landscape to make intelligent decisions about installing such software.

All of this raises questions about how many counties across the US had remote-access software installed—in addition to ES&S customers—and whether intruders had ever leveraged it to subvert elections.

Although Wyden's office asked ES&S to identify which of its customers were sold systems with pcAnywhere installed, the company did not respond. ES&S would only say that it had confirmed with customers who had the software installed that they "no longer have this application installed."

The company didn't respond to questions from Motherboard asking when these customers removed the software—whether ES&S had instructed them to do so back in 2007 when the company says it stopped installing the software on new systems it sold or whether it had only recently told customers to remove it following concerns raised in the 2016 presidential elections that Russian hackers were targeting election networks in the US.

UP NEXT
Solve the Internet Crossword Puzzle: August 1, 2018

Exhibit K

OKANOGAN County Election Procedures

These documents are too voluminous, and will therefore be made available upon request pursuant to Wash. R. Evid. 1006 and related rules.

1. Public Records available upon request from Okanogan County Auditor
2. Basic Instructions
    a. 10-03 Clearinghouse Judicial Elections and Exceptions 2010.pdf
    b. Election Emergency Procedures.doc
    c. Good Vote Bad Vote Poster 2.pdf
    d. Instructions - Preparing Notice of Election.docx
    e. Observer's Guide.pdf
    f. Seal Logs.doc
3. Misc. Instructions
    a. After Election
        i. Mail merge for after certification.doc
        ii. BN Instructions scan and resolve.doc
        iii. Test Election Database.docx
    b. Ballot now
        i. BN Instructions scan and resolve.doc
        ii. Test Election Database.docx
4. Ballots
    a. 1 Extract, Upload ballot, print labels, and voter list - updated.docx
    b. Checking ballots back from the printer. docMail
    c. Certification to OSOS.docx
    d. Placement of issue and offices on ballot.doc
    e. Preparing to print envelopes.doc
5. Canvass Board

a. Ballot to Canvass Board log.doc
    b. Ballots to Canvass Board Master.doc

    c. Canvass.docx
    d. Certify.docx
6. Inspection Boards
    a. WAC 434 Ballot inspection.doc
7. Voter Registration
    a. List of Voters for each election.doc
8. Voting equipment – HART
    a. Processing of ballots as defined in WAC 434.doc
9. WEI
    a. Set candidate statement word length WEI.docx
    b. Testing MyBallot.doc
    c. Turn on MyBallot Ballot Status for UOCAVA Ballots.doc
    d. WEI Candidate filing.pdf
    e. WEI election results Ballots left to count.docx
10. Procedure manual
    a. 10 Elections Department Policy Placement on ballot.pdf
    b. 10-03 Clearinghouse Judicial Elections and Exceptions 2010.pdf
    c. Canvass Board Manual.pdf
    d. Instructions for BOSS Setup.docx
    e. New Procedures Canvass Board 2017.doc
    f. Placement of issue and offices on ballot.doc
    g. Procedures 1 - Voter Registration.doc
    h. Procedures 2 - Election Envelopes, Inactive, Special ballots.doc
    i. Procedures Canvass Board 2017.doc
    j. Procedures Canvass Board 2017.pdf
11. Votec Instructions
    a. Ballot Log.doc
    b. Ballots returned undeliverable.doc
    c. Ballots that need proof of ID.doc
    d. Ballots that were forwarded and you got a notice from the Post Office.doc
    e. Candidate Filing.doc
    f. Candidate Module 1.doc
    g. Candidate Module.doc
    h. Change Notice Letters.doc
    i. Change status of voter from Inactive to Active.doc
    j. Checking signatures.doc
    k. Create an absentee list to be emailed.doc
    l. Election night issue ballots.doc
    m. Election Setup.doc
    n. Get totals of ballots sent and ballots returned.doc
    o. Getting totals of ballots in and out for an election.doc
    p. Handle duplicate registrations.doc
    q. How to get a list of voters with DLV.doc
    r. Inactive Purge.doc
    s. Issuing a ballot over the counter.doc
    t. List of return ballots.doc

u. Lists of ballots in.doc
v. Move winning candidates forward from Primary to General - Copy.doc
w. New registrations after the initial loading of ballots that are in By Mail Precincts or Request Ongoing Ballots.doc
x. Non ID compliant purge.docx
y. Odd year preparation.docx
z. Preparing for an election with State VRDB.doc
aa. Print Mailing Label Dymo for envelope Non ballot.doc
bb. Printing a Precinct with District List.doc
cc. Printing the report of previous registrations.doc
dd. Procedure changes.doc
ee. Process Exceptions.docx
ff. Provisional Ballots.doc
gg. Public Instruction for ballots that were forwarded, and you got a notice from the Post
hh. Offic1.doc
ii. Registration Totals for an election.docx
jj. Remove cancelled voters from election.doc
kk. Report number of ballots requested and received.doc
ll. Update or change Elected Officials list.doc
mm. Update voters who voted a Provisional Ballot.doc
nn. Upload ballot print labels, and voter list.docx
oo. Use of Disabled Access units.doc
pp. VOTEC Candidate File.docx
qq. Voter Stats.docx
rr. When an incorrect serial number was entered, and the wrong person was updated.docx
ss. Using DAU unit.doc

12. 2008 Instructions
    a. New resolve instructions 2008.doc
    b. New Scan instructions 2008.doc
13. Ballot Now
    a. 2012 Ballot Scanning - Resolution - Boards .doc
    b. BACK UP VOTING SYSTEM.doc
    c. Ballot Now Sequential Steps to start up.doc
    d. Print ballot images for the Printer.doc
    e. Write-Ins.doc
14. Instructions for Tally
    a. Finalize Tally after Election Certification.doc
    b. Set up new election database.doc

Exhibit L

James M. Miller. (August 5, 2018). Professional Experience and Resume.

James M. Miller

Professional Experience & Resume

Updated August 5, 2018

Project Management, Business Process, Quality Control and Data Science

I, James M. Miller, worked at Boeing for 17 years in various positions and assignments, mostly as a Project Manager while earning two master's Certificates in Project Management (academic and technical).

For seven of these years, the Petitioner was assigned to Cabin Systems Material as a subject matter expert for new technology for the Boeing interiors, including new In-flight entertainment, satellite communications, and the Boeing contract manager for Connection by Boeing. Ref: (https://en.wikipedia.org/wiki/Connexion_by_Boeing).

During this time period, I was assigned the task of developing a new Boeing business process which resulted in the new Boeing business process BPI-4232, know as "Customer Selected Equipment (CSE)." This resolved the manufacturing conflicts when new technology was desired by the customer demanding that Boeing install the new systems on the customer airlines.

Previous to CSE, supplemental type certifications (STE), were used to qualify new systems as retrofit on existing aircraft. This caused complex manufacturing issues and waste in the Boeing build line, causing delays estimated to be over $400 million per year. I led a team of engineers, finance, supply managers, and customer engineers, CSE was created where pre-qualification data for new technology was first reviewed by Boeing engineering as a fee based contract. I negotiated and managed over $50 million of these initial contracts while in this position.

The CSE process required three years of process review that included manufacturing engineering, multiple vendor engineering, quality reviews, industrial design processes for new equipment, and thousands of hours of overall process design meetings around the globe. The CSE process enabled a multi-billion dollar industry to flourish around the globe. A similar process was adopted by Airbus.

The Petitioner also worked seven years within Boeing’s Cabin System Engineering group, assigned as a project manager for the development of over $34 million dollars in new technology for avionics, cabin server, terminal wireless LAN, video surveillance, and other projects. A notable project of relevance was the Emirates Airline First Class Seat Failure. I was

assigned to manage the investigation and solution of Emirate's very expensive seat failures, given unlimited authority and resources of the Boeing company, to rapidly resolve the issue. I gathered a team of scientists and engineers from Phantom Works, Crane Electronics, Boeing Electronics, and Panasonic Corporation.

Upon examination under electron microscopy of the suspected integrated circuits involved in the seat and supporting Boeing systems, hidden circuits operated by bootlegged undetectable machine language, was discovered in related vendor circuit. This circuit had not been discovered during 'red label' testing, nor properly disclosed by the vendor. This resulted in the decertification, heavy fines, and very bad press with the vendor's airline customers, and a major recall/replacement plan of all of the vendor's part numbers.

The notable part of this testimony is that hidden integrated circuits and bootlegged machine language is possible even under highly scrutinized aerospace procedures. I also worked on other avionics boxes that had to interface with the main airplane computer, or MCU; requiring failure modes analysis of degrees of ten to the ninth (10^9) in order to pass FAA flight regulations. The process control, review, understanding, and acceptance of software, hardware, and signal interfaces is tedious to develop, but necessary for flight safety. Because of this, airplanes do not fall out of the sky with any regularity, or due to systems failure. Almost all airplane failure is operational or administrative involving bad decisions.

I also worked 25 years in the municipal utility industry, obtaining many training certificates involving safety processes, hydraulic and chemical engineering, computer programming in multiple languages, Supervisory Control and Data Acquisition (SCADA) for automating pumping systems, alarms, and basic data telemetry. This often involved a forensic analysis of acquired data with database programming to make and test failure hypotheses to correct intrinsic failure modes. I was certified at the highest operational level with the State of Washington as a WDM-IV.

Currently, I am the Chief Operating Officer (CEO), of Core Data Analytics, where I oversee the daily operations and development of business operations software for government and private business. www.easyops.co I also serve as the business analyst and database designer, ensuring that the database design is efficiently developed to the 5th Normal form—a mathematical formula to produce the least amount of data necessary to reassemble datum into information. https://en.wikipedia.org/wiki/Boyce%E2%80%93Codd_normal_form.

I have extensive experience and education as an expert in project management, forensic processes, troubleshooting, quality control, design and control of complex systems.

System Security

Voters can rest assured that Washington's Election system is secure.

We have embarked on an unprecedented opportunity to work collaboratively with the Department of Homeland Security to ensure that our election systems remain secure. This partnership allows us to work together, elections and IT experts working hand in hand to ensure our systems are secure.

We are thrilled to partner with DHS to –

- Assess vulnerabilities and identify mitigation plans
- Share information
- Rely on DHS for local in person support
- Report incidents or threats

Some highlights of the programs already underway –

The Risk and Vulnerability Assessment (RVA) - The RVA encompasses a wide range of security services including –

- Penetration testing
- Web application testing
- Social engineering

Cyber Resilience Review (CRR) - The CRR measures and enhances the implementation of key cybersecurity capacities and capabilities of critical infrastructure and SLTT governmental entities. This is a non-technical assessment helps the assessed organization to develop an understanding of their operational resilience and ability to manage cyber risk to critical services during normal operations and times of operational stress or crisis.

This DHS partnership provides all of these services to us at no cost.

In addition, Washington employs the recommendations raised by security experts, and have done so for years. Such as –

- Paper-based systems, including voter verifiable paper audit trails.
- Independent testing.
- Pre- and post-election audits.
- Physical security of tabulation equipment.

Before a tabulation system can be used in Washington, we require testing at a federally approved independent testing lab. These expert testers include security reviews as a part of their overall testing efforts. Then, systems are tested here at the state level and reviewed by

our own voting systems certification board, comprised of technology experts, accessibility experts, and county election officials.

Counties must then perform acceptance testing and logic and accuracy testing prior to every election. In addition, we conduct post-election audits, where we draw precincts and races at random and compare the vote totals from the tabulator to a hand count of ballots before the election is certified.

Counties that *optically* scan ballots prior to Election Day have approved tabulation security plans in place and on file with our office. Additionally, counties maintain continuity of operations plans so that they can be ready in the event of a disruption. We are present at logic and accuracy tests where we review and ensure, both visually and through hash testing, that the equipment and software in use hasn't changed from the version certified both federally and in Washington.

We use a paper-based system, which always allows Washington elections officials the opportunity to see first-hand the voter's intent. We can go back to the paper ballot marked by the voter and hand count a race, particularly when the races are very close. And for the few voters who are voting on touch screen voting systems, we require a paper audit trail verified by the voter.

In addition, we work proactively and closely with IT and security experts to routinely review, identify, and correct any vulnerabilities with our technical systems.

Washington has a long-standing tradition of balancing this physical security with technical system security and providing accessible systems to our voters.

In addition to the security of our tabulation systems, Washington takes great pride in securing our other vital systems. The Voter registration Database (VRDB) and Washington Elections Information (WEI) systems are secured by highly skilled Office of the Secretary of State (OSOS) IT staff, using state of the art equipment and following IT industry best practices.

Network Based Security:

- All elections systems are protected by state of the art Intrusion Prevention Systems (IPS) and firewalls. Only authorized Internet Protocol (IP) address are allowed access to these systems. This access is running on a network that is only used by authorized partners and the accessible web servers are isolated on a network demilitarized zone (DMZ) with the database servers placed in another secured inside a isolated network.

Physical Security:

- The servers are housed in a secure single tenant modern facility with dual redundant alarms, security cameras, and FM200 protection. Physical access to the data center is restricted to only three authorized OSOS full-time IT staff members using security proximity cards and unique keypad pin numbers. The data center is located next door to the police station and response times for alarms average 2 to 8 minutes.

Patch Management:

- The Quality Assurance (QA) system is patched the day after any “patches”, “hotfixes”, or “cumulative” updates are received from Microsoft. Production (prod) servers are patched after the system updates are fully tested in QA and authorized for deployment. In most cases, the production system patched two weeks after QA to allow for testing and verification.

Security Audit:

- Regular security scans by OSOS IT security staff are performed to test and verify the security of the firewalls, IPS, and servers.
- Periodic 3rd party contracted security audits are performed to test and verify the security and effectiveness of the firewalls, IPS, servers, and facility.

Log Review:

- Daily firewall logs are reviewed at least 4 times a day and weekend logs are reviewed every Monday morning.
- Daily system event logs are reviewed at least twice a day and weekend logs are reviewed every Monday morning.

Elections Results Site

- The elections results are hosted in Microsoft’s Azure cloud, which provides server and geographic redundancy.
- Results data is retrieved from a secure location provided by Washington Election Information System (WEI) at specified times (intervals).
- Elections results data is parsed and presented to users graphically in read-only and compact web files (html) for speed and performance under heavy user access.
- Graphic representation of the results is not connected to WEI system or network and is not dependent on it after results have been securely transmitted at aforementioned intervals.

Tabulation Systems

Before a system can be considered for state certification, it must be first tested by an independent testing authority that has been accredited by the Election Assistance Commission. There currently are three test labs (certified independent testing authorities) that are accredited by the Election Assistance Commission. NTS Huntsville, Pro V&V, and SLI Compliance. You can find more information about those accreditations here: https://www.eac.gov/testing_and_certification/accredited_test_laboratories.aspx (https://www.eac.gov/testing_and_certification/accredited_test_laboratories.aspx)

All voting system testing documentation, which includes the test lab identification, can be found here: https://www.eac.gov/testing_and_certification/default.aspx (https://www.eac.gov/testing_and_certification/default.aspx). When reviewing these testing

documents, keep in mind that not all of these systems are certified for use in the State of Washington. The list of systems certified for using the State of Washington can be found here: https://www.sos.wa.gov/elections/research/Voting-System-Testing-and-Certification.aspx (https://www.sos.wa.gov/elections/research/Voting-System-Testing-and-Certification.aspx). A list of voting systems that are in use by county can be found here: https://www.sos.wa.gov/elections/research/Voting-Systems-by-County.aspx (https://www.sos.wa.gov/elections/research/Voting-Systems-by-County.aspx)

No tabulation equipment is connected to the internet or capable of wireless communication. Additionally, WAC 434-261-045 requires that security measures be employed to detect any inappropriate access to protect the physical security of the system. That could include video surveillance, however, that is not required. Counties can employ multiple layers of physical security that would detect inappropriate access, for example, logs and seals.

FORTUNE

This Website Graded Apple, Google, Amazon, Microsoft, and Samsung on Their Political Leanings

By **DON REISINGER** October 17, 2017

A site that ranks companies based on their commitment to conservative values has some problems with some of Silicon Valley's biggest names.

On Tuesday, Bloomberg published an interview with David Black, the co-founder and former CEO of Aegis Science, and the husband to Republican representative Diane Black, herself a co-founder in Aegis. In that interview, Black described a site that he's built with more than $1 million of his money called 2ndVote. The goal: to determine how closely companies hold conservative values and rank them on a scale of one to five, with one being most liberal and five as most conservative.

In its look at rankings, 2ndVote appears to have given some of the most major tech companies generally have low scores.

Amazon

Amazon (AMZN, +0.33%) generated a score of 1.9 out of five in the 2ndVote test.

According to 2ndVote, the e-commerce giant scored low marks for prohibiting the sale of firearms on its site and its support for the "liberal 2015 Paris climate deal" as a problem.

However, Amazon got some points back for supporting the Salvation Army, which 2ndVote describes as "a group supporting traditional marriage" and "a pro-life organization."

APX 230

Apple

Apple (AAPL, -0.32%) came in at the bottom of the 2ndVote scale with a rating of one out of five.

In every metric 2ndVote considers, including gun rights, the environment, marriage, life, and immigration, among others, Apple scored a one.

In the marriage measure, for instance, Apple was cited for supporting same-sex marriage. The site also gave Apple low marks for being a corporate supporter of Center for American Progress, "a liberal think tank" that "supports abortion as an equal right for women."

There's even a button on the site said to direct site visitors to e-mail Apple CEO Tim Cook directly.

Get Data Sheet, Fortune*'s technology newsletter*

Google

It's a similar story for Google (GOOG, -0.49%), which earned the lowest-possible one out of five from 2ndVote.

The site criticized Google for matching gifts to the Brady Campaign, an effort that 2ndVote says opposes "Stand Your Ground laws and concealed carry."

In its discussion on the environment, 2ndVote says Google "engages with the World Wildlife Fund, which is an organization that supports a carbon tax and also supports the 2015 Paris climate deal."

Microsoft

Microsoft (MSFT, -0.31%) also couldn't break from its competitors and ultimately scored a one out of five in the 2ndVote test.

Microsoft is another supporter of the Brady Campaign, which earned it low marks on 2nd Amendment rights. The tech giant was also hit for being "a partner of The Nature Conservancy, a liberal and active proponent of cap-and-trade and a carbon tax."

In its evaluation of Microsoft, 2ndVote also says that the company supports organizations, like Center for American Progress and the League of United Latin American Citizens, which support sanctuary cities.

Samsung

Not even the Korea-based Samsung (SSNLF, +242224.56%) could sidestep a 2ndVote rating. And like many others in the technology space, Samsung received a one out of five from 2ndVote.

Interestingly, 2ndVote didn't have much to say about Samsung. While other companies were tapped for having relationships with multiple "liberal" organizations, Samsung's score was based on its support for one organization: the Center for American Progress.

From the 2nd Amendment to religious liberty, it was Samsung's support for the Center that earned it just one point in all the metrics. No other evidence was cited by 2ndVote, nor were other organizations with which Samsung might be involved.

Center for American Progress

Our Supporters

The Center for American Progress' work is supported by generous donors and partners—including individuals, foundations, corporations, and other organizations—that share the Center's mission and objectives. We are proud to recognize the following supporters that gave $5,000 or more to further the Center for American Progress' work during 2017.

The Center for American Progress receives more than 92 percent of its charitable contributions from individuals and foundations. Corporate funding comprises less than 3 percent of the budget, and foreign government funding comprises only 2 percent.

Our policy work is independent and driven by solutions that we believe will create a more equitable and just country. Corporate donors are not permitted to remain anonymous and corporate donations do not fund new research.

$1,000,000 or more

Anonymous (5)
Democracy Forward
Fidelity Charitable Gift Fund
Ford Foundation
Bill & Melinda Gates Foundation
The William and Flora Hewlett Foundation
The Hutchins Family Foundation
W.K. Kellogg Foundation
Jonathan and Jeannie Lavine Family Fund
Open Society Foundations

APX 233

Sandler Foundation

TomKat Charitable Trust

$500,000 to $999,999

Anonymous (2)

Carnegie Corporation of New York

Embassy of the United Arab Emirates

Amy P. Goldman Foundation

Joyce Foundation

John D. and Catherine T. MacArthur Foundation

National Philanthropic Trust

The David and Lucile Packard Foundation

The Rockefeller Foundation

Siegel Family Endowment

Silicon Valley Community Foundation

Walton Family Foundation

$100,000 to $499,999

Anonymous (4)

American Federation of State, County and Municipal Employees (AFSCME)

Apple Inc.

The Arcus Foundation

Stewart Bainum Jr.

Bloomberg Philanthropies

Paul Boskind

William K. Bowes, Jr. Foundation

The California Endowment

Annie E. Casey Foundation

Consolidated Contractors Company

Quinn Delaney and Wayne Jordan

Blair Effron

Paul & Joanne Egerman Family Charitable Foundation

Dr. Anita Friedman

First Five Years Fund

Foundation for the Greatest Good
Mark Gallogly and Lise Strickler
Gill Foundation
Goldman-Sonnenfeldt Foundation
H&R Block
Hagedorn Foundation
Irving Harris Foundation
Heising-Simons Foundation
HR&A Advisors
The Kendeda Fund
The Kresge Foundation
Lumina Foundation
Mai Family Foundation
Microsoft Corporation
Eric Mindich
New Venture Fund
New York Community Trust
Open Philanthropy Project
Robert W. Roche
Robert E. Rubin
Schlosstein-Hartley Family Foundation
Stephen M. Silberstein Foundation
Stiftung Mercator
Vanguard Charitable Endowment Program
The WhyNot Initiative

$50,000 to $99,999

Anonymous (5)
444S Foundation
Robert Abernethy
American Federation of Teachers (AFT)
William and Bonnie Apfelbaum
AT&T
Bank of America

The Bauman Foundation
Blackstone
Campion Foundation
CareFirst BlueCross BlueShield
Coalition for Public Safety
Common Counsel Foundation
Covanta
Embassy of Japan
Marc Fasteau and Anne G. Fredericks
Google
Sanjay Govil
Evelyn & Walter Haas, Jr. Fund
The Nick and Leslie Hanauer Foundation
Fred P. Hochberg and Thomas P. Healy
James Hormel
Infinite Computer Solutions Inc.
Tony James
Johnson Family Foundation
Altman Kazickas Foundation
LaSalle Adams Fund
Dale P. Mathias
Rebecca and Nathan Milikowsky
Ken Miller and Lybess Sweezy
Rockefeller Family Fund
Schwab Charitable Fund
Taipei Economic and Cultural Representative Office in the United States, or TECRO
United Minds for Progress
Henry van Ameringen
Jon F. Vein
Wallace Global Fund
Walmart
Wilburforce Foundation

$5,000 to $49,999

Anonymous (14)
A. L. Mailman Family Foundation
Wendy and Jim Abrams
ADARA Charitable Fund
Madeleine K. Albright
The Albright Stonebridge Group
American Association for Justice (AAJ)
American Beverage Association
The American Express Company
Greg and Anne Avis
Bank of America Charitable Gift Fund
B.W. Bastian Foundation
Nina Beattie and Michael Eberstadt
Carol and Frank Biondi
Adam Blumenthal
Brownstein Hyatt Farber Schreck, LLP
C.J.L. Charitable Foundation
California Community Foundation
James Capalino
Capricorn Management, LLC
Chan Zuckerberg Initiative
Dana Chasin
Simon Clark
Steven Cohen
David Colden
Combined Federal Campaign
Connecticut Street Foundation
CVS Health
Raj Date
Defenders of Wildlife
Discovery Communications
Eileen Donahoe
East Bay Community Foundation
Charles Leonard Egan

Elmo Foundation
Everytown for Gun Safety Action Fund
Express Scripts
Facebook
Federal Foreign Office of the Federal Republic of Germany
Joseph and Marie Field Foundation
Geoffrey Garin
General Electric
Heinrich Böll Foundation
Ann and Gordon Getty Foundation
Lisa and Douglas Goldman Fund
William Goldman
Joshua Greer
Garrett Gruener and Amy Slater Family Fund
Estate of Vincent Gulisano
Margaret and Shashi Gupta
Craig and Kathryn Hall
Heinrich-Böll-Stiftung North America
Joe Henderson
The Heyday Foundation
Belle Horwitz and Jonathan Weiner
Institute of International Education
Invariant
Joan and Irwin Jacobs
Japan Bank for International Cooperation
Jewish Community Foundation
Michael W. Kempner
Ed Kissam
Lebowitz-Aberly Family Foundation
Lefkofsky Family Foundation
Leonardo DRS
Damon & Heidi Lindelof
Hani Masri
Master Your Card
James Mauch

McLarty Associates

The Herbert McLaughlin Children's Trust

Al Mottur

Kristin Mugford

The Philip and Tammy Murphy Family Foundation

Nicole Mutchnik

MWW

Shekar Narasimhan

New Silk Route Advisors LP

Joyce Newstat and Susan Lowenberg

NVG LLC

Peter Orszag

Pacific Gas and Electric Company

Alan Patricof

Pearson Education

PepsiCo Inc.

Anne Peretz

Peter G. Peterson Foundation

Andrew Pincus

Heather Podesta

Portlight Inclusive Disaster Strategies

The Pritzker Children's Initiative

Quest Diagnostics

Deepak Raj

Steven Rattner and Maureen White

Robert Raymar

Francene and Charles Rodgers

Marti and Greg Rosenbaum

Laura Ross

Samsung

Parag Saxena

Alan & Susan Lewis Solomont Family Foundation

The Summers/New Family

Temasek

The Travelers Indemnity Company

Trehan Foundation Inc.
Tom and Janet Unterman
Philippe and Katherine Villers
Jeffrey C. Walker
Hope Warschaw
Herbert S. Winokur Jr
Robert Wolf

If you would like to make a gift to the Center for American Progress, please visit our donation page or contact the Development team at 202-481-8185.

Our previous supporters:

- 2016
- 2015
- 2014
- 2013

© 2018 - Center for American Progress

FILED
SUPREME COURT
STATE OF WASHINGTON
10/12/2018 9:49 AM
BY SUSAN L. CARLSON
CLERK

NO. 96235-9

SUPREME COURT OF THE STATE OF WASHINGTON

JAMES M. MILLER,

Petitioner,

v.

SECRETARY OF STATE, KIM WYMAN,

Respondent.

SECRETARY OF STATE KIM WYMAN'S RESPONSE TO PETITION FOR WRIT OF MANDAMUS

ROBERT W. FERGUSON
Attorney General

REBECCA R. GLASGOW, WSBA 32886
Deputy Solicitor General

PO Box 40100
Olympia, WA 98504-0100
RebeccaR@atg.wa.gov
360-664-3027
OID 91087

TABLE OF CONTENTS

I. INTRODUCTION 1

II. ISSUES 2

1. As a matter of law, is Mr. Miller entitled to an extraordinary writ of mandamus against the Secretary of State where he shows no failure to perform a clear, nondiscretionary duty and his requested remedies conflict with state law? 2

2. Is there another adequate remedy at law that Mr. Miller can exercise, making a writ of mandamus inappropriate? 2

III. STATEMENT OF THE CASE 2

A. Washington's System for Ensuring Election Security and Accuracy 2

B. Mr. Miller's Petition for Writ of Mandamus 6

IV. ARGUMENT 7

A. Mr. Miller Has Not Met the Strict Requirements for Showing That an Extraordinary Writ Is Appropriate 7

1. The Secretary has discretion to adopt rules that ensure secure and accurate ballot processing and tabulation 9

2. Washington law permits electronic tabulation of ballots with mandated safeguards, as well as voting on voting machines with a paper ballot printout 10

3. Washington law requires mail in ballots and voter verification through signature matching 11

4. Washington law requires a strict chain of custody for ballots that does not allow anyone other than election officials to tabulate or handle ballots.....12

B. Washington Law Provides Other Mechanisms for Mr. Miller to Challenge Secretary of State Regulations.....14

V. CONCLUSION 15

TABLE OF AUTHORITIES

Cases

Brown v. Owen,
165 Wn.2d 706, 206 P.3d 310 (2009) 7, 11

City of Seattle v. McKenna,
172 Wn.2d 551, 259 P.3d 1087 (2011) 7

Reid v. Dalton,
124 Wn. App. 113, 100 P.3d 349 (2004) 15

SEIU Healthcare 775NW v. Gregoire,
168 Wn.2d 593, 229 P.3d 774 (2010) 8, 10

Staples v. Benton County,
151 Wn.2d 460, 89 P.3d 706 (2004) 8, 14

State v. City of Seattle,
137 Wash. 455, 242 P. 926 (1926) 8, 10

Walker v. Munro,
124 Wn.2d 402, 879 P.2d 920 (1994) 8, 12, 14

Constitutional Provisions

Const. art. I, § 19 14

Statutes

52 U.S.C. § 20701 5

RCW 29A.04.611 9

RCW 29A.04.611(9) 9

RCW 29A.04.611(11) 9

RCW 29A.04.611(13) 9

RCW 29A.04.611(33) 9

RCW 29A.04.611(34) 9

RCW 29A.04.611(39) 9

RCW 29A.12 10

RCW 29A.12.010 ..... 3, 10

RCW 29A.12.020 3

RCW 29A.12.040 3

RCW 29A.12.050 3

RCW 29A.12.080 3

RCW 29A.12.080(5) 3

RCW 29A.12.085 10

RCW 29A.12.101 3

RCW 29A.12.110 ..... 4, 13

RCW 29A.12.120 ..... 4, 12, 13

RCW 29A.12.130 3

RCW 29A.12.150 10

RCW 29A.40.010 ..... 2, 11

RCW 29A.40.091 ..... 2-3, 11-12

RCW 29A.40.100 ..... 4, 13

RCW 29A.40.110(2) 4, 13

RCW 29A.40.110(3) 3, 12

RCW 29A.40.160 2

RCW 29A.40.160(4) 10

RCW 29A.40.160(7) 3, 12

RCW 29A.40.160(13) 4, 13

RCW 29A.60.110 5

RCW 29A.60.125 ..... 4, 13

RCW 29A.60.165(2) 3, 12

RCW 29A.60.170 ..... 4, 13

RCW 29A.60.170(3) 4, 13

RCW 29A.60.185 ..... 4, 13

RCW 29A.60.235 ..... 4, 13

RCW 29A.68 14

RCW 34.05.570(2) 14

Regulations

WAC 434-250-110 9

WAC 434-250-120 9

WAC 434-250-130 9

WAC 434-260 9

WAC 434-261 9

WAC 434-261-010 ..... 4, 12-13

WAC 434-261-045 ..... 4, 13

WAC 434-261-120 ..... 4, 13

WAC 434-262-200 5

WAC 434-264 9

WAC 434-335 9-10

WAC 434-335-020 3

WAC 434-335-040 ..... 3- 4

WAC 434-335-090 3

Rules

RAP 16.2 ..... 2, 7

RAP 16.2(b) 7

RAP 16.2(c) 7

RAP 16.2(d) 7

RAP 17 7

Other Authorities

https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/ 6

https://www.sos.wa.gov/elections/research/Voting-Systems-by-County.aspx 5

https://www.sos.wa.gov/elections/research/voting-system-testing-and-certification.aspx 5

https://www.sos.wa.gov/elections/system-security.aspx 5

I. INTRODUCTION

Mr. Miller asks this Court to exercise its original jurisdiction to issue a writ of mandamus ordering the Secretary of State to: (1) eliminate electronic voting systems in Washington and require hand tabulation of ballots, (2) implement in-person voting with fingerprint verification, and (3) require "bipartisan groups" (rather than election officials) to process and tabulate ballots, all for the 2018 general election and future elections.

As a matter of law, Mr. Miller has failed to allege any claim for which an order of mandamus would be appropriate. This Court may issue a writ of mandamus to compel a state officer to perform a nondiscretionary act that the law clearly requires as part of the official's duties. The Secretary of State's decision to adopt regulations ensuring the security and accuracy of Washington's elections, including certification of certain voting and tabulation systems, is discretionary, and thus not subject to mandamus or prohibition. Moreover, state law expressly authorizes using electronic voting and tabulation systems with appropriate safeguards, state law requires mail-in voting with signature match verification, and state law requires that ballot processing and tabulation must be conducted by election officials. Therefore, mandamus cannot lie.

In addition, to the extent Mr. Miller believes that the Secretary of State has adopted election regulations that are unconstitutional or beyond

the agency's statutory authority, he has other remedies at law to solve this alleged problem, making mandamus inappropriate.

Mr. Miller may wish to change Washington's election statutes, but that is the legislature's prerogative. Mr. Miller's original action cannot proceed and his petition should be dismissed under RAP 16.2.

II. ISSUES

1. As a matter of law, is Mr. Miller entitled to an extraordinary writ of mandamus against the Secretary of State where he shows no failure to perform a clear, nondiscretionary duty and his requested remedies conflict with state law?

2. Is there another adequate remedy at law that Mr. Miller can exercise, making a writ of mandamus inappropriate?

III. STATEMENT OF THE CASE

A. Washington's System for Ensuring Election Security and Accuracy

Unlike many states, Washington has a paper-based ballot system because Washington votes by mail. *See* RCW 29A.40.010, .091. Even where a person chooses to vote on a disability access voting unit at a county's in-person voting center, a paper record of each vote is printed so that the voter can verify their votes. RCW 29A.40.160; RCW 29A.12.085, .150.

Washington ensures that only registered voters will vote by verifying the signature attesting to the voter's oath on the ballot envelopes. Election officials check each signature against the signature on file in the voter registration database. *See* RCW 29A.40.091, .110(3). Where signatures do not match, the voter is notified, and if they do not provide a matching signature, the ballot is rejected. RCW 29A.60.165(2). A matching signature or identification is also required to vote in person at a voting center. RCW 29A.40.160(7).

Each county must use only voting and tabulation systems that have been certified by federally-approved, independent testing labs. RCW 29A.12.040, .080(5). Systems are also tested and approved at the state level. RCW 29A.12.010, .020, .050. Voting and tabulation systems must be approved by the Secretary of State and a state certification board comprised of people with expertise in election systems, technology, and accessibility for people with disabilities. RCW 29A.12.080, .101; WAC 434-335-020, -040, -090.

Before every election, counties must perform logic and accuracy testing on their tabulation equipment in the presence of Secretary of State staff. RCW 29A.12.130. The public can observe this testing. RCW 29A.12.130. Ballot processing and tabulation are conducted at centralized ballot counting centers in each county, and the public can

observe as long as they follow security rules. RCW 29A.40.100; RCW 29A.60.170; WAC 434-261-010. Official party observers can call for a random check of ballot counting equipment during processing and tabulation if they choose. RCW 29A.60.170(3).

Once tabulation is complete, the county auditor must prepare and make publicly available detailed reports that precisely reconcile the number of ballots received, counted, and rejected, including specific accounting for various ballot types (for example, provisional ballots). RCW 29A.60.235. In addition, election officials conduct audits, randomly selecting precincts and races and comparing a hand count with the vote totals from the tabulator. RCW 29A.60.185.

Only election officials, their employees, and those authorized by the county auditor can touch any ballot, ballot container, or vote tabulation system. RCW 29A.12.120; WAC 434-261-010. Ballots, voting machines, and tabulation equipment must be physically secured at all times, strategies like video cameras and uniquely numbered seals are used to detect improper access, all access is logged (including seal numbers), and no election official is permitted to be alone with a container of ballots. RCW 29A.40.110(2), .160(13); RCW 29A.60.125; RCW 29A.12.110; WAC 434-261-045, -120. Tabulation equipment cannot be connected to the internet or capable of wireless communication. WAC 434-335-040.

After the election, ballots are stored securely for at least 60 days, and longer for a federal election. RCW 29A.60.110; 52 U.S.C. § 20701; WAC 434-262-200. After tabulation is complete, only the canvassing board can access ballots, and only in four specific circumstances: "[1] as part of the canvass, [2] to conduct recounts, [3] to conduct a random check under RCW 29A.60.170 . . . or [4] by order of the superior court in a contest or election dispute." RCW 29A.60.110.

Election security has always been a matter of nationwide concern, but since the 2016 election, public focus has increased. The Secretary of State has been working closely with the Department of Homeland Security and with county auditors to ensure there is no tampering with Washington's election systems. Information about Washington's ongoing security efforts is posted for the public to view on the Secretary of State's website: https://www.sos.wa.gov/elections/system-security.aspx. The Secretary of State has also posted the list of voting systems certified for use in Washington State, as well as a list of systems used by each county. https://www.sos.wa.gov/elections/research/voting-system-testing-and-certification.aspx; https://www.sos.wa.gov/elections/research/Voting-Systems-by-County.aspx. In addition, the federal Election Assistance Commission has posted all accredited voting systems as well as documentation about

their accreditation process. https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/.

B. Mr. Miller's Petition for Writ of Mandamus

Mr. Miller, apparently concerned about election security, brought a petition for a writ of mandamus in Okanogan County Superior Court asking the court for the same relief requested here. *Miller v. Wyman*, Okanogan County Superior Court Cause No. 18-2-00370-24, Pet. at 23-24. Without calling for an answer from the Secretary of State, the Superior Court dismissed the petition without prejudice. *Miller v. Wyman*, Okanogan County Superior Court Cause No. 18-2-00370-24. Mr. Miller then sought a writ imposing the same relief through a new petition filed directly in this court.

Mr. Miller requests that this Court require the Secretary of State to:

(1) Stop using electronic voting machines in Washington, and require hand tabulation of ballots (Req. for Remedy Nos. 1, 3, 6);

(2) Verify voter identity and qualification to vote in person (Req. for Remedy Nos. 2, 4, 5);

(3) Implement an "unbroken bipartisan chain of custody" where "bipartisan groups" conduct elections, rather than county election officials, including verifying the qualifications of each voter, performing tabulation,

and transporting tallies to the "state tabulator." (Req. for Remedy Nos. 6, 7, 8, 9). *See* Pet. for Writ of Mandamus at 23-24.

IV. ARGUMENT

Under RAP 16.2, a petition originating an action in the Washington Supreme Court is first evaluated by the Commissioner or Clerk. RAP 16.2(b), (d). The petition is treated as a motion, and RAP 17 governs the procedure for the hearing and decision on the petition. RAP 16.2(c). The Commissioner or Clerk will "determine if the petition should be decided by the Supreme Court, transferred [to the superior court], or dismissed." RAP 16.2(d)

The Secretary of State respectfully requests that the Commissioner or Clerk dismiss Mr. Miller's petition because he fails to state a claim upon which relief can be granted, and no development of fact can cure the petition's legal defects.

A. Mr. Miller Has Not Met the Strict Requirements for Showing That an Extraordinary Writ Is Appropriate

A writ of mandamus is an extraordinary remedy available "only to compel an official to do a nondiscretionary (i.e., 'ministerial') act" pursuant to a mandatory duty. *City of Seattle v. McKenna*, 172 Wn.2d 551, 555, 259 P.3d 1087 (2011). "A mandatory duty exists when a constitutional provision or statute directs a state officer to take some course of action." *Brown v.*

Owen, 165 Wn.2d 706, 724, 206 P.3d 310 (2009). A writ of mandamus will not be issued in anticipation of some future failure to perform a duty—"it must appear that there has been an actual default in the performance of a clear legal duty then due at the hands of the party against whom relief is sought." *Walker v. Munro*, 124 Wn.2d 402, 409, 879 P.2d 920 (1994). (internal quotation marks omitted). Mandamus is available only when there is no plain, speedy, and adequate remedy at law. *Staples v. Benton County*, 151 Wn.2d 460, 464, 89 P.3d 706 (2004).

Thus, in order to justify a writ of mandamus here, Mr. Miller must show that the Secretary of State has actually defaulted on a clear legal duty that "'leave[s] nothing to the exercise of discretion or judgment.'" *SEIU Healthcare 775NW v. Gregoire*, 168 Wn.2d 593, 599, 229 P.3d 774 (2010) (quoting *State v. City of Seattle*, 137 Wash. 455, 461, 242 P. 926 (1926)). He must establish the Secretary has a clear legal duty under a statute or the constitution: to require elimination of electronic voting and tabulation systems; to require in person verification of registered voters' qualification to vote; and to require ballot tabulation by bipartisan groups rather than election officials.

The Secretary of State has no clear legal, ministerial duty to do any of these things, nor has she violated a clear legal duty related to the 2018 election. The legislature has granted the Secretary broad discretion to

develop regulations to ensure election accuracy and security, and in fact, Mr. Miller's requested remedies would violate state election law.

1. The Secretary has discretion to adopt rules that ensure secure and accurate ballot processing and tabulation

Washington law gives the Secretary of State significant discretion in developing regulations to ensure election security and accuracy. The Washington legislature has specifically delegated to the Secretary of State the authority, as the state's chief election officer, to make reasonable rules for the orderly, timely, and uniform conduct of elections. RCW 29A.04.611. The Secretary must create rules establishing standards and procedures "to ensure the accurate tabulation and canvassing of ballots," "to prevent fraud," to ensure the security of ballots, and to "guarantee the secrecy of ballots" in all circumstances. RCW 29A.04.611(9), (11), (13), (33), (34), (39). The Secretary has exercised her discretion to do just that by adopting numerous regulations that ensure secure and accurate ballot processing and tabulation. *E.g.*, WAC 434-250-110 (processing ballots), -120 (signature verification), -130 (audit trail); WAC 434-260 (election review process); WAC 434-261 (counting and tabulation procedures); WAC 434-264 (recount procedures); WAC 434-335 (testing and certification of voting systems).

The development of these election regulations falls squarely within the discretion that the legislature granted to the Secretary, and mandamus cannot require her to exercise her discretion differently. *See SEIU Healthcare 775NW*, 168 Wn.2d at 599, (quoting *City of Seattle*, 137 Wash. at 461).

2. Washington law permits electronic tabulation of ballots with mandated safeguards, as well as voting on voting machines with a paper ballot printout

Rather than mandate only hand tabulation of ballots, Washington law expressly allows counties to use electronic tabulation equipment. Washington law also mandates at least one electronic voting unit in each county to provide access to individuals who are blind or visually impaired, enabling them to vote with privacy and independence.

Washington law expressly allows electronic vote tabulation systems, so long as the system has been approved under RCW 29A.12. RCW 29A.12.010. The law also mandates specific safeguards to ensure accuracy. *See, e.g.*, RCW 29A.12; WAC 434-335. A writ ordering that counties hand count ballots would directly contradict this legislative authorization.

Further, each county must make available at least one electronic voting machine, certified by the secretary of state, that provides access to people who are blind or visually impaired. RCW 29A.40.160(4). Such

devices must produce a paper record of each vote that the voter can then review for accuracy, and which must be retained for tabulation. RCW 29A.12.085, .150. While Mr. Miller seeks an order from this court eliminating the use of these electronic voting machines, Pet. at 23, doing so would directly contradict a requirement in state law and improperly hinder access for visually impaired voters.

Mr. Miller is not entitled to a writ ordering the Secretary of State to stop using electronic voting machines or to require hand tabulation of ballots. Pet. at 23-24 (Req. for Remedy Nos. 1, 3, 6). The Secretary has no mandatory duty under the law to impose such restrictions on counties, and in fact, the Secretary cannot prohibit something that the legislature has plainly and expressly authorized, so long as the statutory conditions are met. *See Brown*, 165 Wn.2d at 724.

3. Washington law requires mail-in ballots and voter verification through signature matching

Mr. Miller asks the court to order that a "bipartisan group" verify the identity and qualification of each person to vote. Pet. at 23-24 (Req. for Remedy Nos. 4, 5). He also insists on in-person voting. Pet. at 23-24 (Req. for Remedy No. 4). But Washington law expressly allows ballot return by mail. RCW 29A.40.010, .091.

Washington law also permits election officials to ensure that only registered voters have voted by verifying the voter's signature on the ballot envelope. *See* RCW 29A.40.091. Election officials check each signature against the signature on file in the voter registration database. *See* RCW 29A.40.091, .110(3). A matching signature or identification is also required to vote in person at a voting center. RCW 29A.40.160(7). Where signatures do not match, the voter is notified, and if they do not provide a matching signature, the ballot is rejected. RCW 29A.60.165(2). Nothing in Washington's vote by mail statutes allows the Secretary of State to suddenly require in-person voting.

There is no mandatory duty that the Secretary require counties to cease acceptance of mailed ballots. Nor is the Secretary authorized to permit "bipartisan groups" to vet the qualifications of voters attempting to vote. Absent a mandatory duty requiring the Secretary to impose Mr. Miller's proposed limitations, this Court cannot use its mandamus power to order her to do so. *See Walker*, 124 Wn.2d at 409.

4. Washington law requires a strict chain of custody for ballots that does not allow anyone other than election officials to tabulate or handle ballots

Finally, even though members of the public can observe ballot processing and tabulation, Washington law expressly forbids people other than election officials to handle or tabulate ballots.

Only election officials, their employees, and those authorized by the county auditor can touch any ballot, ballot container, or vote tabulation system. RCW 29A.12.120; WAC 434-261-010. Ballots, voting machines, and tabulation equipment must be physically secured at all times, and counties use security precautions like video cameras and uniquely numbered seals to detect improper access. RCW 29A.40.110(2), .160(13); RCW 29A.60.125; RCW 29A.12.110; WAC 434-261-045, -120.

While Mr. Miller asks this Court to mandate that "bipartisan groups" perform tabulation and transport tabulation results by hand to the Secretary of State, Washington law does not permit people who are not election officials, their employees, and those authorized by the county auditor to touch any ballot, much less tabulate ballots by hand. *See* Pet. at 23-24 (Req. for Remedy Nos. 6-9); RCW 29A.12.120; WAC 434-261-010. Nor does state law require existing election officials and employees to be checked for bipartisanship. Instead state law includes significant safeguards to prevent individuals from being able to tamper with election results, and to ensure any attempted tampering is detected. *E.g.*, RCW 29A.40.100; RCW 29A.60.170; WAC 434-261-010 (public observation); RCW 29A.60.170(3) (random checks of ballot counting equipment); RCW 29A.60.235 (detailed reconciliation reports); RCW 29A.60.185 (random audits). There is no mandatory duty that the Secretary require

"bipartisan groups" to tabulate ballots or otherwise participate in ballot processing or tabulation.

Absent a mandatory duty, this Court cannot issue a writ of mandamus against a state officer. Mr. Miller has not identified a mandatory duty with which the Secretary of State has failed to comply.

B. Washington Law Provides Other Mechanisms for Mr. Miller to Challenge Secretary of State Regulations

Mr. Miller appears to argue, in part that, Washington's election regulations are unconstitutional or the result of administrative overreach. *See* Pet. at 1 (citing Const. art. I, § 19 requiring free and equal elections). But mandamus is available only when there is no plain, speedy, and adequate remedy at law. *Staples*, 151 Wn.2d at 464. There are other ways to challenge the validity of a Washington regulation, short of a writ of mandamus. For example, the Administrative Procedure Act provides a mechanism for a challenge if a person believes a regulation is unconstitutional or outside of an agency's statutory authority. *See* RCW 34.05.570(2).

Moreover a writ of mandamus will not issue in anticipation of some future failure to perform a duty—"it must appear that there has been an actual default in the performance of a clear legal duty then due at the hands of the party against whom relief is sought." *Walker*, 124 Wn.2d at 409

(internal quotation marks omitted). Thus, mandamus would not be appropriate to address speculative harm that Mr. Miller thinks might occur in the 2018 general election. Instead, if a registered voter believes that there has been fraud or error in the course of an election, the proper remedy is to contest the election under RCW 29A.68. The election contest is the singular method for challenging an election. RCW 29A.68; *Reid v. Dalton*, 124 Wn. App. 113, 122, 100 P.3d 349 (2004).

Because these alternative remedies exist, even if Mr. Miller's allegations were correct (which they are not), mandamus would not be appropriate.

V. CONCLUSION

The Petition for Extraordinary Writ of Mandamus does not state a claim for relief because it does not identify any lawful basis for mandamus. The Secretary of State respectfully asks the Court to dismiss the petition with prejudice.

RESPECTFULLY SUBMITTED this 12th day of October, 2018.

ROBERT W. FERGUSON
Attorney General

s/ Rebecca R. Glasgow
REBECCA R. GLASGOW, WSBA 32886
Deputy Solicitor General

PO Box 40100
Olympia, WA 98504-0100
RebeccaR@atg.wa.gov
360-664-3027

CERTIFICATE OF SERVICE

I certify, under penalty of perjury under the laws of the state of Washington, that on this date I served a true and correct copy of the foregoing document via the United States Postal Service postage prepaid and electronic mail on the following:

James M. Miller
1 Blue Sky Place
Omak, WA 98841
jmiller@leader.com

DATED this 12th day of October 2018.

s/ Stephanie N. Lindey
STEPHANIE N. LINDEY
Legal Secretary

SOLICITOR GENERAL OFFICE

October 12, 2018 - 9:49 AM

Transmittal Information

Filed with Court:	Supreme Court
Appellate Court Case Number:	96235-9
Appellate Court Case Title:	James M. Miller v. Secretary of State, Kim Wyman

The following documents have been uploaded:

- 962359_Answer_Reply_20181012094657SC339624_6198.pdf
  This File Contains:
  Answer/Reply - Other
  The Original File Name was 8_SOS_Response.pdf

A copy of the uploaded files will be sent to:

- calliec@atg.wa.gov
- jimomak@leader.com
- sgoolyef@atg.wa.gov
- stephaniel1@atg.wa.gov

Comments:

Secretary of State Kim Wyman's Response to Petition for Writ of Mandamus

---

Sender Name: Kristin Jensen - Email: kristinj@atg.wa.gov
Filing on Behalf of: Rebecca R Glasgow - Email: rebeccag@atg.wa.gov (Alternate Email: RebeccaG@atg.wa.gov)

Address:
PO Box 40100
1125 Washington St SE
Olympia, WA, 98504-0100
Phone: (360) 753-4111

Note: The Filing Id is 20181012094657SC339624

Washington Examiner

Devin Nunes calls for ban on electronic voting systems

by Caitlin Yilek | July 26, 2018 09:38 AM

House Intelligence Committee Chairman Devin Nunes wants to ban electronic voting systems, calling them “really dangerous.”

"The one thing we've been warning about for many, many years on the intelligence committee is about the electronic voting systems," Nunes, R-Calif., told Hill.TV's Buck Sexton.

"Those are really dangerous in my opinion, and should not be used. In California ... at least in the counties that I represent, they do not use an electronic system," he added.

Electronic voting systems can be susceptible to hackers, so a paper trail is needed in case of a recount, Nunes said.

The head of cybersecurity at the Department of Homeland Security said in February that Russians successfully penetrated voter registration rolls in several states ahead of the 2016 presidential election. There has been no evidence that any of the registration rolls were changed, U.S. officials have said.

Congress has allocated $380 million in 2018 to fund election security in the states. House Republicans voted last week against including additional funding for election security grants to states in a spending bill, infuriating Democrats. Republicans argued that states already had plenty of funding from previous congressional allotments to upgrade election security.

U.S. Election Assistance Commission Commissioner Thomas Hicks told lawmakers Tuesday that about 75 percent of funding provided to states is going toward voter registration, cyber upgrades, and the purchase of new voting equipment.

Official website of the Department of Homeland Security

Secretary Kirstjen M. Nielsen's National Cybersecurity Summit Keynote Speech

Release Date: July 31, 2018

Introduction

Thank you Chris for that kind introduction, and for giving us a beautiful roadmap for everything we look to accomplish today.

It is my great honor and pleasure to welcome you here today, it's so wonderful when an idea with such passion actually comes to fruition, so it's very much a pleasure of mine to see you all here today.

We have a lot of serious threats to discuss today. Americans are worried about what our digital enemies might do…whether it is taking down the power grid…holding healthcare systems hostage…or the nightmare scenario: blocking access to the web the day a new TV show drops on Netflix. I often hear about this from folks that that keeps them up at night.

But I'd like to thank Secretary Perry, Director Wray, and General Nakasone, who will join me on stage in just a little bit, for bringing their expertise and leadership to this discussion as well. What you will see before you today is a true effort from the United States government, to work with the private sector, and academia to combat these threats.

I'd also like to Director Alles of the United States Secret Service who is here bringing his level of expertise, of course Under Secretary Krebs, and those of you in the audience, and who are watching from home so-to-speak, to the men and women from DHS, for everything you do to protect our country, thank you. And whether you represent government, industry, or academia, we are glad to have you on our team, and I want to thank you for your continued collaboration and for the time you're giving us today, and your future efforts to work with us as we look at these threats.

This afternoon, we will also have the pleasure of hearing from Vice President Pence. He will lay out how this Administration is strengthening cybersecurity across the board—and why we will be *relentless* against our cyber adversaries.

This event is the first of its kind. Today we are coming together—government leaders, CEOs, academics, and cyber experts—to send a message to these online threat actors: *Game. Over.* Our team is formed, our team is ready and we are ready to combat you wherever you might manifest your threat.

We are not waiting for the next intrusion before we act. We are taking a clear-eyed look at the threat and taking action—and notably, as Under Secretary Krebs mentioned—*collective* action to combat them.

And, that's truly the only way we'll win this struggle.

Today is a watershed moment, a chance for us to cement partnerships in order to protect our networks and repel digital invaders together.

Roadmap

This morning I'm going to give you a stark overview of the threat landscape. I won't sugar-coat it.

But I will also tell you how DHS and this Administration are fighting back.

And I'd like announce bold new efforts—starting *today*—that will make the digital infrastructure of our country more resilient.

The Threat

So let me give you the bottom line up front: we are facing an urgent, evolving crisis in cyberspace. Our adversaries' capabilities online are outpacing our stove-piped defenses.

In fact, I believe that cyber threats collectively now exceed the danger of physical attacks against us. This is a major sea change for my Department and for our country's security.

Indeed, most Americans go about their daily lives without fear of personal injury or harm from our adversaries. But our *digital* lives are now in danger every single day.

And these virtual threats can have very real-world consequences. When the bad guys can remotely turn off the lights, steal money from your bank account, and shut down emergency services, the impacts go far beyond our smartphone screens.

But don't get me wrong. Terrorists and criminals still pose a serious threat to our lives, we take this mission at DHS very seriously, and they are plotting against Americans daily; however, the "attack surface" in cyberspace is now broader and under more frequent assault.

This has forced us to rethink homeland security.

DHS was founded fifteen years ago to prevent another 9/11, but today I believe the next major attack is more likely to reach us online than on an airplane.

DNI Intelligence Dan Coats recently said that "the warning lights are blinking red" in cyberspace. I agree. Intruders are in our systems, they are seeking to compromise more of them every day, and they represent a very active threat to our digital security as a nation.

Every*one* and every*thing* is a target: individuals …industries …infrastructure …institutions … and our international interests. And the scope of the problem keeps getting wider.

The cyber-threat landscape is different today because cyberspace is not only a target. Cyber can also be used as a weapon, an attack vector, or a means for which nefarious activity can be conducted.

Today, our innovations can be stolen and used to diminish our prosperity…our infrastructure can be hijacked and used to hold us hostage…and our institutions can be compromised and used to undermine our democratic process.

Our smartphones and computers can be turned into bad-guy force multipliers without us even realizing it. Your compromised computer can become part of the bot army. Or your CPU power can be commandeered to steal Bitcoin to finance a rogue regime.

I wish I could tell you that we've rounded a corner. But last year was the worst-ever in terms of cyberattack volume. The headlines seemed never-ending, and not to be the Debby Downer but I think continue to see them this year.

Nearly half of all Americans had sensitive personal information exposed online in 2017. But that wasn't the *total* for 2017. That resulted from a *single breach,* when cybercriminals hacked a major credit bureau.

We witnessed North Korea's WannaCry ransomware spread to more than 150 countries, which held healthcare systems hostage and brought factories to a halt.

And we saw Russia probing our energy grid, compromising thousands of routers around the world, and unleashing NotPetya malware, which wreaked havoc and ended up being one of the costliest cyber incidents in history.

These incidents, though, are only the beginning. Rogue regimes and hostile groups are probing critical systems worldwide every moment as we speak. And without aggressive action to secure our networks, it is only a matter of time before we get hit hard in the homeland.

It's not just risks to our prosperity, privacy, and infrastructure we have to worry about.

Our democracy itself is in the crosshairs. Let me take just a moment to touch on these because I think it's important to do so.

Two years ago, as we all know, a foreign power launched a brazen, multi-faceted influence campaign to undermine public faith in our democratic process and to distort our presidential election.

That campaign was multifaceted and involved cyber espionage, leaks of stolen data, cyber intrusions into voter registration systems, online propaganda, and more.

Let me be clear: Our intelligence community had it right. It was the Russians. We know that, they know that. It was directed from the highest levels. And we *cannot* and *will not* allow it to happen again.

Although NO actual votes were changed in 2016, let me be clear in this, ANY attempt to interfere in our elections is a direct attack on our democracy, it is unacceptable, and it will not be tolerated.

Mark my words: America will not tolerate this meddling.

Key Challenges

So it's clear that we are in a tough fight right now. The cybersecurity headwinds are against us. I could talk about this all day but let me give you a few examples.

First, increased connectivity has led to increased systemic risk.

There's no getting around it. The wider and deeper the web gets, the more vulnerable we become.

The "internet of things"—which is really now the "internet of *everything*"—has compounded the problem by giving cyber criminals a direct route onto our doorsteps and into our homes.

Wherever and whenever you are connected to the internet, you are unlocking doors and windows you may not even be aware of to let the bad guys in.

What's more, our growing digital dependence means that vulnerabilities can have widespread, unpredictable, and cascading consequences when they are exploited.

Whether it's common tools such as GPS or payment systems, everything is closely intertwined.

An attack on a single tech company, for instance, can rapidly spiral into a crisis affecting the financial sector, the energy grid, water systems, or the healthcare industry.

Secondly, our cyber rivals are getting more sophisticated.

Several years ago, a cyber-intrusion by a foreign adversary might be similar to a sloppy home break-in. The window would be broken, furniture would be overturned, and missing jewelry would be a dead giveaway that someone had been in your house— that you had been hit.

But they are getting savvier. Now when you get home, the door is still locked, and your house appears exactly as you left it. But no, in reality, the intruder has been inside for hours, perhaps days and weeks, and will remain in hiding, waiting for the right moment to strike.

That's what we're up against.

So, to prevent cyber intrusions today, we don't just need an alarm system. Or a neighborhood watch. Or security cameras. Or armed guards constantly roaming the hallways. We need it *all.*

Third, similar to the pre-9/11 days, and this is where we'll focus today, we still have trouble "connecting the dots."

Between all of us—government, the private sector, and individuals—we *do* have the data to disrupt and prevent cyberattacks.

But we aren't sharing fast enough or collaborating deeply enough to make it happen.

This is partly because we are operating in a legal and operational paradigm designed for a different era—long before brand-name breaches could threaten to cripple entire industries.

We still have the walls up and we still have stovepipes, and we still have sidewalks.

How We Are Responding

So what are we doing about it?

First and foremost, let me say this: *we are replacing complacency with consequences*. To deter bad behavior, you have to punish it. And we cannot wait for "the big one" to do just that.

Our adversaries have the capability to destroy. So we cannot afford to bide time as they prep the battlefield and identify our hidden digital evacuation routes or try to outmaneuver us. We must act now.

That starts with calling out the offenders. Whether it is the North Koreans or the Russians, we are identifying countries that have compromised our systems or have unleashed destructive malware.

And we are imposing costs—whole of government costs, diplomatically, financially, legally, and through other means.

The United States possesses a wide range of response options—some of them seen, and some unseen—and we will no longer hesitate to use them to hold foreign adversaries accountable and to deter cyber hostility.

Let me also again take this opportunity today to issue a warning, as I have in other speeches, to any foreign power that would consider meddling in our networks or in the affairs of our democracy: *The United States will no longer tolerate your interference. You will be exposed. And, you will pay a high price.*

Second, we are changing our posture and setting course to confront systemic risk head on.

Traditionally, DHS, and our sector specific agencies, has focused primarily on protecting individual "assets," companies, individual systems or "sectors." But now we are looking more across government, across sectors, across government-private, at those nationally critical "functions." What are they? These are the lifeblood of our economy, of our national security, and of our day-to-day lives.

We must identify single points of failure, concentrated dependencies and interdependencies that can create those ripple effects across sectors.

To do this, we are launching voluntary supply-chain risk management programs. Under Secretary Krebs will talk about that later. And we are partnering with companies to hunt down unseen security weaknesses and to limit our attack surface.

I urge you to join us and lend your expertise to these efforts.

Third, we are reorganizing ourselves for a new fight.

I am working with Congress to pass legislation to establish the Cybersecurity and Infrastructure Security Agency within DHS.

This would recast what is now NPPD, or the National Protection and Programs Directorate—our cybersecurity arm—into an ambitious operational agency capable of better confronting digital threats.

But we all know that waiting for Congress to act is like waiting for a new Game of Thrones book to come out. You really, really want it—but you don't hold your breath.

So in the meantime we are taking other steps—including one that I will announce today—to make sure we keep up and stay ahead of our online adversaries.

This also includes dramatically ramping up efforts to protect our election systems, including through a new Elections Task Force and deploying a *vast* array of services, programs, and partnerships nationwide to help our partners secure our election infrastructure.

Finally, we are embracing a "collective defense" posture.

As I've said many times before, in a hyper-connected world, and as Chris mentioned in his introduction, *your* risk is now *my* risk and *my* risk is *your* risk. Each of us is on the frontlines of the digital battlefield, so we must work together to protect ourselves.

Any of us could be the weak link that not only allows adversaries to infect our systems but allows them to use our systems to spread further into others.

The adversary's approach is like a flood. It will find every crack, crevice, and seam. Even if I place sandbags around my house to prepare for the flood, if my neighbors don't do it too, my house will be underwater.

Collective defense calls for *all of us* to use sandbags, if you will—to optimally configure our systems, to employ patch management, to share, receive, and act on threat indicators.

To that end, DHS is improving and expanding our information-sharing programs, including those focused on sharing threat indicators.

And we are developing novel ways for government and industry to collaborate to identify threats before they hit our networks and to respond more quickly and effectively to incidents, which we will discuss throughout the day.

Taking the Next Step & Call to Action

We've made a lot of progress. But it's simply not enough.

We must move beyond routine information sharing. And we must do better at teaming up with the private sector to combat our common enemies in cyberspace—to understand their goals, to understand their actions, to understand the operational effects and implications of their intrusions, manipulations, and disruptions.

As we all here know, the majority of U.S. infrastructure is owned and operated by the private sector—not the government.

So we must be working to enable those in this room—across industries—to better defend your systems and our critical functions.

For far, far too long we have lacked a single focal point to bring government agencies and industry together to assess the digital dangers we face—and to counter them…a place where analysts and network defenders can address these risks *together* through the full myriad of mission sets when we address cyber.

I am pleased to announce that we are going to change that.

This week the Department of Homeland Security is launching the National Risk Management Center—an initiative driven by industry needs and focused on fostering a cross-cutting approach to defend our nation's critical infrastructure.

It will employ a more strategic approach to risk management borne out of the re-emergence of nation-state threats, our hyperconnected environment, and our survival and its need to effectively and continually collaborate with the private sector.

So what does that actually mean in practice?

Housed at DHS, the Center will bring together government experts with willing industry partners so that they can influence how we support them. Our goal is to simplify the process—to provide a single point of access to the full range of government activities to defend against cyber threats.

I occasionally still hear of companies and locals that call 9-1-1 when they believe they've been under a cyberattack, the best thing to do would be to call this center. This will provide that focal point, we will work with our partners in government who will be on stage today, and others, to provide you what you need to help repel, to help mitigate, to root out the adversary from your systems.

We will be able to take a piece of intelligence, and with the help of the private sector, ask ourselves "so what," and determine what we're going to do about it—together.

These days, cyber threat data is like a puzzle piece, for those of you when you started to begin a puzzle with your children and they pick up a puzzle piece, the first question is, “what puzzle does that puzzle piece belong to?” Having the private sector with us will help us to determine what puzzle it belongs to, and then determine how it fits into the puzzle so we can see the trend, we can see the thread, and we can see the purpose, perhaps, of the attack, but certainly the implications and effects. So this is where the expertise of the private sector comes in, to help us contextualize the threat both in the planning phase as well as in the response and recovery. The private sector also knows its operational environment better than we will ever know in the government, so we will look to their expertise to help us understand how the pieces fit together.

So, we will welcome industry experts, side-by-side with ours, to break down the silos and engage daily to develop actionable solutions to defend our critical infrastructure.

We will begin with a tri-sector model focusing on financial services, telecommunications, and energy sectors.

We will push this effort forward in 90-day “sprints” starting immediately to identify key priorities and to conduct joint risk assessments. And we will have a major cross-sector exercise this fall.

We will look to you to influence how we can support you best…to help us tailor our assessments, plans, and playbooks that you can then action.

As I often say from a Department with myriad missions – let’s do what we do best and partner with you to do the rest.

But time is not on our side. So we are moving quickly. I ask all of you to consider working with us to develop the Center and deepen engagement so that we can fortify our defenses.

I would also ask that everyone here—whether you are from a federal agency, a Fortune 500 company, a think tank, or a university—identify at least one new actionable, operational way you can contribute to our nation’s collective cyber defense.

That’s why we are here today. Think about it now. Think about it throughout the day. Commit to it this afternoon. And follow through on it when you leave.

We don’t put together summits to keep admiring all the problems. We do it to solve them.

Our adversaries are crowdsourcing attacks, and today I am pleased to say we will crowdsource our response.

Closing

I am sure I speak for my colleagues when I say we do not take your presence here lightly. We appreciate your time, your efforts, your commitment, your leadership, and we thank you for being here. And we hope to enlist your continued efforts in this fight if you're not already in it with us.

Our digital enemies are taking advantage of all of us. They are exploiting our open society to steal, to manipulate, to intimidate, to coerce, to disrupt, and to undermine. They are using our interconnectedness to attack us—but let's use the fact that we are all connected *to our advantage.*

As I noted at the beginning, we are in crisis mode—the "Cat 5" hurricane has been forecast. And now we must prepare.

That leaves us with a choice: admit defeat and assume that our devices and networks will always be compromised—OR respond decisively and dramatically in order to restore security and resiliency to the web. If we prepare individually, we will surely fail collectively.

You're here today because you believe in working together with clear-eyed urgency. And together, I have no doubt we will turn the tide. So thank your attendance today, thank you for your participation, we look forward to many conversations to come, and we look at the end of the day to announce some very tangible actions that we will agree to throughout the day. So thank you very much and again thank you for joining us at this summit.

Topics: Cybersecurity (/topics/cyber-security) , Secretary of Homeland Security (/topics/secretary-homeland-security)

Keywords: Cybersecurity (/keywords/cybersecurity)

Last Published Date: August 22, 2018

Presidential Advisory Commission on Election Integrity

July 13, 2017 | 5 minute read

On May 11, 2017, President Donald J. Trump signed an Executive Order establishing the Presidential Advisory Commission on Election Integrity. Vice President Mike Pence chairs the Commission, and Kansas Secretary of State Kris Kobach serves as the vice chair.

Please check back regularly for further updates regarding the Commission and its future meetings and agendas.

Statements & Releases

MAY 2017

- President Announces Formation of Bipartisan Presidential Commission on Election Integrity (5/11/2017)

JUNE 2017

- Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (6/28/2017)

JULY 2017

- Statement from Kris Kobach, Kansas Secretary of State and Vice Chair of the Presidential Advisory Commission on Election Integrity (7/05/2017)
- Remarks by President Trump and Vice President Pence at the Presidential Advisory Commission on Election Integrity Meeting (7/19/2017)
- Remarks by Vice President Pence and Elected Officials at the First Meeting of the Presidential Advisory Commission on Election Integrity (7/19/2017)

AUGUST 2017

- Announcement of September 12, 2017 Meeting in New Hampshire (8/24/2017)

Commission Members

- Vice President Mike Pence, Chair
- Kris Kobach, Secretary of State of Kansas, Vice-Chair
- Connie Lawson, Secretary of State of Indiana
- Bill Gardner, Secretary of State of New Hampshire
- Matthew Dunlap, Secretary of State of Maine
- Ken Blackwell, Former Secretary of State of Ohio
- Christy McCormick, Commissioner, Election Assistance Commission
- David Dunn, Former Arkansas State Representative
- Mark Rhodes, Clerk of Wood County, West Virginia
- Hans von Spakovsky, Senior Legal Fellow and Manager of Election Law Reform Initiative, Edwin Meese Center for Legal & Judicial Studies, The Heritage Foundation
- J. Christian Adams, President and General Counsel, Public Interest Legal Foundation
- Alan King, Probate Judge, Jefferson County, Alabama

Meetings

- Meeting Notice for September 12, 2017 Meeting
- Updated Agenda for September 12, 2017 Meeting (With Clerical Change to Presenter Title)

This meeting will be livestreamed for remote viewing at the following link: https://www.youtube.com/watch?v=l93GoVJTR5Q. Please be advised that this link WILL NOT be live BEFORE 10 a.m. EST on Tuesday, September 12.

Press Credentials for September 12, 2017 Meeting in New Hampshire

To request Press credentials for the September 12, 2017 meeting of the President's Advisory Commission on Election Integrity at the New Hampshire Institute of Politics (NHIOP) at Saint Anselm College, Please submit the form at this link: http://www.anselm.edu/Academics/Institutes-Centers-and-the-Arts/NH-Institute-of-Politics/Election-Integrity-Request-for-Press-Credentials.htm. Due to limited physical space, the NHIOP will do its best to accommodate all requests, however a request for credentials does not guarantee approval of credentials.

The Advisory Commission's meeting will be livestreamed for remote viewing as well as at the NHIOP. Journalists' assignments within the NHIOP, including potential access to the Advisory Commission meeting room, will be determined upon a final configuration of table, seating and equipment requirements for Commission members, panelists, witnesses and elected officials.

You will be notified of approval prior to the event along with additional instruction for directions, parking, etc.

Commission Documents

- Commission Charter
- Federal Register Notice – Meeting Announcement
- Meeting Agenda

- Revised Meeting Agenda
- Meeting Materials
- Public Documents

Any member of the public wishing to submit written comments for the Commission's consideration may do so at any time at www.Regulations.gov via the Federal eRulemaking portal at the following link: https://www.regulations.gov/document?D=GSA-GSA-2017-0002-0180. Click "Comment Now" and then follow the instructions provided. Please include your name, organization (if any), and the notice number on your attached document. Please note that any information, including personal or contact information, that you provide on the www.Regulations.gov comment form or in an attachment will be publicly disclosed as it is entered, searchable on the Internet, and included in any paper docket. Commenters may also choose to remain anonymous.

Public comments may also be submitted via mail. Please address public comments to: Presidential Advisory Commission on Election Integrity, 1650 Pennsylvania Avenue, NW, Eisenhower Executive Office Building (EEOB), Rm. 268, Washington, D.C. 20504. Please note that any written comments received via mail will be uploaded to the docket on www.Regulations.gov, where they will be viewable in full by the public, including any personal or contact information. The Commission values public comments and input.

Please check back soon for further updates regarding the Commission and its future meetings and agendas.

Mission

Pursuant to Executive Order 13799, the Commission shall, consistent with applicable law, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President that identifies the following:

(a) those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections;

(b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and

(c) those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting.

STATEMENTS & RELEASES

Statement by the Press Secretary on the Presidential Advisory Commission on Election Integrity

Issued on: **January 3, 2018**

★ ★ ★

Despite substantial evidence of voter fraud, many states have refused to provide the Presidential Advisory Commission on Election Integrity with basic information relevant to its inquiry. Rather than engage in endless legal battles at taxpayer expense, today President Donald J. Trump signed an executive order to dissolve the Commission, and he has asked the Department of Homeland Security to review its initial findings and determine next courses of action.

Americans for Innovation™

To ensure you are reading the latest post, click the logo above.
SEARCH by topic, keyword or phrase. Type in Custom Search box e.g. "IBM Eclipse Foundation" or "racketeering"

Custom Search

Saturday, September 15, 2018

HILLARY CLINTON CONTROLS 50,000 FBI ENCRYPTION KEYS—PROVES MUELLER'S WITCH HUNT IS TREASONOUS

With these encryption keys, nothing in our digital lives is off limits to the Clinton's and their conspirators

President Trump's new executive order can be sabotaged with these keys; alternatively, he can use the order to prosecute these criminals

Many foreign powers have conspired with the SES and their Queen's Privy Council overlords since before 1993

CONTRIBUTING WRITERS | OPINION | *AMERICANS FOR INNOVATION* | SEP. 16, 2018, UPDATED OCT. 01, 2018 | PDF | https://tinyurl.com/y9yhgksg

DEEP STATE SHADOW GOVERNMENT POSTER

Member

Harvard | Yale | Stanford Sycophants

Bookmark: #stand-with-roger-stone

ROGER STONE SPEAKS: On Nov. 18, 2017, Twitter censored *New York Times* best-selling author Roger Stone completely. Every red-blooded American should be outraged, Republican, Democrat and Independent alike. If Roger's voice is silenced today, yours is next. We must *break* this embargo. Click here to read and share Roger's latest perspectives on the Battle for our Republic, including his responses to his critics (who have not been censored).

Updated Sep. 26, 2018.

CLICK HERE TO SEE COMBINED TIMELINE OF THE HIJACKING OF THE INTERNET

PAY-to-PLAY NEW WORLD ORDER

This timeline shows how insiders sell access & manipulate politicians, police, intelligence, judges and media to keep their secrets

Clintons, Obamas, Summers were paid in cash for outlandish speaking fees and Foundation donations. Sycophant judges, politicians, academics, bureaucrats and media were fed tips to mutual funds tied to insider stocks like Facebook. Risk of public exposure, blackmail, pedophilia, "snuff parties" (ritual child sexual abuse and murder) and Satanism have ensured silence among pay-to-play beneficiaries. The U.S. Patent Office is their toy box from which to steal new ideas.

Fig. 1—Hillary Clinton has all of our encryption keys, including the FBI's. "Encryption keys" is a general reference to several encryption functions hijacked by Hillary and her surrogate ENTRUST. They include hash functions (used to indicate whether the contents have been altered in transit), PKI public/private key infrastructure, SSL (secure socket layer), TLS (transport layer security), the Dual_EC_DRBG NSA algorithm (Dual Eliptical Curve Deterministic Random Bit Generator) and certificate authorities. The convoluted structure managed by the gutless agency chief information officer "Federal Common Policy" group says it has "hundreds" of certificate authorities, but this is a material lie. They have ceded "Root" authority (the *basis* of the X.509-based public key infrastructure) to key companies like ENTRUST INC, including the ability to sublicense their authority to third parties who in turn manage entire other networks (cross-certificates, subordinate certificates, Bridge certificate authorities) in a Gordian knot of incestuous commercial relationships clearly designed to fool the public to hide their devilish criminality. All roads lead back to Hillary and the Rose Law Firm.

AFI (Nov. 06, 2015). Complicit encryption geeks enable the American spy state. *Americans for Innovation*.

AFI (Nov. 25, 2015). Dell and Lenovo (IBM) ship computers with spy state backdoors. *Americans for Innovation*.

https://youtu.be/-zWWJ1BzKgI | (Raw *.mp4 video file—use if the YouTube version is censored).

Click here to read a list of just some of the *"more than 2000 organizations in 60 different countries"* for which Hillary has backdoor encrytion keys. Source: ENTRUST 10-K Annual Reports (1998-2009). SEC Edgar. Annual reports from 1998 to 2009 and selected other filings.

1999 | 2000 | 2001 | 2002 | 8-K. FBI Contract Press Release (Oct. 29, 2003) | Jones' Stock Options (Dec. 05, 2003) | 2003 | Co. Overview (2003) | Jones' Signature (Dec. 23, 2003) | Jones' Bio (Mar. 15, 2004) | 2005 | 2006 | 2007 | 2008 | 2009 | 2009A | Relationships (1998-2009)

Graphic: The Judiciary Report.

DECIPHERING HILLARY'S ENCRYPTION KEYS THAT HAVE KEPT HER ONE STEP AHEAD OF THE SHERIFF

SPECIAL NOTICE: *This post is a work in progress. You are encouraged to return to pick up additional evidence as it is added.* Indictable evidence continues to pour in for use by prosecutors, alternative media, Treasury, U.S. Marshalls and military tribunals. These criminals have relied on the fact that encryption, cryptography and cryptanalysis is a field of esoteric mathematics for which the average person has little interest. Hopefully, that will now change.

Cryptography—the use of codes and ciphers to protect secrets—began thousands of years ago. Until recent decades, it has been the story of what might be called classic cryptography — that is, of methods of encryption that use pen and paper, or perhaps simple mechanical aids. In the early 20th century, the invention of complex mechanical and electromechanical machines, such as the Enigma rotor machine, provided more sophisticated and efficient means of encryption; and the subsequent introduction of electronics and computing has allowed elaborate schemes of still greater complexity, most of which are entirely unsuited to pen and paper.

In a simple form, simply scrambling the letters in a word is a basic form of cryptography. HELLO might become OLHEL or LEHLO. In more sophisticated approaches, look up tables contain readable words in the first column and a

G+

CONGRESS CONTACT LOOKUP

Contacting the Congress

= Universal Toxic Substance Symbol & Warning

FINANCIAL HOLDINGS OF OBAMA POLITICAL APPOINTEES, BY AGENCY

FOLLOW BY EMAIL

Email address... Submit

BLOG ARCHIVE

▼ 2018 (16)

▼ September (1)

replacement word in the second. The resulting message looks like jibberish until the look up table is used by the recipient. The public key infrastructure and certificate authorities discussed in this post are simply more scrambled forms of encryption.

The earliest example known was from an Egyptian scribe about 1900 BC. Assyrian merchants used a form of encryption called intaglio in 1500 BC. Hebrew scribes wrote a copy of the Book of Jeremiah in a substitution cipher in 605 BC. In 487 BC the Greeks used a "skytale" to encrypt important messages. Julius Caesar (100-44 BC) encrypted government communications. Abu ' Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi wrote a book on cryptography in 725-790 AD. Thomas Jefferson invented a wheel cipher. Tellingly, a design in 1976 by IBM based on "the Lucifer cipher" is now used and called "triple-DES" (the Triple Data Encryption Algorithm).

When the German Enigma Machine was cracked in World War II, the Allies could read ALL German communications from that point forward. In the same way, Hillary's access to the PKI, Dual_EC_DRBG algorithm and Certificate Authorities gives her access to The Internet of Things' version of the Enigma Machine break, which was considered by western Supreme Allied Commander Dwight D. Eisenhower to have been "decisive" to the Allied victory. *See History of Encryption*.

(SEP. 16, 2018)—Imagine that your identity is stolen suddenly.

Your healthcare, education, police, employment and bank records are all altered overnight to make you look like an embezzler. Imagine you are jolted awake the following morning by the police bashing in your door to arrest you. Imagine that the local TV is already carrying news of your arrest using a drunken party photo of you off your phone.

Imagine further that you are Hillary Clinton. You need for 55,000 Clinton Foundation emails on FBI director James Comey computer to disappear. Poof. They're wiped without a trace.

Imagine still further that you are Lord Mark Malloch-Brown from the Queen's Privy Council. You need to erase the U.S. Department of Treasury's new evidence of foreign meddling embedded in your Smartmatic voting machines. Your bunk buddy George Soros makes a call to Hillary. Poof. This evidence is digitally wiped, without a trace.

This cannot happen in America you say? Think again.

Since these people have full backdoor access to any computer or phone on the Internet, can they ever be caught? Yes, once we realize how they do it. That method has just been discovered.

Truth is, Hillary Clinton literally has access to *every* computer on the Internet through a company named ENTRUST. Her 19-year Rose Law Firm partner Jerry C. Jones directs the company (now ostensibly run by a Silicon Valley dude named Orlando Bravo and his private equity firm Thoma Bravo, LLC), and has done since Dec. 2003. Entrust issues the encryption keys for most major governments and companies in the world.

Bookmark: #hillary-jones-acxiom | https://tinyurl.com/ya8u98aw

HILLARY CLINTON CONTROLS 50,000 FBI ENCRYPTION KEY...

- ► August (2)
- ► July (1)
- ► June (1)
- ► May (1)
- ► April (1)
- ► March (3)
- ► February (3)
- ► January (3)

► 2017 (27)
► 2016 (39)
► 2015 (34)
► 2014 (26)
► 2013 (28)
► 2012 (6)

UPDATE MAR. 25, 2014

FIVE CRITICAL AFI POSTS ON JUDICIAL COMPROMISE

Fully updated Mar. 25, 2014 in the wake of the Scribd censorship:

1. **HOW PATENT JUDGES GROW RICH ON THE BACKS OF AMERICAN INVENTORS**

Patent Office filings are shuffled out the USPTO backdoor to crony lawyers, banks and deep-pocket clients.
2. **WAS CHIEF JUSTICE ROBERTS BLACKMAILED** into supporting Obamacare by his ethical compromises in *Leader v. Facebook*?
3. **JUSTICE ROBERTS MENTORED** Facebook Gibson Dunn LLP attorneys.

4. **JUSTICE ROBERTS HOLDS** substantial Facebook financial interests.
5. **JUDGE LEONARD STARK FAILED** to disclose his Facebook financial interests and his reliance on Facebook's Cooley Godward LLP attorneys for his appointment.

BARACK OBAMA'S DARK POOLS OF CORRUPTION

Bookmark: #jones-options | https://tinyurl.com/ybt47xz6

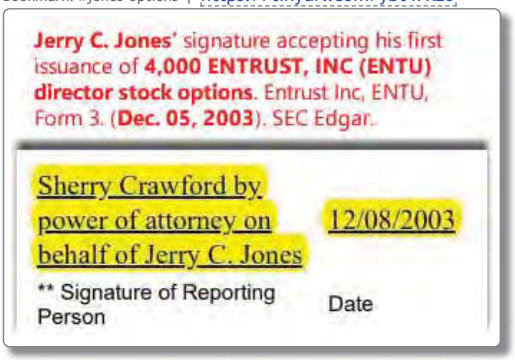


Fig. 2—Jerry C. Jones, Rose Law Firm, first ENTRUST, INC. (ENTU) director stock option award issued in secret on Dec. 05, 2003.

WHERE DID HILLARY SEND JERRY C. JONES AFTER SHE TOOK CONTROL OF ENTRUST?

ACXIOM (LITTLE ROCK, AR)—A CARBON COPY OF CAMBRIDGE ANALYTICA & SCL LIMITED (SIR GEOFFREY E. PATTIE)

The Securities & Exchange Commission records reveals that at the same time Jerry C. Jones secretly became a director of ENTRUST, Inc., he also became a director of Acxiom Corp—a data analytics firm that appears to be a carbon copy of Cambridge Analytica and SCL Limited in the UK owned by the Queen's Privy Counsellor in charge of mass surveillance, Sir Geoffrey E. Pattie. See for yourself. Here is a PDF of the SEC filings. Here is an Excel spreadsheet showing the bevy of me-too beta-males and females who feed off of the Clintons and the SES in Little Rock, Arkansas.

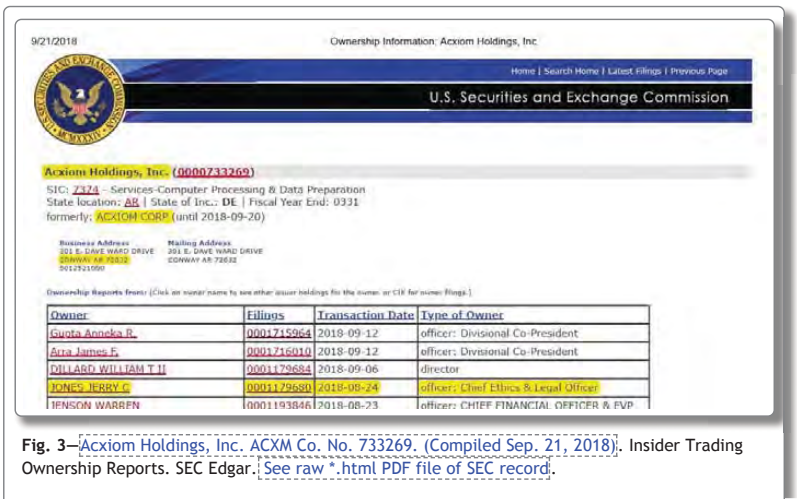
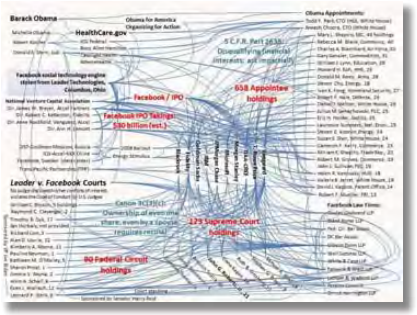


Fig. 3—Acxiom Holdings, Inc. ACXM Co. No. 733269. (Compiled Sep. 21, 2018). Insider Trading Ownership Reports. SEC Edgar. See raw *.html PDF file of SEC record.

Click to enlarge

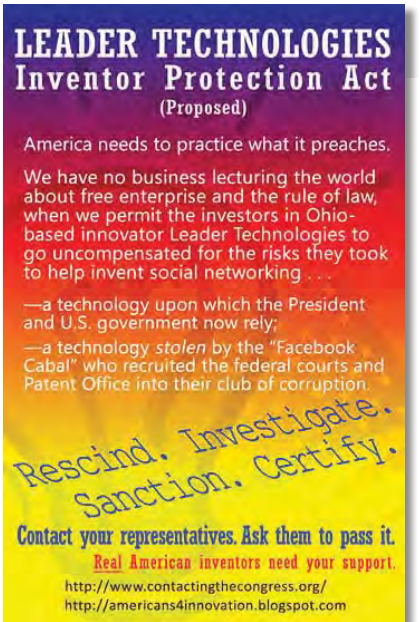


CLICK HERE FOR WASHINGTON'S ETHICAL DISEASE DISCOVERIES RE. FACEBOOK "DARK POOLS"

STOP FACEBOOK PROPERTY THEFT

WILL HUMANKIND EVER LEARN? Facebook's Orwellian doublespeak about property and privacy (theft) merely repeats the eventual dehumanization of the individual under MAO's Red Star, Stalin's SOVIET Hammer & Cycle and Hitler's NAZI Swastika. Respect for the inalienable rights of each individual is a bedrock value of democracy. The members of the Facebook Cabal abuse this principle at every opportunity. They evidently believe that they deserve special privileges and are willing to lie, cheat and steal in order to treat themselves to these privileges.

ASK CONGRESS: PASS THE INVENTOR PROTECTION ACT!



Click image above to download a poster-quality PDF optimized for a 11in. x 17in. (ledger-size) poster. America should not be in the business of cheating its entrepreneurial investors simply because the cheaters buy off judges with the money gained from their theft. Such permissiveness is obscene.

Graphic: SEC Edgar.

Bookmark: #hillary-entrust | https://tinyurl.com/yae5sous

HILLARY HAS ALL YOUR ENCRYPTION KEYS

Fig. 4—McKibben, Gabriel. (Sep. 13, 2018). Trump's September Surprise is a Doozy. *American Intelligence Media, Americans for Innovation.* https://youtu.be/-zWWJ1BzKgI | (Raw *.mp4 video file).).

Video: American Intelligence Media, Americans for Innovation.

Bookmark: #hillary-prison-planet | https://tinyurl.com/yd6sbgcl

HILLARY'S PRISON PLANET UNLOCKED

Fig. 5—McKibben, Gabriel. (Sep. 17, 2018). Hillary's PRISON PLANET Unlocked. *American Intelligence Media, Americans for Innovation.* https://youtu.be/uLlfnh6st9U | (Raw *.mp4 video file).

Video: American Intelligence Media, Americans for Innovation.

Bookmark: #acxiom-moving-to-china | https://tinyurl.com/y86lponw

LEADER V. FACEBOOK BACKGROUND

Jul. 23, 2013 NOTICE: DonnaKlineNow! has gone offline. All her posts are available as a PDF collection here (now updated, post-Scribd censorship).

Mar. 20, 2014 READER NOTICE: On Mar. 7, 2014, all of our documents linked to Scribd were deleted by that "cloud" service using the flimsiest of arguments . Some of our documents have been there for two years and some had almost 20,000 reads.

George Orwell wrote in *1984* that one knows one is in a totalitarian state when telling the truth becomes an act of courage.

All the links below were updated Mar. 20, 2014 (many thanks to our volunteers!)

1. Summary of Motions, Appeal, Petition, Evidence, Analysis, Briefings (FULL CITATIONS) in *Leader Technologies, Inc. v. Facebook, Inc.*, 08-cv-862-JJF-LPS (D. Del. 2008), published as *Leader Techs, Inc. v. Facebook, Inc.*, 770 F. Supp. 2d 686 (D. Del. 2001)
2. Dr. Lakshmi Arunachalam's Censored Federal Circuit Filings (Archive)
3. Brief Summary of *Leader v. Facebook*
4. Backgrounder
5. Fenwick & West LLP Duplicity
6. Instagram-scam
7. USPTO-reexam Sham
8. Zynga-gate
9. James W. Breyer / Accel Partners LLP Insider Trading
10. Federal Circuit Disciplinary Complaints
11. Federal Circuit Cover-up
12. Congressional Briefings re. Leader v. Facebook judicial corruption
13. Prominent Americans Speak Out
14. Petition for Writ of Certiorari
15. Two Proposed Judicial Reforms
16. S. Crt. for Schemers or Inventors?
17. Attorney Patronage Hijacked DC?

18. Justice Denied | Battle Continues
19. FB Robber Barons Affirmed by S. Crt.
20. Judicial Misconduct WALL OF SHAME
21. Corruption Watch - "Oh what webs we weave, when first we practice to deceive"
22. Facebook | A Portrait of Corruption
23. White House Meddling
24. Georgia! AM 1080 McKibben Interview

NEW! OCT. 1, 2018: ACXIOM MOVING TO CHINA—SPOOKED U.S. EMPLOYEES—WE ARE AT WAR WITH CHINA

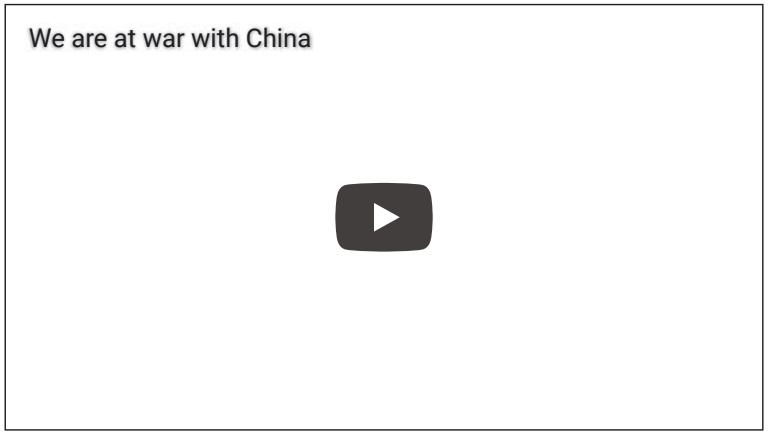


Fig. 6—Douglas Gabriel, Michael McKibben. (Sep. 28, 2018). We are at war with China. *American Intelligence Media, Americans for Innovation*. https://youtu.be/q00TB9Ns-qc | (Raw *.mp4 video file). See also Staff. (Sep. 28, 2018). ACXIOM (owned by C.I.A.-led Blackrock, controlled by Hillary) moving "data onboarding" operation from Little Rock, AR to China. *Patriots4Truth*.

Video: American Intelligence Media, Americans for Innovation.

Bookmark: #acxiom-china-distraction | https://tinyurl.com/y8lyuc6t

NEW! OCT. 1, 2018: WHILE WE WERE DISTRACTED. . .

Fig. 7—Staff. (Sep. 29, 2018). While We Were Distracted. Headlines With A Voice.. https://youtu.be/Y6okYlZJmmU | (Raw *.mp4 video file).

Video: Headlines With A Voice.

25. Constitutional Crisis Exposed
26. Abuse of Judicial Immunity since *Stump*
27. Obamacare Scandal Principals are intertwined in the Leader v. Facebook scandal
28. S.E.C. duplicity re. Facebook

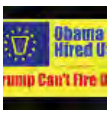
GIBSON DUNN LLP exposed as one of the most corrupt law firms in America

Investigative Reporter Julia Davis investigates **Facebook's *Leader v. Facebook* attorney Gibson Dunn LLP**. She credits this firm with the reason why not a single Wall Street banker has gone to jail since 2008. **Click here** to read her article "Everybody hates whistleblowers." *Examiner.com*, Apr. 10, 2012. Here's an excerpt:

> "Skillful manipulation of the firm's extensive media connections allows Gibson Dunn to promote their causes, while simultaneously smearing their opponents and silencing embarrassing news coverage."

This statement followed right after Davis cited Facebook's chief inside counsel in the *Leader v. Facebook* case, Theodore Ullyot, who appears to have helped lead the *Leader v. Facebook* judicial corruption. Interesting word choices associated with Gibson Dunn LLP: manipulation, smear. Attorneys swear a solemn oath to act morally, ethically, and in support of democratic principles. They promise to conduct themselves in a manner than instills confidence among the citizenry in the rule of law and the judicial system. These promises appear to be meaningless. **Click here** for a PDF version of Julie Davis' article.

POPULAR POSTS



OBAMA HIRED THEM. TRUMP CANNOT FIRE THEM. SO THEY SAY.

Senior Executive Service (SES) is ~10,000 Deep State shadow government employees who are sabotaging the American Republic for the globali...

PROOF: ROBERT MUELLER CANNOT BE IMPARTIAL IN THE RUSSIA INVESTIGATION

Mueller's Deep State relationships will politicize the FBI yet again Contributing Writers | Opinion | AMERICANS FOR INNOVATION | ...

LEADER TECHNOLOGIES FILES TRILLION DOLLAR BOND LIEN ON THE U.S. GOVERNMENT

WHAT IS AN ENCRYPTION KEY WHY IS THIS DISCOVERY SO DEVASTATING TO THE DEEP STATE SHADOW GOVERNMENT?

Put simply, encryption keys are used on both the sender's and receiver's computers to send data. It takes two keys to make a connection to send or receive data. The Clinton Administration created "trusted Certificate Authorities (CA)" to check with to make sure that the two keys are the real sender and receiver. If your keys are not approved by the CA, your connection will be blocked. In the hands of tyrannical globalists like Hillary Clinton, Barack Obama, George Soros, Eric Schmidt and Robert Mueller, this will be the new censorship on the Internet.

Bookmark: #what-are-encryption-keys | https://tinyurl.com/ybkforoz

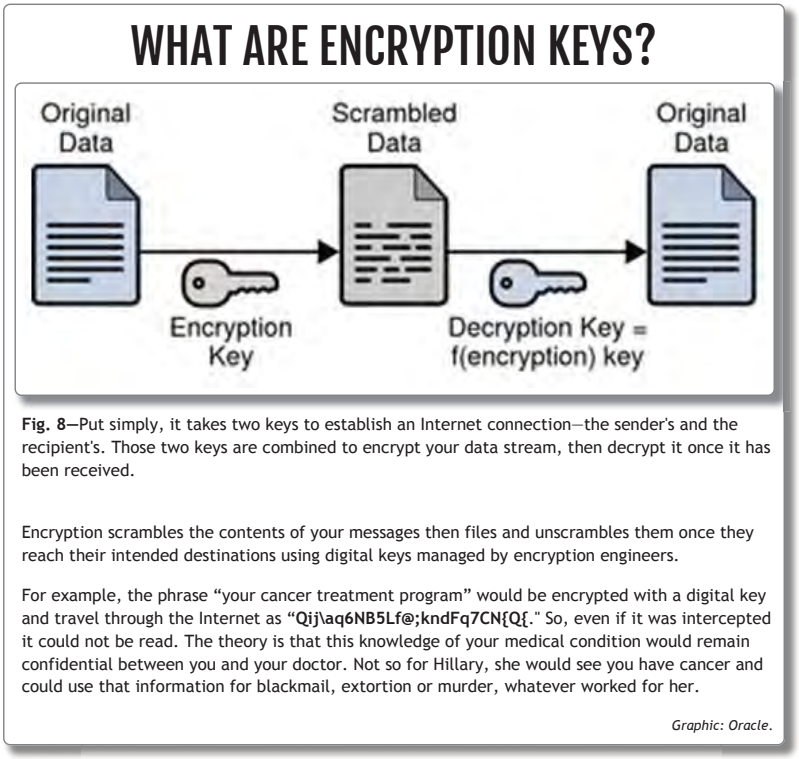


Fig. 8—Put simply, it takes two keys to establish an Internet connection—the sender's and the recipient's. Those two keys are combined to encrypt your data stream, then decrypt it once it has been received.

Encryption scrambles the contents of your messages then files and unscrambles them once they reach their intended destinations using digital keys managed by encryption engineers.

For example, the phrase "your cancer treatment program" would be encrypted with a digital key and travel through the Internet as "**Qij\aq6NB5Lf@;kndFq7CN{Q{**." So, even if it was intercepted it could not be read. The theory is that this knowledge of your medical condition would remain confidential between you and your doctor. Not so for Hillary, she would see you have cancer and could use that information for blackmail, extortion or murder, whatever worked for her.

Graphic: Oracle.

These CA's make a big deal in their propaganda that you can "trust" them not to use or spoof your identity to get access to data that you and they are not authorized to have. That is a **boldface** lie. No wonder these people have the countenances of criminals. They are, and they know it.

Suppose you are the CA who issues keys to the FBI. Suppose you want to see the evidence being gathered against you in an

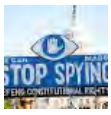
President Trump is asked to compensate Leader for the theft of their inventions by the Deep State shadow government Leader's social net...

LEADER PROPOSES TRILLION DOLLAR FED REVENUE WHILE LOWERING TAXES

User fee on social networking will generate $300+ billion a year to fund major initiatives Surcharge on social networking will pay for 17...

OHIO STATE'S PRESIDENT MICHAEL V. DRAKE MIRED IN PERSONAL CONFLICTS OF INTEREST

Trustees and Provost promote learning technology that benefits trustee clients and is stolen from OSU alums Contributing Writers | Opini...



AMERICAN MORAL UNDERPINNINGS ARE UNDER SIEGE BY GODLESS DEEP STATE CORPORATE GLOBALISTS

Trump under surveillance for many years MSM fake news is INTENDED to degrade our Republic Judeo-Christian moral values of our Founde...

MEET THE PERSON WHO CAN REMOTELY CRASH PLANES AND CAN READ YOUR MIND

Monstrous Patent calls people "wet ware" Implanted devices deliver electric shock, poisons, dopamine, adrenaline, emit mind control freq...

OSU BAND INVESTIGATION UNEARTHS SURPRISE TRUSTEE COLLUSION IN PATENT THEFT

Breaking News, Sep. 3, 2014 , 10:05am OSU Trustee President, Jeffrey Wadsworth, "counterattacks" the Band Alumni leadership T...

HILLARY CLINTON CONTROLS 50,000 FBI ENCRYPTION KEYS—PROVES MUELLER'S WITCH HUNT IS TREASONOUS

With these encryption keys, nothing in our digital lives is off limits to the Clinton's and their conspirators President Trump's n...

THE SHADOW GOVERNMENT USES SES, SERCO AND OPIC AS PORTALS INTO HORRIFIC CORRUPTION

These lawyers, bankers, academics, journalists, bureaucrats and self-styled elitists sponge off the actual wealth-creation of hard working ...

EDITORIALS

1. DC Bar refuses to investigate attorney misconduct in Leader v. Facebook - Unwillingness of DC attorneys to self-

investigation.

All you have to do is “borrow” the FBI key from Hillary or ENTRUST. Then you can connect to the target FBI computer using a bogus key created for you by ENTRUST, and voile! You then have two “trusted” keys so the FBI computers let you in. There are technical nuances to this description, but basically, you can do what you want with these keys. Don't let trollers try to baffle you with techno-jargon to throw your dogs off the scent. **Lucifer** (literally, IBM Triple-DES) is in these encryption details.

Hillary Clinton has this level of access to practically all data on the planet, including the FBI, NSA, Departments of State, Commerce, Energy, Treasury, GSA, Patent Office, Post Office, NIST, as well as numerous foreign government and commercial entities. *See* ENTRUST 10-K Annual Reports (1998-2009). SEC Edgar.

Now that we finally know how the Clinton's stay one step ahead of the sheriff, we can now stop them.

MORE HARD PROOF THAT HILLARY CLINTON IS A DIGITAL MONSTER

In this post, we will prove without a doubt how Hillary Clinton cleverly wormed her way into full access and control for 50,000 FBI encryption keys.

They are likely managing this empire from Obama’s Google-constructed U.S. Digital Service bunker three blocks from the White House manned by Valerie Jarrett and Eric Holder.

We admit that these findings sound more like Grisham fiction. But the evidence is a pesky thing. The evidence is now pouring out.

THE EVIDENCE PROVIDED IS “JUDICIALLY RECOGNIZABLE” AND INDICTABLE, WE BELIEVE

“Notoriously public” information, like the U.S. Securities & Exchange Commission filings that we cite, is evidence that requires no further verification to be used in litigation, hence the adjective “notoriously.” This means that the information is

police may explain why Washington is broken, Dec. 30, 2012

2. Will the U.S. Supreme court support schemers or real American inventors? Facebook's case dangles on a doctored interrogatory. Eighteen (18) areas of question shout for attention, Dec. 27, 2012

3. Two Policy Changes That Will Make America More Democratic (and less contentious), Dec. 21, 2012

OUR MISSION

American citizens must fight abuse of the constitutional right for authors and inventors to enjoy the fruits of their inventions, as a matter of matter of basic property rights and sound public policy. Otherwise, instead of innovation, creativity, genius, ideas, vision, courage, entrepreneurship, respect, property, rejuvenation, morals, ethics, values, renewal, truth, facts, rights, privacy, solutions and judicial faithfulness,

. . . our society and economy will be dragged down (and eventually destroyed) by copying, infringement, thievery, counterfeiting, hacking, greed, misinformation, exploitation, abuse, waste, disrespect, falsity, corruption, bribery, coercion, intimidation, doublespeak, misconduct, lies, deception, attorney "dark arts," destruction, confusion, dishonesty, judicial chicanery and lawlessness.

If we do not speak up, impeach derelict judges and imprison corrupt attorneys, we cannot possibly hope to start fixing the current ills in our society. Without justice and respect for private property, democracy has no sure foundation.

CURRENT EDITORIAL FOCUS

We are an opinion blog that advocates for strong intellectual property rights. We welcome commenters and contributors. The *Leader v. Facebook* patent infringement case first came to our attention after learning that the trial judge, Leonard P. Stark, U.S. District Court of Delaware, ignored his jury’s admission that they had no evidence to support their on-sale bar verdict, but the judge supported it anyway.

The judicial misconduct has deteriorated from there, replete with two of the three judges on the Federal Circuit appeal panel, Judges Alan D. Lourie and Kimberly A. Moore, holding Facebook stock that they did not disclose to the litigants, and later tried to excuse through a quick motion slipped in at the last minute by the Clerk of Court, Jan Horbaly, and his close friends at The Federal Circuit Bar Association. (The DC Bar subsequently revealed that Mr. Horbaly is not licensed to practice law in Washington D.C.)

The judges ignored shocking new evidence that Mark Zuckerberg withheld 28 hard drives

so publicly noteworthy that further proof of validity is unnecessary. For example, John F. Kennedy was assassinated in 1963. That is a notoriously public fact and no proof is needed.

Notoriously public facts, like SEC filings, are "judicially recognizable" and can be accepted as truthful since the submitter attests to the SEC that they are true. It is criminal fraud to lie intentionally in SEC filings.

TIMELINE: BILL & HILLARY CLINTON BEGAN ORCHESTRATING UNFETTERED ACCESS TO THE FBI'S ENCRYPTION KEYS IN 1993

On Jun. 07, 1993, the new Clinton Administration convened the "Third CPSR Cryptography and Privacy Conference (CPSR - Computer Professionals For Social Responsibility)."

The conference was held two days before an important Jun. 09, 1993 House hearing on "encryption and telecommunications network security." The conference gathered over 106 attendees representing government, politics, commerce, manufacturing, industry, media, technology, telecommunications, healthcare, banking, education, faith and accounting. That's plenty of arm-twisting, even for Washington, D.C.

The meeting sponsor was globalist advocate Carnegie Endowment for International Peace.

The hosts included:

(1) **James P. Chandler, III**, George Washington University intellectual property and national security law professor, and later patent attorney for social networking inventor Leader Technologies, Inc. (Jan. 2000);

2) **John D. Podesta**, chief of staff and campaign manager to Bill Clinton, Barack Obama and Hillary Clinton; and

(3) **Stephen D. Crocker**, founding member of the illegal public-private conspiracy group Highland's Forum/Group (Feb. 1995), then Barack Obama's director of ICANN (Internet Corporation for Assigned Names and Numbers) who ceded control to the UN on

of 2003-2004 evidence from Leader Technologies that could prove actual theft (and therefore claims even more serious than infringement). In addition, Facebook's appeal attorney, Thomas G. Hungar of Gibson Dunn LLP, has close personal ties to just about every judicial player in this story. The misconduct appears to reach into the U.S. Patent Office through abuse of the reexamination process by Facebook. We will stay focused on *Leader v. Facebook* until justice is served, but we also welcome news and analysis of intellectual property abuse in other cases as well.

WELCOME TO DONNA KLINE NOW! READERS!

AFI has been supporting Donna and is now picking up the main Leader v. Facebook coverage (she will continue coverage as well).

Anonymous Posts Are Welcomed! Blogger has more posting constraints than Donna's WordPress, but we will continue to welcome anonymous posts. Simply send us an email at **NEW Leader® Private Email: afi@leader.com** with your post. Once the moderator verifies that your email address is real, your comment will be posted using your real name or handle, whatever you wish, like John Smith or Tex.

Click here to view a complete *Donna Kline Now!* posts archive.

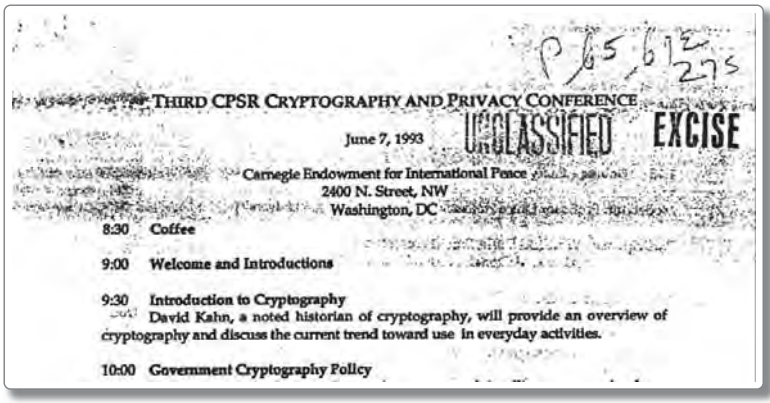
Oct. 01, 2016—one month before Donald J. Trump was elected president.

HILLARY HID THE 1993 ENCRYPTION MEETING ATTENDEE LIST

The information about this meeting was hidden on Hillary's private email server. It was unearthed by corruption watchdog Judicial Watch after they pressed the State Department in court to release the document.

Bookmark: #clinton-fbi-encryption-scam-begins | https://tinyurl.com/ybpflzqn

THE ENCRYPTION KEY SET UP



THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE

June 7, 1993 UNCLASSIFIED EXCISE

Carnegie Endowment for International Peace
2400 N. Street, NW
Washington, DC

8:30 Coffee

9:00 Welcome and Introductions

9:30 Introduction to Cryptography
David Kahn, a noted historian of cryptography, will provide an overview of cryptography and discuss the current trend toward use in everyday activities.

10:00 Government Cryptography Policy

Fig. 9—1993 Clinton encryption conference to give the FBI backdoor keys to the Internet.

James P. Chandler, III, John D. Podesta. (Jun. 07, 1993). Third CPSR Cryptography and Privacy Conference, included Stephen D. Crocker, John D. Podesta, James P. Chandler, III, Ann Harkins, Ken Mendelson (Stroz Friedberg), Juan Osuna, Cathy Russell, Steven Wolff, IBM, HP, AT&T. FOIA No. 9403963. U.S. Dept. of State. Note: This PDF file contains a spreadsheet of the attendees (click on the paper clip inside the PDF).

Graphic: Judicial Watch.

In 1993-1994, more than 20 people close to or investigating Clinton corruption died under suspicious circumstances.

THEFT & WEAPONIZATION OF U.S. INVENTIONS

In Feb. 1995, the Highlands Forum/Group was formed. It was and is a highly illegal private "public-private" meeting sponsored by the Department of Defense Net Assessment group run by Senior

CODE OF CONDUCT FOR U.S. JUDGES

"CANON 2: A JUDGE SHOULD AVOID IMPROPRIETY AND THE APPEARANCE OF IMPROPRIETY IN ALL ACTIVITIES"

GALLERY OF JUDICIAL MISCONDUCT

Judge Leonard P. Stark, U.S. District Court of Delaware, trial judge in *Leader Techs, Inc. v. Facebook, Inc.*, 770 F. Supp. 2d 686 (D.Del. 2011). Judge Stark heard his jury foreman admit that the jury made the on-sale bar decision *without any evidence other than speculation*, and yet he supported that verdict anyway. Just months before trial, Judge Stark allowed Facebook to add the on-sale bar claim after the close of all fact discovery and blocked Leader from preparing its defenses to this new claim. Judge Stark allowed the claims despite Leader's prophetic argument that the action would confuse the jury and prejudice Leader. He also permitted the jury to ignore the *Pfaff v. Wells Electronics, Inc.* test for on-sale bar, even after instructing the jury to use it. (See that Jury Instruction No. 4.7 here.) He also contradicted his own instruction to Leader to answer Interrogatory No. 9 in the

Like
Like

Executive Service (SES) members Richard P. O'Neill and Andrew W. Marshall. *See* also AFI. (Nov. 22, 2017). The Weaponization of Social Media Should Concern Us All. *Americans for Innovation*.

The no-notes meetings involve no-bid crony insiders from the military, intelligence, banking, technology, telecom, transportation, defense, venture capital, media an academia to discuss the weaponization of new inventions stolen by DARPA (Defense Advanced Research Projects Agency).

On Apr. 17, 1995, Clinton signed Executive Order 12958 titled "Classified National Security."

This order consolidated control of classification procedures to *just seven people*: (1) Secretary of State, (2) Secretary of Defense, (3) Attorney General, (4) C.I.A. Director, (5) U.S. Archivist, (6) National Security Director and (7) the President.

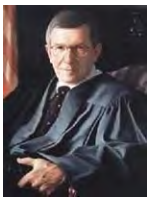
A most dubious provision said that *any* U.S. security classification that contradicted another country's laws or treaty rendered it of no effect. In other words, if Obama wanted to release a classified document, all he had to do was call up Justin Trudeau in Canada and ask him to pass a law saying America's XYZ classified information was harmful to beavers on the northern slopes. That would nullify the U.S. classification and give Obama the excuse to release it. Clearly, it was a precursor to Obama's foreign trade entanglements in the Trans-Pacific Partnership (TPP) that President Trump killed, thankfully.

On Apr. 19, 1995, the Alfred P. Murrah Federal Building in downtown Oklahoma City, was bombed by Timothy McVeigh and Terry Nichols—just *two days* after Bill Clinton formed a secret White House intelligence operation via Executive Order 12958 cited above.

This bombing created more excuses for mass surveillance against Americans. Notably, Clinton body guard Alan G. Whicher was killed in this weapons grade-energy blast that could not have been caused by a fertilizer bomb, as were led to believe by MSM. Retired FBI superstar Theodore L. Gunderson, a short-list candidate to be FBI director, revealed that psychiatrist Dr. Jolly West, one of the founders of the C.I.A. MKUltra mind control program, paid a visit to McVeigh before the trial. Gunderson said he believed that McVeigh was a brainwashed MKUltra drone.

On Jul. 12, 1995, IBM and Lotus merged. Lotus Notes became the Deep State's groupware platform of choice for establishing a global mass surveillance spy grid. PKI (Public Key Infrastructure) encryption standards were selected to build into IBM/Lotus/Microsoft/Novell/Red Hat software, hardware and firmware.

present tense (2009), then permitted the jury to interpret it as a 2002 admission as well. Facebook's entire on-sale bar case is based upon this interrogatory. (*Editorial*: Hardly sufficient to meet the "heavy burden" of the clear and convincing evidence standard.)



Judge Alan D. Lourie, U.S. Court of Appeals for the Federal Circuit, panel judge in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Lourie stood to benefit financially from undisclosed holdings in Facebook. See analysis of Judge Lourie's T. Rowe Price holdings re. the Facebook IPO. Judge Lourie also failed to apply his own law-test in *Group One v. Hallmark Cards* to the evidence.

Like

After debunking all of Facebook's evidence on appeal, Judge Lourie created new argument in the secrecy of chambers to support Facebook and prevent the on-sale bar verdict from being overturned—a clear breach of constitutional due process.

Judge Kimberly A. Moore, U.S. Court of Appeals for the Federal Circuit, panel judge in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Moore stood to benefit financially from undisclosed holdings in Facebook. See disclosure of substantial holdings in Facebook and Facebook-related stocks. Judge Moore failed to follow the long-held precedent for testing on-sale bar evidence in *Pfaff v. Wells Electronics, Inc.*—an evident and intentional omission coming from a former patent law professor. After debunking all of Facebook's evidence on appeal, Judge Moore created new argument in the secrecy of chambers to support Facebook and prevent the on-sale bar verdict from being overturned—a clear breach of constitutional due process.

Like

LAWS CHANGED TO PREPARE FOR THE PATRIOT ACT ABOLISHMENT OF THE BILL OF RIGHTS

Between 1995-1999, a series of national security laws, executive orders (EOs) and presidential policy directives (PPDs) were written for Clinton by James P. Chandler, III, his national security and intellectual property advisor.

Magically, the laws that Chandler drafted passed nearly unanimously. (Note: Whenever that occurs, all of Congress has been bought off or fooled *en masse* before the vote. Remember: Clinton had likely already had access to the FBI encryption keys by this time. Therefore, he had amassed plenty of blackmail and extortion information on every influential member of Congress.)

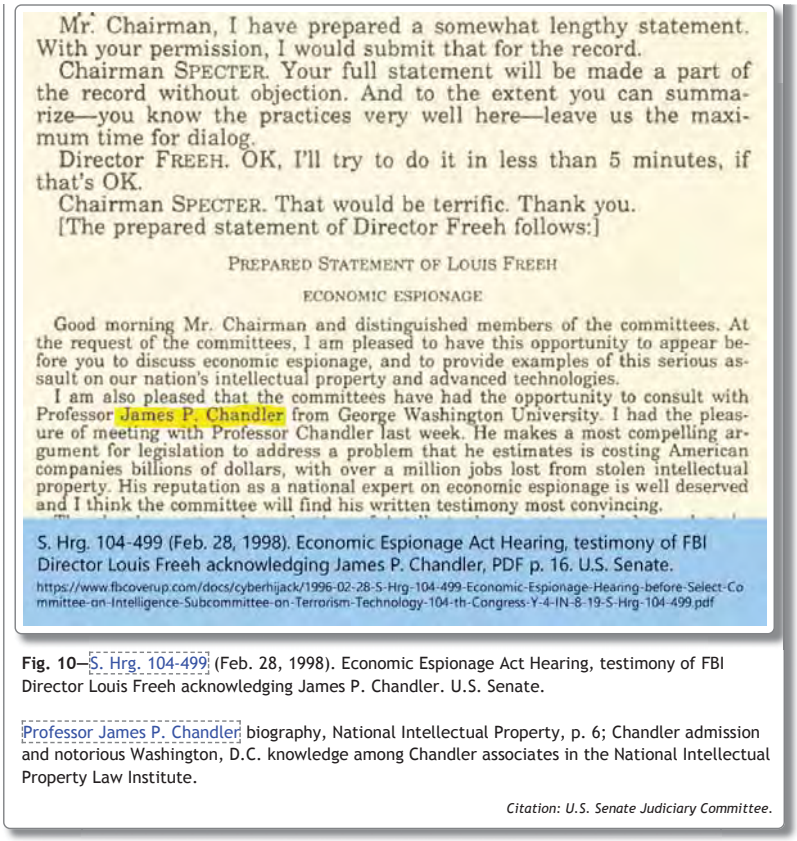
On Feb. 28, 1996, FBI Director Louis Freeh self-consciously deferred to James P. Chandler, III in his testimony on economic espionage, revealing that Chandler controlled FBI security policy for Clinton. Freeh was clearly the puppet and Chandler the puppet master.

Bookmark: #chandler-fbi-freeh-clinton-mueller-congress-mass-surveillance-scam | https://tinyurl.com/y7vhfozr

JAMES P. CHANDLER, III HAS DRIVEN THE FBI ENCRYPTION KEY SCAM FOR THE CLINTONS

Judge Evan J. Wallach, U.S. Court of Appeals for the Federal Circuit, member of the three-judge panel in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Wallach is not a patent attorney. This begs the question as to why a judge with no knowledge of patent law was assigned to the case. Would anyone ask a dentist to perform brain surgery? The Federal Circuit was specially formed to appoint patent-knowledgeable judges to patent cases. There is no evidence so far in the judicial disclosures that Judge Wallach holds stock in Facebook, although when he was asked on a motion to disclose potential Facebook holdings and other conflicts of interest, he refused along with the other judges. See Motion to Disclose Conflicts of Interest. Judge Wallach continued in silence even after Clerk of Court Horbaly failed to provide him with Dr. Lakshmi Arunachalam's motions (according to his Federal Circuit staffer Valeri White), and yet the Clerk signed an order regarding that motion on Judge Wallach's behalf. See a full analysis of these events at Donna Kline Now! Judge Wallach also failed to police his court's violation of Leader's Fifth and 14th Amendment constitutional right to due process when he participated in the fabrication of new arguments and evidence for Facebook in the secrecy of judge's chambers after he had just invalidated Facebook's sole remaining item of evidence (using disbelieved testimony as ostensible evidence of an opposite). Judge Wallach also failed to police his court when he failed to apply the Supreme Court's *Pfaff v. Wells Electronics, Inc.* test for on-sale bar evidence, which included even the Federal Circuit's own *Group One v. Hallmark Cards, Inc.* test—a test which Judge Lourie should have advised Judge Wallach to follow since Judge Lourie *helped write* that opinion. *Group One* test omission analysis.

Like



Mr. Chairman, I have prepared a somewhat lengthy statement. With your permission, I would submit that for the record.

Chairman SPECTER. Your full statement will be made a part of the record without objection. And to the extent you can summarize—you know the practices very well here—leave us the maximum time for dialog.

Director FREEH. OK, I'll try to do it in less than 5 minutes, if that's OK.

Chairman SPECTER. That would be terrific. Thank you.

[The prepared statement of Director Freeh follows:]

PREPARED STATEMENT OF LOUIS FREEH

ECONOMIC ESPIONAGE

Good morning Mr. Chairman and distinguished members of the committees. At the request of the committees, I am pleased to have this opportunity to appear before you to discuss economic espionage, and to provide examples of this serious assault on our nation's intellectual property and advanced technologies.

I am also pleased that the committees have had the opportunity to consult with Professor James P. Chandler from George Washington University. I had the pleasure of meeting with Professor Chandler last week. He makes a most compelling argument for legislation to address a problem that he estimates is costing American companies billions of dollars, with over a million jobs lost from stolen intellectual property. His reputation as a national expert on economic espionage is well deserved and I think the committee will find his written testimony most convincing.

S. Hrg. 104-499 (Feb. 28, 1998). Economic Espionage Act Hearing, testimony of FBI Director Louis Freeh acknowledging James P. Chandler, PDF p. 16. U.S. Senate.

https://www.fbicoverup.com/docs/cyberhijack/1996-02-28-S-Hrg-104-499-Economic-Espionage-Hearing-before-Select-Committee-on-Intelligence-Subcommittee-on-Terrorism-Technology-104-th-Congress-Y-4-IN-8-19-S-Hrg-104-499.pdf

Fig. 10—S. Hrg. 104-499 (Feb. 28, 1998). Economic Espionage Act Hearing, testimony of FBI Director Louis Freeh acknowledging James P. Chandler. U.S. Senate.

Professor James P. Chandler biography, National Intellectual Property, p. 6; Chandler admission and notorious Washington, D.C. knowledge among Chandler associates in the National Intellectual Property Law Institute.

Citation: U.S. Senate Judiciary Committee.

On Oct. 11, 1996, Congress passed three Clinton-Chandler laws that were used to further gut Congressional oversight over security and privacy. It enabled the FBI to increase mass surveillance, then lie about it.

The Economic Espionage Act, 18 U.S. Code § 1831;

The Federal Trade Secrets Act, 18 U.S.C. § 1836; and

The False Statements Accountability Act of 1996, 18 U.S.C. § 1001.

Hindsight shows that the names for these laws were a cruel, unlawful, immoral, devilish deceit and had the opposite of the intentions of the rogue C.I.A., Clinton's, Chandler, Mueller, Comey, etc. to fuel economic espionage, theft of trade secrets and lying to Congress, courts, the President and We the People.

On Feb. 12, 1997, Chandler incorporated Eurotech, Ltd. to hire former Soviet scientists and engineers to build embedded encryption spy backdoors inside *all* computer hardware, firmware and software in Italy. The key Eurotech players were/are Microsoft, IBM, Intel, Cisco, Oracle and Wind River, among others. JPMorgan Chase's John McNeil Wilkie helped expand the company, as did Fenwick & West LLP (another

Clerk of Court Jan Horbaly, U.S. Court of Appeals for the Federal Circuit, clerk who signed all the opinions in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Clerk Horbaly and his staff obfuscated when the court's ruling was challenged by an *amicus curiae* brief revealing clear mistakes of law and new evidence. See analysis of the misconduct and misrepresentations within the Federal Circuit Clerk of Court in *Leader v. Facebook*. Mr. Horbaly failed to disclose his conflicts of interest and close associations with numerous Facebook attorneys and law firms, as well as his close association with one of Facebook's largest shareholders, Microsoft, who is a Director of The Federal Circuit Bar Association where Mr. Horbaly is an ex officio officer. Additionally, the DC Bar revealed in a written statement that Clerk Horbaly is not licensed to practice law in the District of Columbia. [Editorial: What does that make the Federal Circuit with its location within in a stone's throw of the White House? A self-governing state?]

Like

Judge Randall R. Rader, U.S. Court of Appeals for the Federal Circuit, chief judge responsible for the (mis)conduct of his judges and Clerk of Court in *Leader Techs v. Facebook, Inc.*, 678 F.3d 1300 (Fed. Cir. 2012). Judge Rader failed to manage his court resulting in a likely situation where his judges never even received briefs that they allegedly ruled on in favor of Facebook. Judge Rader also failed to disclose his conflicting relationships with a Leader principle with whom he may have had deep professional differences during his time at the Senate Judiciary Committee—his former professor of law at George Washington University Law Center, former Leader director Professor James P. Chandler. See analysis of Judge Rader's undisclosed conflicts of interest in *Leader v. Facebook*. Judge Rader also did not stop his judges from creating new arguments and evidence for Facebook in the secrecy of

Like

Like

Leader Technologies patent attorney and Silicon Valley C.I.A. co-conspirator).

On Oct. 23, 1997, The Clinton Foundation was formed.

Mar. 5, 1998—Jul. 11, 1999, Clinton and Gen. Wesley Clark prosecuted the Kosovo fraud based on a so-called “Račak genocide massacre” false flag. French journalists have proved that Račak was *completely staged*. However, it did succeed in cajoling Congress to approve U.N. intervention (led by Gen. Wesley K. Clark), and it succeeded in disabling Orthodox Christian resistance to the planned jihadi migration wave now occurring.

On Aug. 06, 1998, Robert S. Mueller, III's law firm Hale & Dorr (now Wilmer Hale) helped file "The Internet of Things" patents for Hewlett-Packard’s Richard C. Walker that described a global surveillance grid that even monitors and controls individual body functions and describes human beings as "wet-ware." The invention also contains an accounting and taxing capability to manage "certificate authorities" to control Public Key Infrastructure (PKI) encryption, tax the Internet and control "wet-ware" access.

Bookmark: #walker-patent | https://tinyurl.com/y87pvqgq

Click image to enlarge

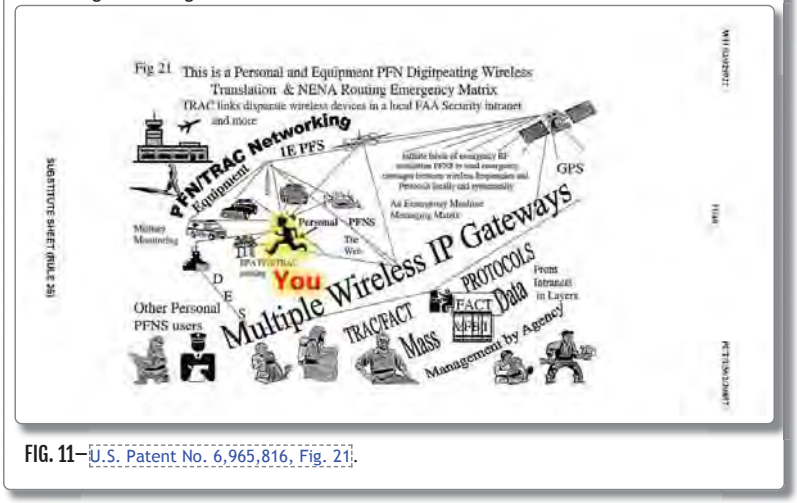


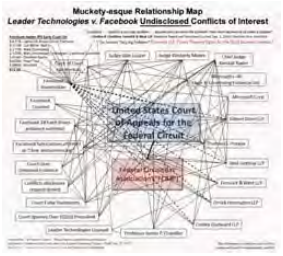
FIG. 11—U.S. Patent No. 6,965,816, Fig. 21.

Bookmark: #hillary-qrs-11-crashes-planes | https://tinyurl.com/ybnuvrnq

chambers—after they had debunked all of Facebook's evidence on appeal, which is a clear breach of constitutional due process.

Updated May 22, 2015

Click here to view a Federal Circuit *Leader v. Facebook* **Conflicts of Interest** Map.



See "Cover-up In Process At The Federal Circuit?" *Donna Kline Now!* Sep. 17, 2012.

Leader v. Facebook Legal Research Links

NOTICE: Opinion

This is an opinion blog. Any information contained or linked herein should be independently verified and should be considered the sole opinion of the writer. Free Speech and Freedom of the Press are protected by the First Amendment of the U.S. Constitution and other local, state, national and international laws. Therefore, as with all opinion, such opinion should not be relied upon without independent verification.

This site is a not-for-profit effort focused on education, news, investigation of issues in the public interest, and research, and relies on fair use copyright exemptions under 17 U.S.C. 106(a)-117 of the United States Copyright Act, in addition to any and all other related and relevant privileges to which a fair and reasonable person would attribute to this grassroots effort to root out corruption and promote justice. No rights whatsoever to third party content are claimed or implied.

AFI LOGO (with text)

AFI LOGO (no text)

Click image to enlarge

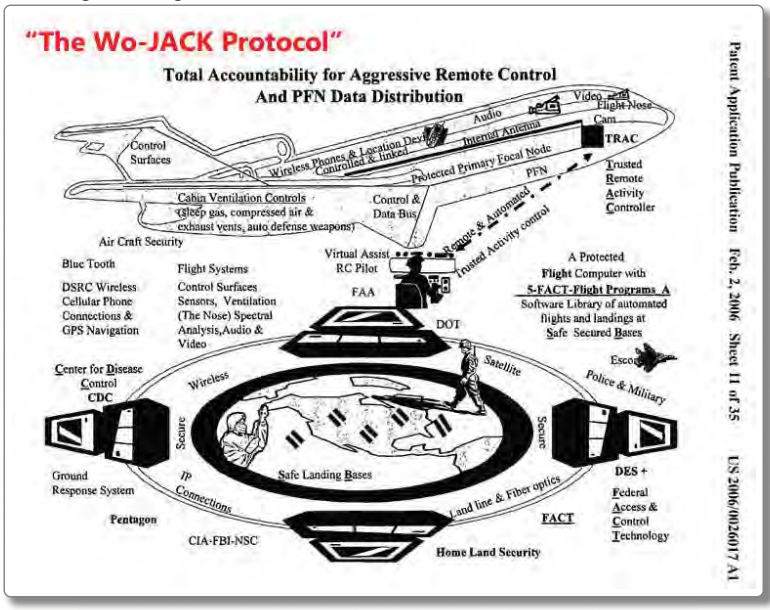


FIG. 12—U.S. Patent No. 6,965,816, Fig. 1.AFI. (Jan. 11, 2018). Meet The Person Who Can Remotely Crash Planes And Can Your Mind. *Americans for Innovation*.

Bookmark: #hillary-entrust-pki | https://tinyurl.com/y7zf3eku

Click image to enlarge

FIG. 13—Hillary Clinton has controlled ENTRUST INC ever since his 19-year Rose Law Firm partner Jerry C. Jones was secretly slipped onto the Board of ENTRUST INC. in Dec. 2003, just after thge IBM Eclipse Foundation received the debugged version of Leader Technologies' social

CORRUPTION WATCH LIST

Faces of the Facebook Corruption (PDF) (currently being updated after the Fri. Mar. 7, 2014 Scribd censorship of this document:

Here is the cast of characters in *Leader v. Facebook*. We encourage you to report their corrupt activities to this site and others, like Lawless America. Feel free to communicate anonymously in any way in which you are most comfortable. The attempt of these people and their organizations to corrupt American justice and commerce cannot be tolerated. Vigilance. We will expose them. See Congressional Briefings (currently being updated after Scribd censored the documents on Fri. Mar. 7, 2014).

A. Facebook's law firms:

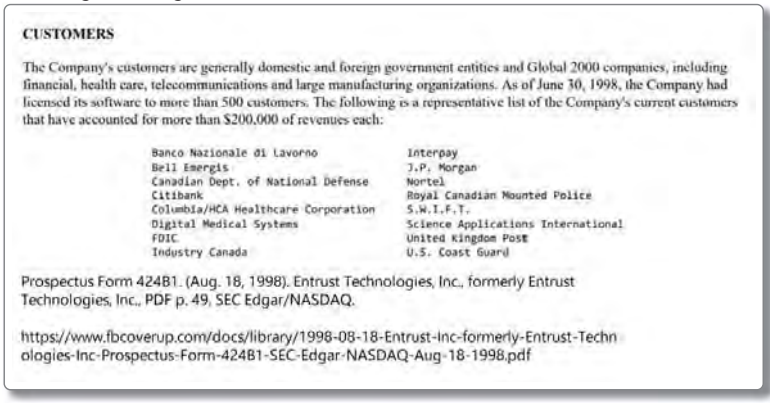
1. **Fenwick & West LLP** (Facebook securities and patent law firm; former Leader Technologies counsel; attempted an appearance in *Leader v. Facebook*; did not seek conflicts waiver from Leader prior to representing Facebook)
2. **Cooley Godward LLP** (Facebook law firm in *Leader v. Facebook*; McBee Strategic energy stimulus partner; Obama Justice Dept. advisor; former employer to patent judges)
3. **Blank & Rome LLP** (Facebook law firm in *Leader v. Facebook*; former employer to patent judges)
4. **White & Case LLP** (Facebook law firm in *Leader v. Facebook*; undisclosed former employer to Patent Office Freedom of Information Act (FOIA) officer involved in *Leader v. Facebook*)
5. **Gibson Dunn LLP** (Facebook law firm in *Leader v. Facebook*; undisclosed counsel to the Federal Circuit; undisclosed protégé of Chief Justice John Roberts, Jr.; undisclosed former employer to Preetinder ("Preet") Bharara, U.S. Attorney currently persecuting Paul Ceglia in *U.S. v. Ceglia* (*Ceglia v. Zuckerberg*))
6. **Orrick Herrington LLP** (longtime Facebook law firm and destroyer of evidence for the cabal in

networking engineering source code from Leader's patent lawyer James P. Chandler, III, who was secretly working with IBM and the rogue C.I.A. to build a new mass surveillance system based on social networking. *See* Federal PKI Graph.

On Aug. 18, 1998, Entrust Technologies, Inc. went public after being started as a spin-off of Nortel Networks (Canada) to manage and distribute Public Key Infrastructure (PKI) Certificate Authorities—the encryption keys for the Internet. Their customers include important military, banking, healthcare and government entities in the U.S., U.K., Australia, Canada, Sweden, Denmark, France, Italy, Spain and China.

Bookmark: #entrust-1998-prospectus | https://tinyurl.com/y9h6ogel

Click image to enlarge



CUSTOMERS

The Company's customers are generally domestic and foreign government entities and Global 2000 companies, including financial, health care, telecommunications and large manufacturing organizations. As of June 30, 1998, the Company had licensed its software to more than 500 customers. The following is a representative list of the Company's current customers that have accounted for more than $200,000 of revenues each:

Banco Nazionale di Lavoro	Interpay
Bell Emergis	J.P. Morgan
Canadian Dept. of National Defense	Nortel
Citibank	Royal Canadian Mounted Police
Columbia/HCA Healthcare Corporation	S.W.I.F.T.
Digital Medical Systems	Science Applications International
FDIC	United Kingdom Post
Industry Canada	U.S. Coast Guard

Prospectus Form 424B1. (Aug. 18, 1998). Entrust Technologies, Inc., formerly Entrust Technologies, Inc., PDF p. 49, SEC Edgar/NASDAQ.

https://www.fbcoverup.com/docs/library/1998-08-18-Entrust-Inc-formerly-Entrust-Technologies-Inc-Prospectus-Form-424B1-SEC-Edgar-NASDAQ-Aug-18-1998.pdf

FIG. 14—Prospectus Form 424B1. (Aug. 18, 1998). Entrust Technologies, Inc., formerly Entrust Technologies, Inc., PDF p. 49. SEC Edgar/NASDAQ.

On Oct. 14, 1998, SI International, LLC, later renamed SERCO SERVICES, Inc., was allowed to form with Lockheed Martin and Senior Executive Service (SES) executives associated with the treasonous Highlands Group (Feb. 1995). Lockheed Martin runs the Queen's "Golden Share" company British Nuclear Fuels Limited with SERCO.

On Dec. 20, 1998, globalist psychopath George Soros admitted to having been a Hungarian Jewish Nazi collaborator without remorse for betraying his own Jewish brothers and sisters.

On Mar. 09, 1999, Clinton's Vice President Al Gore took credit for founding the Internet, laughably.

On Jul. 01, 1999, Clinton Attorney General Janet Reno created a new "Office of Special Counsel" inside the Department of Justice after the Special Counsel law was not re-authorized by Congress. This dubious Department of Justice policy (not a law) is now being used to justify the Mueller witch hunt.

Winklevoss v. Zuckerberg and *ConnectU v. Facebook*)

7. **Weil Gotshal LLP** (Federal Circuit counsel in *Leader v. Facebook*; Judge Kimberly A. Moore's undisclosed former client)
8. **Latham & Watkins LLP** (Facebook Director James W. Breyer's counsel; Judge Kimberly A. Moore's husband, Matthew J. Moore's new law firm)
9. **Federal Circuit Bar Association** ("FCBA") (Federal Circuit's bar association; second largest in the U.S.; Facebook's law firms extert much influence in its policy and activity, incl. Fenwick & West LLP, Gibson Dunn LLP, Orrick Herrington LLP, Weil Gotschal LLP; Facebook's large shareholder, Microsoft, is a director; Federal Circuit Clerk of Court Jan Horbaly is an officer; FCBA made an appearance in *Leader v. Facebook* to oppose the *amicus curiae* (friend of the court) motion of Dr. Lakshmi Arunachalam, former Director of Network Architecture at Sun Microsystems, in favor of Leader Technologies and objecting to the evident conflicts of interest within the court itself, her motion was denied, the judges refused to disclose their conflicts which we now know include Facebook and Microsoft stocks)
10. **DC Bar Association**
11. **Perkins Coie LLP** (Facebook's "rapid response enforcement team;" law firm for Obama's chief counsels, the husband and wife team of Robert F. Bauer and Anita B. Dunn; Bauer was identified on Aug. 1, 2013 as having directed the IRS targeting of the Tea Party)
12. **Stroz Friedberg** (Facebook's "forensic expert" who manipulated the data in *Paul Ceglia v. Mark Zuckerberg*, and who first revealed the existence of 28 Zuckerberg hard drives and Harvard emails that they told Leader Technologies in 2009 were "lost")
13. **Chandler Law Firm Chartered** (Professor James P. Chandler, III, principal; Leader Technologies patent counsel; adviser to IBM and David J. Kappos; adviser to Eric H. Holder, Jr. and the U.S. Department of Justice; author of the Economic Espionage Act of 1996 and the Federal Trade Secrets Act)

B. Facebook attorneys & cooperating judges:

14. **Gordon K. Davidson** (Fenwick; Facebook's securities and patent attorney; Leader Technologies' former attorney)
15. **Christopher P. King** (*aka* Christopher-Charles King *aka* Christopher King *aka* Christopher-Charles P. King, Fenwick & West LLP)
16. **Theodore B. Olson** (Gibson Dunn)
17. **Thomas G. Hungar** (Gibson Dunn)
18. **Eric H. Holder, Jr.** (Attorney General, U.S. Dept. of Justice)

On Jul. 02, 1999, Clinton appointed Larry H. Summers Treasury Secretary. The next day, on Jul. 03, 1999, Summers appointed Sheryl K. Sandberg as chief of staff. Sandberg later started Gmail in Jan. 20, 2001, and then became Facebook chief operating officer on Mar. 14, 2008.

Summers' former Treasury staffer (1993-2001), Marne L. Levine (Deutch) became Summers' chief of staff starting at Harvard on Jul. 02, 2001 where she oversaw the C.I.A.'s MKUltra establishment of the 19-year old Mark Zuckerberg as their Facebook cardboard cut out. Then, she became product vice president at AOL on Apr. 06, 2009. Then, she became Summers' chief of staff for the National Economic Council on Jan. 21, 2009. Then, she became Obama's Special Assistant to the President for Economic Policy on Jun. 24, 2010. Then, she attended an exclusive dinner with Hillary and Sandberg on Mar. 27, 2012. Then, she became chief operating officer of Instagram on Oct. 07, 2014. Truly magical.

WHITE HOUSE ROGUE INTELLIGENCE NOC (NETWORK OPERATING CENTER): NATIONAL INFRASTRUCTURE ASSURANCE COUNCIL

On Jul. 14, 1999, the Clinton White House set up a spy skunk works that has run rogue intelligence operations called the "National Infrastructure Assurance Council (NIAC)" On Jan. 18, 2001, Clinton appointed James P. Chandler, III and Bill Gates, Microsoft, as directors on NIAC the day before he left office and the same day he pardoned his former CIA director John M. Deutch (Marne L. Levin-Deutch's father in law) and fraudster Marc Rich.

On Sep. 16, 1999, Clinton announced "relaxed" encryption rules in a flurry of press releases and letters to Congress, which were most assuredly drafted by national security advisor James P. Chandler, III. This action effectively *gutted* normal engineering security practices. It had the effect of enabling unfettered foreign and domestic access to U.S. classified data.

On Sep. 29, 1999, Bill Clinton established In-Q-Tel Silicon Valley cardboard cutouts for the C.I.A. to be able to raise private venture capital funds to build its rogue operations. It is *illegal* for a government agencies to invest in private companies.

Bookmark: #in-q-tel-formed-by-cia | https://tinyurl.com/ydcmaxpp

19. **James Cole** (Deputy Attorney General, U.S. Dept. of Justice)
20. **Tony West** (Associate Attorney General, U.S. Dept. of Justice; 2008 Obama California Campaign Manager)
21. **Robert F. Bauer** (Obama Attorney; White House Chief Counsel; directed IRS targeting of the Tea Party; formerly and currently employed by Perkins Coie LLP, Facebook's "rapid response enforcement team;" spouse is Anita B. Dunn)
22. **Anita B. Dunn** (Obama Attorney; White House Chief Counsel; husband Robert F. Bauer directed IRS targeting of the Tea Party, formerly employed by Perkins Coie LLP, Facebook's "rapid response enforcement team")
23. **Mary L. Schapiro** (former Chairman, Securities & Exchange Commission (S.E.C.); holds investments in 51 Facebook Club basket funds)
24. **James "Jamie" Brigagliano** (former Deputy Director of the Division of Trading and Markets at the Securities and Exchange Commission; Mary L. Schapiro's chief lieutenant on "dark pool" rule making)
25. **Joseph P. Cutler** (Perkins Coie)
26. **David P. Chiappetta** (Perkins Coie)
27. **James R. McCullagh** (Perkins Coie)
28. **Ramsey M. Al-Salam** (Perkins Coie)
29. **Grant E. Kinsel** (Perkins Coie)
30. **Reeve T. Bull** (Gibson Dunn)
31. **Heidi Keefe** (Cooley)
32. **Michael G. Rhodes** (Cooley; Tesla Motors)
33. **Elizabeth Stameshkin** (Cooley)
34. **Donald K. Stern** (Cooley; Justice Dept. advisor)
35. **Mark R. Weinstein** (Cooley)
36. **Jeffrey Norberg** (Cooley)
37. **Ronald Lemieux** (Cooley)
38. **Craig W. Clark** (Blank Rome)
39. **Tom Amis** (Cooley / McBee Strategic)
40. **Erich Veitenheimer** (Cooley / McBee Strategic)
41. **Roel Campos** (Cooley; former Commissioner of the U.S. Securities & Exchange Commission at the time of the infamous Facebook 12(g) exemption)
42. **Lisa T. Simpson** (Orrick)
43. **Indra Neel Chatterjee** (Orrick)
44. **Samuel O'Rourke** (Facebook; Cooley-directed)
45. **Theodore W. Ullyot** (Facebook; Cooley-directed)
46. **Amber H. Rover**, aka **Amber L. Hagy** aka **Amber Hatfield** (Weil Gotshal LLP; Judge Kimberly A. Moore's former client)
47. **Edward R. Reines** (Weil Gotschal)
48. **Trish Harris** (DC Bar Association)
49. **Elizabeth A. Herman** (DC Bar Association)

Click image to enlarge

C.I.A. In-Q-Tel founding military-industrial complex technocracy trustees:

Individual:	*Organization:*
Ault III, Lee A.	Telecredit, Inc.
Augustine, Norman R.	Lockheed Martin Corporation
Brown, John Seely	Xerox Corporation
Crow, Michael M.	Columbia University
Friedman, Stephen	Goldman Sachs; Marsh & McLennan Capital, Inc.
Kaminski, Paul G.	Technovation, Inc., Global Technology Partners, U.S. Under Sec. of Defense
Kim, Jeong H.	Lucent Technologies, Yurie Systems
Mandl, Alex J.	AT&T, Teligent,Inc.
McMahon, John N.	Lockheed Missile & Space Systems Company; C.I.A.
Perry, William J.	U.S. Department of Defense, Stanford University

FIG. 15—On Sep. 29, 1999, Clinton C.I.A. *institutionalized* crony capitalism and the digital take over of America by a Shadow Government, *on this day*, by forming a "private" venture capital company named In-Q-Tel (Intel with a Q) to create a private funding and control vehicle for the rogue C.I.A.

On Nov. 12, 1999, Bill Clinton and Larry Summers abolished Glass-Steagall banking controls, enabling the banks to fund In-Q-Tel "private" companies.

On Nov. 17, 1999, Agilent Technologies went public using Robert S. Mueller's III's law firm Hale and Dorr (renamed Wilmer Hale). Agilent Technologies was tasked with building the digital infrastructure for "The Internet of Things" global mass surveillance of everything using the Richard C. Walker HP/Agilent patents for monitoring all human beings called "wet-ware" in the patents.

On Jun. 08, 2000, Clinton espionage attorney James P. Chandler, III, participated in seminal Leader invention design meetings as Leader's newly-appointed patent attorney. He was fully briefed on Leader's social networking innovations at this meeting (see photo below) without disclosing his Deep State shadow government conflicts of interest and treachery.

Bookmark: #chandler-learned-leader-innovations-jun-08-2000 | https://tinyurl.com/y9medtrp

50. **Elizabeth J. Branda** (DC Bar Association)
51. **David J. Kappos** (former Patent Office Director; former IBM chief intellectual property counsel; ordered unprecedented 3rd reexam of Leader Technologies' patent; Obama political appointee)
52. **Preetinder ("Preet") Bharara** (U.S. Attorney *Ceglia v. Zuckerberg;* formerly of Gibson & Dunn LLP; protects Zuckerberg)
53. **Thomas J. Kim** (SEC Chief Counsel)
54. **Anne Krauskopf** (SEC Special Sr. Counsel)
55. **John G. Roberts, Jr.** (Chief Justice, U.S. Supreme Court)
56. **Jan Horbaly** (Federal Circuit, Clerk of Court)
57. **Kimberly A. Moore** (Judge, Federal Circuit)
58. **Matthew J. Moore** (Latham & Watkins LLP; husband of Judge Kimberly A. Moore)
59. **Kathryn "Kathy" Ruemmler** (Latham & Watkins LLP; White House counsel)
60. **Evan J. Wallach** (Judge, Federal Circuit)
61. **Alan D. Lourie** (Judge, Federal Circuit)
62. **Randall R. Rader** (Chief Judge, Federal Circuit)
63. **Terence P. Stewart** (Federal Circuit Bar Association)
64. **Leonard P. Stark** (Judge, Delaware U.S. District Court)
65. **Richard J. Arcara** (Judge, N.Y. Western District, *Ceglia v. Holder et al*)
66. **Allen R. MacDonald** (Administrative Judge, U.S. Patent Office)
67. **Stephen C. Siu** (Administrative Judge, U.S. Patent Office)
68. **Meredith C. Petravick** (Administrative Judge, U.S. Patent Office)
69. **James T. Moore** (Administratie Judge, U.S. Patent Office)
70. **Pinchus M. Laufer** (Sr. Counsel, Patent Trial and Appeal Board, PTAB)
71. **Kimberly Jordan** (Counsel, Patent Trial and Appeal Board, PTAB)
72. **Daniel J. Ryman** (Counsel, Patent Trial and Appeal Board, PTAB)
73. **William J. Stoffel** (Counsel, Patent Trial and Appeal Board, PTAB)
74. **James C. Payne** (Counsel, Patent Trial and Appeal Board, PTAB)
75. **Deandra M. Hughes** (Examiner, *Leader v. Facebook* reexamination)
76. **Kathryn Walsh Siehndel** (FOIA Counsel, U.S. Patent Office - bio and conflicts log concealed)
77. **Dennis C. Blair** (Director, U.S. National Intelligence)
78. **Dennis F. Saylor, IV** (Judge, Foreign Intelligence Surveillance Court, FISA)
79. **James E. Boasberg** (Judge, Foreign Intelligence Surveillance Court, FISA)

FIG. 16—ON JUN. 08, 2000, JAMES P. CHANDLER, IIII, BILL CLINTON SPY MASTER first learned about Leader/McKibben's social networking designs in early 2000. By this meeting on Jun. 8, 2000 he was studying every detail. Chandler is pictured here seated in the white shirt against the wall on the right side of this photo with his legal assistant Kelley E. Clements to the viewer's right. Co-inventor Michael McKibben and Jeffrey Lamb are picture standing in the back left of the photo. *Photo*: Leader Technologies, Inc.

On Jun. 20, 2000, Sir Geoffrey E. Pattie was awarded the ISSA Silver Star Award in Washington, D.C. Pattie is the primary spy director for the Queen's Privy Council and founder of SCL Ltd. and Cambridge Analytica—two C.I.A. MKUltra mind control and brain washing operations in the UK.

On Aug. 25, 2000, F. Gary Davis, Acting Director of the U.S. Office of Government Ethics, issued a tortured 13-page "advisory" that dramatically muddied the waters on mutual fund investing disclosure. Davis left government service soon thereafter. This opinion opened the door to massive nondisclosure fraud by politicians, SES and federal bureaucrats.

In 2001, NSA Director Michael V. Hayden recommended expansion of the NSA's Senior Executive Service (SES) programs.

On Apr. 15, 2001, C.I.A. whistleblower Susan Lindauer warned American senior intelligence leadership that "I first learned of the 9/11 Conspiracy from my CIA handler, Dr. Richard Fuisz, in mid-April, 2001." She was *imprisoned* for a year without due process to shut her up as the first casualty of The Patriot Act.

In Jul. 2001, Department of Justice John C. Yoo was hired into the Office of Legal Counsel (OLC) and gave legal opinion cover for a proposed NSA project "Stellar Wind" for mass surveillance of American citizens.

80. **James P. Chandler, III** (President, National Intellectual Property Law Institute, NIPLI; The Chandler Law Firm Chartered; advisor to Asst. Att'y Gen. Eric H. Holder, Jr., Dept. of Justice; Member, National Infrastructure Assurance Commission, NIAC; advisor to Federal Circuit Chief Judge Randall R. Rader; advisor to Sen. Orrin Hatch; author, The Federal Trade Secrets Act and the Economic Espionage Act of 1996; Leader Technologies' legal counsel, along with Fenwick & West LLP)

C. Facebook puppet masters:

81. **President Barack Obama** (appointed Leonard P. Stark to the judge's seat in Delaware Federal District Court eight days after Stark's court allowed Facebook to get away with jury and court manipulation of an on-sale bar verdict which was attained without a single piece of hard evidence; Barack and Michelle Obama were evidently protecting their 47 million "likes" on Facebook)
82. **Lawrence "Larry" Summers** (Harvard President who aided Zuckerberg's light-speed rise to prominence with unprecedented *Harvard Crimson* coverage; Obama bailout chief; Clinton Treasury Secretary; World Bank Chief Economist; "Special Advisor" to Marc Andreessen in Instagram; co-creator of the current Russian robber baron economy; close 20-year relationships with protégés Sheryl Sandberg & Yuri Milner; aided in recommendations that *created* the Russian robber baron economy—and Yuri Milner/DST/Asmanov's money used to purchase Facebook stock)
83. **James W. Breyer, Accel Partners LLP;** Facebook director; client of Fenwick & West LLP since the 1990's; apparently received technology from other Fenwick clients that was shuffled to Zuckerberg, incl. Leader Technologies' inventions)
84. **David Plouffe**; directed Obama's 2008 and 2012 campaigns; a self-described "statistics nerd;" likely directed the activities of the Facebook Club; employed Robert F. Bauer, Perkins Coii LLP in 2000 at the Democratic Congressional Campaign Committee
85. **McBee Strategic** (one of the main "private" arms responsible for dolling out the billions in Obama "green energy" stimulus funds; partnered with Cooley Godward LLP)
86. **Mike Sheehy** (Cooley-McBee Strategic principal; former National Security Adviser to House Speaker Nancy Pelosi)
87. **Nancy Pelosi** (U.S. Congresswoman; appears to be running political cover in the House for Facebook, McBee Strategic, Cooley Godward, Fenwick & West, Breyers, etc.)
88. **Harry Reid** (U.S. Senator; Judge Evan J. Wallach patron)
89. **Thomas J. Kim** (SEC, Chief Counsel & Assoc. Director) approved

On Sep. 04, 2001, Robert S. Mueller, III was sworn in as FBI Director by President George W. Bush, just 10 days before 9/11.

On Sep. 11, 2001, World Trade Center, Pentagon and Shanksville "terror" attacks were timed simultaneously with DoD NORAD war games and a stand down order.

On Oct. 04, 2001, President Bush approves operation "Stellar Wind" mass surveillance on American citizens.

On Oct. 16, 2001, President Bush signed Executive Order 13231 "Critical Infrastructure Protection in the Information Age" forming the "National Infrastructure Advisory Council (NIAC)." The order used the same NIAC acronym used by Clinton as the excuse for setting up a mass surveillance networking operating center run out of the White House.

On Oct. 26, 2001, President Bush signed The Patriot Act that has essentially destroyed the Bill of Rights. Just look at the flies that gathered to watch the signing.

Bookmark: #patriot-act-signed | https://tinyurl.com/y8zvjr4x

FIG. 17—On Oct. 26, 2001, a 132-page, seemingly ready-made USA PATRIOT Act was approved by an Act of Congress that was signed into law by President George W. Bush on October 26, 2001. With its ten-letter abbreviation (USA PATRIOT) expanded, the full title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001."

On Oct 31, 2001, NSA whistleblower and former chief architect William E. Binney resigned the NSA saying the agency had "gone rogue."

On Nov. 29, 2001, IBM intellectual property attorneys James P. Chandler, III and David J. Kappos used a $40 million IBM "donation" to start the IBM Eclipse Foundation which has been

Facebook's 500-shareholder exemption on Oct. 14, 2007, one day after it was submitted by Fenwick & West LLP; Facebook used this exemption to sell $3 billion insider stock to the Russians Alisher Asmanov, Yuri Milner, DST, Digital Sky, Mail.ru which pumped Facebook's pre-IPO valuation to $100 billion; another Harvard grad, Kim worked at Latham & Watkins LLP which was the chief lobbyist for the National Venture Capital Association in 2002-2004 whose Chairman was . . . James W. Beyer, Accel Partners LLP; in other words Breyer and Kim, both Harvard grads, were associated at the time of the Zuckerberg hacking and theft of Leader Technologies' software code)

90. **Ping Li** (Accel Partners, Zuckerberg handler)
91. **Jim Swartz** (Accel Partners; Zuckerberg handler)
92. **Sheryl K. Sandberg** (Facebook, Summers protégé; Facebook director)
93. **Yuri Milner** (DST aka Digital Sky, Summers protégé; former Bank Menatep executive; Facebook director)
94. **Alisher Asmanov** (DST aka Digital Sky; Goldman Sachs Moscow partner; Russian oligarch; Friend of the Kremlin; Became the Richest Man in Russia after the Facebook IPO)
95. **Marc L. Andreessen** (Zuckerberg coach; client of Fenwick & West LLP and Christopher P. King *aka* Christopher-Charles King *aka* Christopher King *aka* Christopher-Charles P. King; Summers' sponsor during Instagram-scam; Facebook director)
96. **Peter Thiel** (19-year old Zuckerberg coach; PayPal; Facebook director; CEO, Clarion Capital)
97. **Clarion Capital** (Peter Thiel)
98. **Reid G. Hoffman** (19-year old Zuckerberg coach; PayPal; LinkedIn; Facebook director)
99. **Richard Wolpert** (Accel Partners)
100. **Robert Ketterson** (Fidelity Ventures; Fidelity Equity Partners; Fidelity Ventures Telecommunications & Technology)
101. **David Kilpatrick** (*Business Insider*; "The Facebook Effect"; PR cleanse-meister re. Facebook origins)
102. **Zynga/Groupon/LinkedIn/Square/Instagram** ("Facebook Money/Credits/Bitcoin" feeder companies)
103. **Tesla Motors** (received $465 million in Obama stimulus funds and hired Cooley's Michael Rhodes in the seven months before the *Leader v. Facebook* trial, just before veteran Judge Joseph Farnan made the surprise announcement of his retirement, just six days after Facebook's disasterous *Markman* Hearing)
104. **Solyndra** (received $535 million in Obama stimulus at the recommendation of the Cooley-McBee Strategic "consulting" alliance)
105. **BrightSource** (received $1.6 billion in Obama stimulus at the

the exclusive distributor of Leader Technologies' social networking innovations.

On Aug. 29, 2002, IBM Eclipse Foundation distributed Version 2.0.1 that included all of Leader Technologies' social networking innovations.

On Sep. 18, 2002, career IBMer Thomas E. Noonan (Internet Security Systems, Inc.) was appointed to the National Infrastructure Assurance Council (NIAC) by George W. Bush, surely recommended by James P. Chandler, and he remains a member of the Council to this day. In 2003, Noonan became a partner to ENTRUST INC. Public Key Infrastructure (PKI) controlled by Hillary Clinton.

On Dec. 04, 2002, the entire Silicon Valley military-industrial complex began joining the IBM Eclipse Foundation to receive Leader Technologies' social networking invention source code, all of which IBM criminally claimed copyright, and then criminally declared "open source." They admitted a "single company [Leader Technologies]" for their code.

Bookmark: #ibm-eclipse-distributes-stolen-leader-social-networking-invention | https://tinyurl.com/y9mmr36z

recommendation of the Cooley-McBee Strategic "consulting" alliance)

106. **John P. Breyer** (father of James W. Breyer; founder of IDG Capital Partners - China; coached his son on exploiting Western markets while he quietly built a venture capital business in China for the last 20 years; the real brain behind the Breyer exploitations
107. **IDG Capital Partners (China)** (founded by John P. Breyer, the father of James W. Breyer, Accel Partners; the current launderer of the tens of billions James W has fleeced from the U.S. market from the bailout, stimulus and the "pump & dump" Facebook IPO schemes)
108. **Goldman Sachs** (received US bailout funds; then invested with DST in Facebook private stock via Moscow; took Facebook public; *locked out* American investors from investing)
109. **Morgan Stanley** (received US bailout funds; took Facebook public; probably participated in oversees purchases of Facebook private stock before IPO)
110. **State Street Corporation** (received U.S. taxpayer bailout monies along with Goldman Sachs and Morgan Stanley; consolodating control of ATM banking networks internationally
111. **JP Morgan Chase** (received U.S. taxpayer bailout monies along with Goldman Sachs, Morgan Stanley and State Street Corporation)
112. **Lloyd Blankfein** (Goldman Sachs, CEO)
113. **Jamie Dimon** (JP MorganChase, CEO)
114. **Steve Cutler** (JP MorganChase, General Counsel)
115. **Rodgin Cohen** (JP MorganChase, Outside Counsel; Sullivan Cromwell, LLP)
116. **U.S. Securities & Exchange Commission** (granted Fenwick & West's application on behalf of Facebook for an unpredented exemption to the 500 shareholder rule; opened the floodgated for Goldman Sachs and Morgan Stanley to make a private market in Facebook pre-IPO insider stock; facilitated the influx of billions of dollars from "dubious" sources associated with Russian oligarchs, Alisher Asmanov and Yuri Milner, and the Kremlin; Goldman Sachs is a partner with this Moscow company, Digital Sky Technologies, aka DST, aka Mail.ru)
117. **Jeff Markey** (McBee Strategic LLC; allied with Facebook's Cooley Godward Kronish LLP to arrange Obama's green energy funding; arranged $1.6 billion for failed BrightSource and $535 million for failed Solyndra)
118. **Steve McBee** (McBee Strategic LLC; allied with Facebook's Cooley Godward Kronish LLP to arrange Obama's green energy funding; arranged $1.6 billion for failed BrightSource and $535 million for failed Solyndra)
119. **Michael F. McGowan** (Stroz Friedberg; Facebook forensic expert who lied about his knowledge of the

Minutes of the Eclipse Board Meeting
December 4, 2002

The fifth meeting of the Eclipse Board was held from 9:30 AM to 4:30 PM CST on Wednesday, Dec 4, 2002 at the Hyatt Regency (Airport) in Dallas, Texas.

The following are the minutes of this meeting.

Stewards in Attendance

AltoWeb	Elli Albek
Borland	Simon Thornhill
Catalyst Systems	Tracy Ragan
Flashline	Adam Wallace
Fujitsu	Ronald Alepin
HP	Mike Rank
Hitachi	Ryuji Takamuki & Koichi Yokota
IBM	Lee Nackman
Instantiations	Mike Taylor
MKS	Dave Martin
Oracle	Ted Farrell
Parasoft	Roman Salvador
QNX	Dan Dodge
Rational	Dave Bernstein
Red Hat	Michael Tiemann
SAP	Michael Bechauf
Scapa Technologies	Mike Norman
Serena Software	Boris Kapitanski
SlickEdit	Ed Hintz
SuSE	Juergen Geck
TeamStudio	Ian Smith
Telelogic	Tony Chang
TimeSys	Manas Saksena
TogetherSoft	Todd Olson

Stewards who voted electronically

MontaVista Software	Jim Ready
Sybase, Inc	Karl Reti

Associate Members in Attendance

Academic & Research	Brian Barry
Object Management Group	Jamie Nemiah for Richard Soley

Eclipse representatives in Attendance

Eclipse Chairperson	Skip McGaughey
Eclipse Tools PMC	John Duimovich
Eclipse Platform PMC	Dave Thomson
Eclipse Platform PMC	John Wiegand
Eclipse Technology PMC	Brian Barry
Eclipse Communications	Marc Erickson

Invited Guests

QNX	Linda Campbell

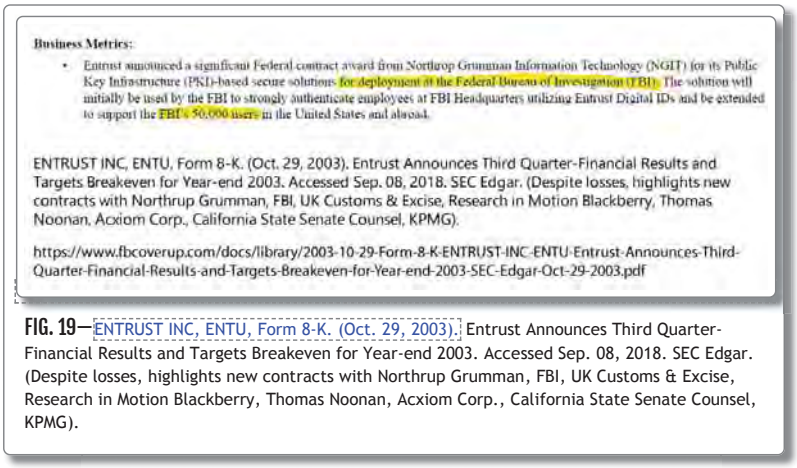
FIG. 18—On Dec. 04, 2002, Eclipse released Version 1.0.1. The development effort set as its priority to change the Leader SWING design to SWT to conform to IBM preferences. They disclosed everything except Leader's name in the statement: *"Eclipse 2.0 was based primarily on contributions of a single company [Leader Technologies, Inc.]."*

On Oct. 29, 2003, ENTRUST INC was awarded the contract to supply all 50,000 encryption keys for the Federal Bureau of Investigation (FBI).

Bookmark: #fbi-entrust-conspiracy | https://tinyurl.com/ycscm59j

contents of the 28 Zuckerberg hard drives and Harvard Email accounts)

120. **Bryan J. Rose** (Stroz Friedberg; Facebook forensic expert who lied about his knowledge of the contents of the 28 Zuckerberg hard drives and Harvard Email accounts)
121. **Dr. Saul Greenberg** (Facebook's expert witness from the University of Calgary; disingenuously waived his hands and said he would be "wild guessing" about the purpose of a Java "sessionstate" import statement (even Java newbies know it is used for tracking a user while in a web session); in short, Dr. Greeberg lied to the jury, thus discrediting his testimony)
122. **Toni Townes-Whitley** (CGI Federal; Michelle Obama's 1985 Princeton classmate; CGI "donated" $47 million to the Obama campaign; CGI won the no-bid contract to build the www.healthcare.gov Obamacare website; CGI shut off the security features on Obama's reelection donation sites to increase donations)
123. **CGI Federal** (US division of a Canadian company; Donated $47 million to Obama's reelection, then received the no-bid contract to build the ill-fated Obamacare website; Michelle Obama's Princeton classmate, Toni Townes-Whitely, is a Senior Vice President of CGI; the website is replete with social features and links to Facebook)
124. **Kathleen Sebelius** (Obama's Secretary of Health & Human Services since 2009 responsible for $678 million Obamacare implementation; made the decision to hire CGI Federal on a no-bid contract despite the evident conflict of interest with Michelle Obama and $47 million in Obama campaign donations by CGI; the website is replete with social features and links to Facebook)
125. **Todd Y. Park** (White House Chief Technology Officer (CTO); former CTO for Health & Human Services; chief architect of HealthCare.gov; founder, director, CEO, Athenahealth, Inc.; founder, director, CEO, Castlight Health, Inc.)
126. **Frank M. Sands, Sr. / Frank M. Sands, Jr.** (Founder and CEO, respectively, of Sands Capital Management LLC; failed to file S.E.C. Form SC 13G acquisition reports for Athenahealth, Inc., Baidu, Inc. (ADR) and Facebook stock during 2012; masked the association of Todd Y. Park with Athenahealth, Inc. and Baidu, Inc., and the association of both of those companies with the Facebook IPO fraud)
127. **Robin "Handsome Reward" Yangong Li** (CEO, Baidu, Inc. (ADR); appointed Jan. 2004, the same month that Mark Zuckerberg obtained Leader Technologies' social networking source code to start Facebook; **Robin Y. Li** is very likely associated with John P. and James W. Breyer through their Chinese entities, including IDG Capital Partners, IDG-Accel and other variants; Li appointed a junior attorney from Fenwick & West LLP, Palo Alto/Mountain View, namely Parker Zhang, to be his "Head of Patents;" Fenwick & West LLP



Business Metrics:

- Entrust announced a significant Federal contract award from Northrop Grumman Information Technology (NGIT) for its Public Key Infrastructure (PKI)-based secure solutions for deployment at the Federal Bureau of Investigation (FBI). The solution will initially be used by the FBI to strongly authenticate employees at FBI Headquarters utilizing Entrust Digital IDs and be extended to support the FBI's 50,000 users in the United States and abroad.

ENTRUST INC, ENTU, Form 8-K. (Oct. 29, 2003). Entrust Announces Third Quarter-Financial Results and Targets Breakeven for Year-end 2003. Accessed Sep. 08, 2018. SEC Edgar. (Despite losses, highlights new contracts with Northrup Grumman, FBI, UK Customs & Excise, Research in Motion Blackberry, Thomas Noonan, Acxiom Corp., California State Senate Counsel, KPMG).

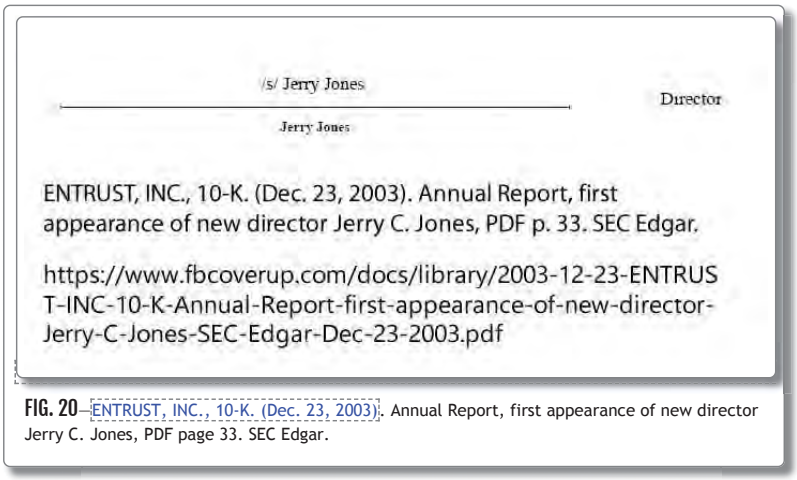
https://www.fbcoverup.com/docs/library/2003-10-29-Form-8-K-ENTRUST-INC-ENTU-Entrust-Announces-Third-Quarter-Financial-Results-and-Targets-Breakeven-for-Year-end-2003-SEC-Edgar-Oct-29-2003.pdf

FIG. 19—ENTRUST INC, ENTU, Form 8-K. (Oct. 29, 2003). Entrust Announces Third Quarter-Financial Results and Targets Breakeven for Year-end 2003. Accessed Sep. 08, 2018. SEC Edgar. (Despite losses, highlights new contracts with Northrup Grumman, FBI, UK Customs & Excise, Research in Motion Blackberry, Thomas Noonan, Acxiom Corp., California State Senate Counsel, KPMG).

On Dec. 04, 2003, ENTRUST INC elected Jerry C. Jones as a "Class I" director to replace retiring Gen. Wesley K. Clark. Jones is a 19-year Hillary Clinton partner at the Rose Law Firm, Little Rock, Arkansas. With the appointment of Jones, FBI Director Robert S. Mueller, III had an ethical duty to disclose to the public that his approval of ENTRUST INC to manage 50,000 FBI encryption keys enabled his political mentor Hillary Clinton to have full access to the entire FBI operation.

Bookmark: #fbi-entrust-mueller-jones-hillary-conspirators | https://tinyurl.com/y8fsqmjl

Bookmark: #jones-secretly-elected-entrust-director | https://tinyurl.com/yamr7zad



/s/ Jerry Jones

Jerry Jones

Director

ENTRUST, INC., 10-K. (Dec. 23, 2003). Annual Report, first appearance of new director Jerry C. Jones, PDF p. 33. SEC Edgar.

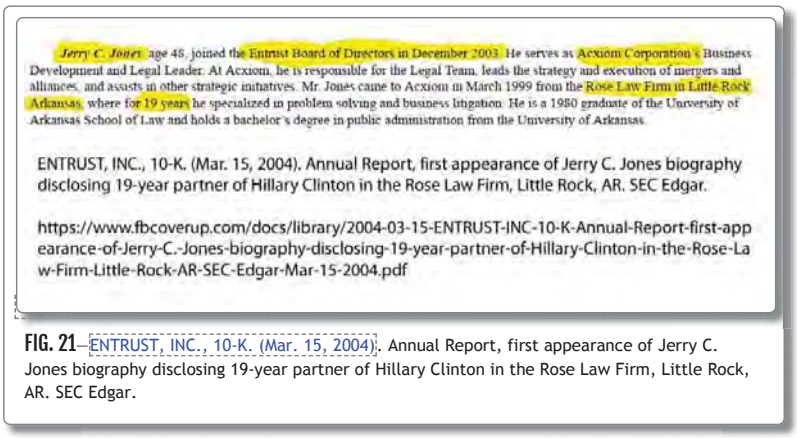
https://www.fbcoverup.com/docs/library/2003-12-23-ENTRUST-INC-10-K-Annual-Report-first-appearance-of-new-director-Jerry-C-Jones-SEC-Edgar-Dec-23-2003.pdf

FIG. 20—ENTRUST, INC., 10-K. (Dec. 23, 2003). Annual Report, first appearance of new director Jerry C. Jones, PDF page 33. SEC Edgar.

represented both Leader Technologies, Inc. and Accel Partners LLC in 2002-2003 and had Leader's source code in their files.)

128. **Parker Zhang** ("Head of Patents" at Baidu, Inc. (ADR), appointed in approx. May 2012; formerly a junior Associate attorney at Fenwick & West LLP; graduate from Michigan Law in 2005)
129. **Penny S. Pritzker** (Secretary, Department of Commerce; replaced Rebecca M. Blank; holds over $24 million in Facebook "dark pools" stock, most notably in Goldman Sachs, Morgan Stanley and JPMorgan)
130. **Rebecca M. Blank** (Secretary, Department of Commerce; oversaw the dubious Leader v. Facebook activities of the Patent Office Director, David J. Kappos, who held over one million dollars in Facebook "dark pools" during the *Leader v. Facebook* proceedings; Kappos purchased this stock within weeks of his surprise recess appointment by President Obama; Kappos also was formerly employed by IBM, who sold Facebook 750 patents during the *Leader v. Facebook* proceedings; right before leaving the Patent OFfice, Kappos also ordered an unprecedented 3rd reexamination of Leader's patent without even identifying claims)
131. **Mary L. Schapiro** (Chairman, Securities & Exchange Commission; holds 51 Facebook "dark pools" stocks which held stock in Facebook, Baidu and more than a dozen Facebook crony companies; failed to regulate the "dark pools;" failed to disclose her substantial conflict of interest in regulating the run up to the Facebook IPO)
132. **Robert C. Hancock** (Chief Compliance Officer, Sands Capital Management, LLC; failed to file S.E.C. Form SC 12G notice of acquisition reports for Athenahealth, Baidu and Facebook during the period of the Facebook IPO in 2012; this conduct masked the conflicts of interest of Todd Y. Park, who was appointed by President Obama to be the U.S. Chief Technology Officer during this same period; Todd Y. Park is/has been founder, director and CEO of both Athenahealth and Castlight Health; Todd Y. Park deeply embedded the software from Athenahealth and Castlight Health into HealthCare.gov when he was CTO at Health & Human Services; none of these conflicts of interest were disclosed; Todd Y. Park's ethics pledges and reports are missing from the Office of Government Ethics)
133. **Jonathan Goodman** (Chief Counsel, Sands Capital Management, LLC; failed to file S.E.C. Form SC 12G notice of acquisition reports for Athenahealth, Baidu and Facebook during the period of the Facebook IPO in 2012; this conduct masked the conflicts of interest of Todd Y. Park, who was appointed by President Obama to be the U.S. Chief Technology Officer during this same period; Todd Y. Park is/has been founder, director and CEO of both Athenahealth and Castlight Health; Todd Y. Park deeply embedded the software from Athenahealth and Castlight Health

Bookmark: #jones-bio-first-published-by-entrust | https://tinyurl.com/y7ehyw3y



Jerry C. Jones, age 48, joined the Entrust Board of Directors in December 2003. He serves as Acxiom Corporation's Business Development and Legal Leader. At Acxiom, he is responsible for the Legal Team, leads the strategy and execution of mergers and alliances, and assists in other strategic initiatives. Mr. Jones came to Acxiom in March 1999 from the Rose Law Firm in Little Rock, Arkansas, where for 19 years he specialized in problem solving and business litigation. He is a 1980 graduate of the University of Arkansas School of Law and holds a bachelor's degree in public administration from the University of Arkansas.

ENTRUST, INC., 10-K. (Mar. 15, 2004). Annual Report, first appearance of Jerry C. Jones biography disclosing 19-year partner of Hillary Clinton in the Rose Law Firm, Little Rock, AR. SEC Edgar.

https://www.fbcoverup.com/docs/library/2004-03-15-ENTRUST-INC-10-K-Annual-Report-first-appearance-of-Jerry-C.-Jones-biography-disclosing-19-year-partner-of-Hillary-Clinton-in-the-Rose-Law-Firm-Little-Rock-AR-SEC-Edgar-Mar-15-2004.pdf

FIG. 21—ENTRUST, INC., 10-K. (Mar. 15, 2004). Annual Report, first appearance of Jerry C. Jones biography disclosing 19-year partner of Hillary Clinton in the Rose Law Firm, Little Rock, AR. SEC Edgar.

On Sep. 09, 2008, the IBM Eclipse Foundation boasted 191 members [Silicon Valley allies of the fascist Senior Executive Service (SES)] , including Microsoft, AT&T, Verizon, Facebook, Google, YouTube, SAP, Cisco, Oracle, HP, Samsung, Motorola, Nokia, Sony, JPMorgan Chase, Goldman Sachs and Tsinghua University (Beijing, China). Most if not all of these companies are ENTRUST INC (or sublicenser) clients, and probably all of them embed the NSA Dual_EC_DRBG encryption backdoor key algorithm in their hardware, software and firmware. See AFI (Nov. 06, 2015). Complicit encryption geeks enable the American spy state. *Americans for Innovation*.

Bookmark: #ibm-eclipse-membership-sep-17-2008 | https://tinyurl.com/y9xntl6j

FIG. 22—IBM Eclipse Foundation Members, page 1, prepared as of Sep. 09, 2008 and reported to the Board of Directors on Sep. 17, 2008. Click here for image of page 2.

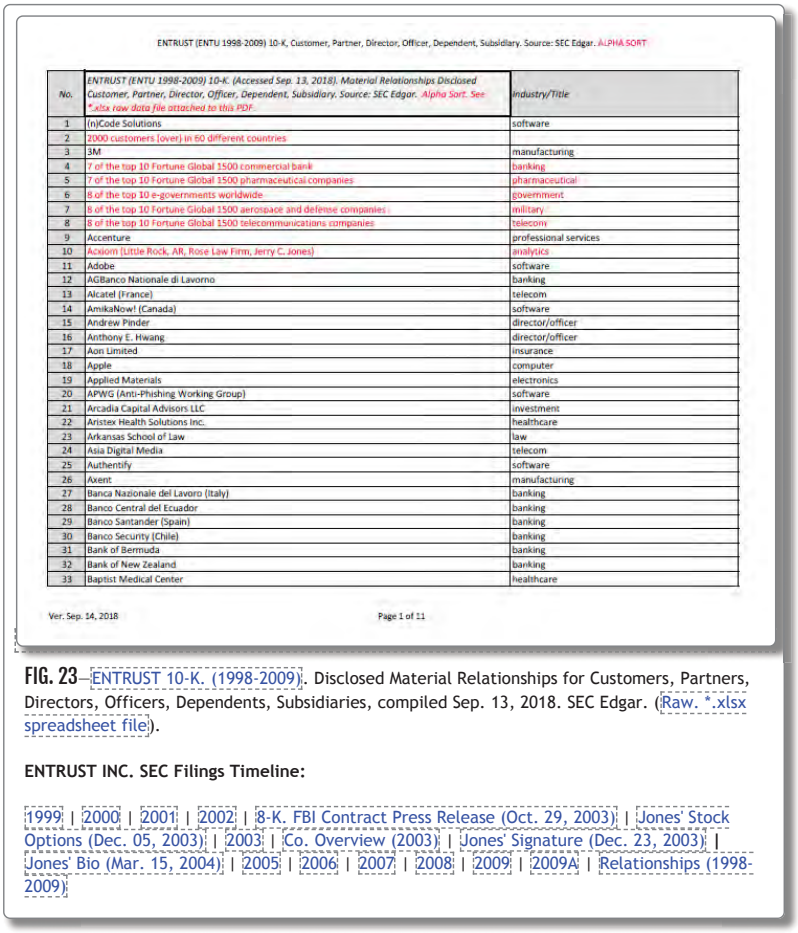
into HealthCare.gov when he was CTO at Health & Human Services; none of these conflicts of interest were disclosed; Todd Y. Park's ethics pledges and reports are missing from the Office of Government Ethics; Goodman was formerly employed by Gibson Dunn LLP, Facebook appeals counsel in *Leader v. Facebook*)

134. **Trip Adler** ("Co-Founder" of Scribd; Harvard contemporaries of Mark Zuckerberg with a dubious orgins story, like Zuckerberg's; Scribd held AFI documents for two years, then summarily deleted the entire library without warning on Fri. Mar. 7, 2014; AFI's library contained only public documents and much evidence proving the *Leader v. Facebook* judicial corruption)
135. **Jared Friedman** ("Co-Founder" of Scribd; Harvard contemporaries of Mark Zuckerberg with a dubious orgins story, like Zuckerberg's; Scribd held AFI documents for two years, then summarily deleted the entire library without warning on Fri. Mar. 7, 2014; AFI's library contained only public documents and much evidence proving the *Leader v. Facebook* judicial corruption)
136. **Jeffrey Wadsworth** (CEO, Battelle Memorial Institute; President, Ohio State University Board of Trustees; former Deputy Director of Science & Technologies, Lawrence Livermore National Laboratory, University of California Board of Trustees)
137. **Michael V. Drake** (President, The Ohio State University; former Chancellor, University of California, Irvine)
138. **Woodrow A. Myers** (Chief Medical Officer, Wellpoint, Inc.; formerly Corporate Operations Officer, Anthem Blue Cross Blue Shield of Indiana)
139. **Alex R. Fischer** (aka Alexander Ross Fischer; Trustee, The Ohio State University; former Sr. Vice President, Battelle Memorial Institute; Chairman, OmniViz; married to Lori Barreras)
140. **Chris Glaros** (author of the discredited Waters Report re. The Ohio State University Marching Band; protege of Eric H. Holder, Jr., Professor James P. Chandler, III, and Algernon L. Marbley)
141. **Lori Barreras** (Commissioner, Ohio Civil Rights Commission; former Vice President of Human Resources, The Ohio State University; former Vice President, Battelle Memorial Institute; married to Alex R. Fischer)
142. **David Vaughn** (Criminal Attorney, David Vaughn Consulting Group; former Assistant U.S. Attorney; appointed to the discredited Waters Commission at Ohio State)
143. **Betty Montgomery** (former Ohio Attorney General; appointed to the discredited Waters Commission at Ohio State; accepted campaign contributions from Woodrow A. Myers, Wellpoint, Inc. and friend of Michael V. Drake)
144. **Joseph A. Steinmetz** (Provost, The Ohio State University; author of Psychological Science article on

See The Eclipse Foundation (Sep. 09, 2008). Membership Logos [Board minutes]; *See* also The Eclipse Foundation (Sep. 17, 2008). The Members of Eclipse, Minutes of the Eclipse Board Meeting, Sep. 17, 2008; AFI. (Jan. 15, 2015). IBM plots digital control with federal judges; steals inventions, p. 6.

On Mar. 11, 2009, ENTRUST INC. issued its last 10-K annual report before selling its operation to Orlando Bravo and his Thoma Bravo, LLC private equity firm in San Francisco, CA. They disclosed that they had "more than 2,000 customers in 60 different countries."

Bookmark: #entrust-relationships | https://tinyurl.com/y77rkg4q



ENTRUST (ENTU 1998-2009) 10-K, Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. ALPHA SORT

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	Industry/Title
1	(n)Code Solutions	software
2	2000 customers [over] in 60 different countries	
3	3M	manufacturing
4	7 of the top 10 Fortune Global 1500 commercial bank	banking
5	7 of the top 10 Fortune Global 1500 pharmaceutical companies	pharmaceutical
6	8 of the top 10 e-governments worldwide	government
7	8 of the top 10 Fortune Global 1500 aerospace and defense companies	military
8	8 of the top 10 Fortune Global 1500 telecommunications companies	telecom
9	Accenture	professional services
10	Acxiom (Little Rock, AR, Rose Law Firm, Jerry C. Jones)	analytics
11	Adobe	software
12	AGBanco Nationale di Lavorno	banking
13	Alcatel (France)	telecom
14	AmikaNow! (Canada)	software
15	Andrew Pinder	director/officer
16	Anthony E. Hwang	director/officer
17	Aon Limited	insurance
18	Apple	computer
19	Applied Materials	electronics
20	APWG (Anti-Phishing Working Group)	software
21	Arcadia Capital Advisors LLC	investment
22	Aristex Health Solutions Inc.	healthcare
23	Arkansas School of Law	law
24	Asia Digital Media	telecom
25	Authentify	software
26	Axent	manufacturing
27	Banca Nazionale del Lavoro (Italy)	banking
28	Banco Central del Ecuador	banking
29	Banco Santander (Spain)	banking
30	Banco Security (Chile)	banking
31	Bank of Bermuda	banking
32	Bank of New Zealand	banking
33	Baptist Medical Center	healthcare

Ver. Sep. 14, 2018 Page 1 of 11

FIG. 23—ENTRUST 10-K. (1998-2009). Disclosed Material Relationships for Customers, Partners, Directors, Officers, Dependents, Subsidiaries, compiled Sep. 13, 2018. SEC Edgar. (Raw. *.xlsx spreadsheet file).

ENTRUST INC. SEC Filings Timeline:

1999 | 2000 | 2001 | 2002 | 8-K. FBI Contract Press Release (Oct. 29, 2003) | Jones' Stock Options (Dec. 05, 2003) | 2003 | Co. Overview (2003) | Jones' Signature (Dec. 23, 2003) | Jones' Bio (Mar. 15, 2004) | 2005 | 2006 | 2007 | 2008 | 2009 | 2009A | Relationships (1998-2009)

On Jul. 16, 2009, ENTRUST, INC. proposed to shareholders to sell to Orlando Bravo and his Thoma Bravo, LLC private equity firm in San Francisco, CA., which occurred on Aug. 07, 2009.

CONCLUSIONS:

MOOC (Massive Open Online Course) that triggered the discovery of massive double-dealing and fraud within the Ohio State trustees)

D. Facebook boy-puppets:

145. **Mark E. Zuckerberg**
146. **Chris Hughes**
147. **Dustin Moskowitz**
148. **Eduardo Saverin**
149. **Matthew R. Cohler**
150. **Elon Musk**

E. *Corruption Watch*—Patent Office Judges:

151. **Anderson, Gregg**
152. **Best, George**
153. **Bonilla, Jackie W.**
154. **Boucher, Patrick**
155. **Braden, Georgianna W.**
156. **Branch, Gene**
157. **Bisk, Jennifer Bresson**
158. **Bui, Hung H.**
159. **Busch, Justin**
160. **Clements, Matt**
161. **Crumbley, Kit**
162. **Droesch, Kristen**
163. **Elluru, Rama**
164. **Fitzpatrick, Michael**
165. **Gerstenblith, Bart A.**
166. **Giannetti, Thomas L.**
167. **Guest, Rae Lynn**
168. **Hastings, Karen M.**
169. **Hoff, Marc**
170. **Horner, Linda**
171. **Hughes, James R.**
172. **Hume, Larry**
173. **James, Housel**
174. **Jung, Hung J.**
175. **Kamholz, Scott**
176. **Katz, Deborah**
177. **Lucas, Jay**
178. **MacDonald, Allen R.** (bio unavailable) – *Leader* 3rd reexam judge (bio and conflicts log concealed by FOIA)
179. **Mahaney, Alexandra**
180. **Martin, Brett**
181. **McKone, Dave**
182. **McNamara, Brian**
183. **Medley, Sally**
184. **Moore, Bryan**
185. **Moore, James T** – *Leader* 3rd reexam judge (bio and conflicts log concealed by FOIA)
186. **Morgan, Jason V.**
187. **Morrison, John**
188. **Pak, Chung K.**
189. **Perry, Glenn J.**
190. **Petravick, Meredith C.** (bio and conflicts log concealed by FOIA) – *Leader* 3rd reexam judge
191. **Pettigrew, Lynne**

Conclusion #1: Robert S. Mueller, III had an affirmative duty to disclose his approval of the contract for ENTRUST to manage the FBI's 50,000 encryption keys in late 2003. The FBI itself has been scandalously compromised to Hillary Clinton and the Rose Law Firm ever since.

Conclusion #2: ENTRUST's planetary control of the encryption keys for "over 2000 customers in 60 different countries" means that any matter handled by their customers at the FBI, Department of State, NSA, Treasury, etc. is the fruit of a poisonous tree—tainted by Clinton corruption.

Conclusion #3: President Trump has enough evidence here to *seize and prosecute* the leaders of every government agency that has involved that agency, or induced other agencies to work with ENTRUST, without disclosing their *total compromise* to Hillary Clinton and her crime syndicate.

Clearly, Hillary Clinton's director surrogate at ENTRUST, INC., Jerry C. Jones (2003-2009), steered the development of the company's control over encryption keys for the maximum benefit of his Clinton overlords.

At a bare minimum, Mueller and the FBI leadership has had an ethical duty ever since Jerry C. Jones became an ENTRUST director to disclose his direct conflict of interest and compromise of FBI operations by Hillary Clinton, his mentor.

* * *

Return to return to the beginning of this post.

Posted by K. Craine at 5:45 PM 44 comments:

Home Older Posts

Subscribe to: Posts (Atom)

192. **Praiss, Donna**
193. **Quinn, Miriam**
194. **Reimers, Annette**
195. **Saindon, William**
196. **Scanlon, Patrick**
197. **Siu, Stephen C.** – *Leader* 3rd reexam judge (bio and conflicts log concealed by FOIA)
198. **Smith, James Donald**
199. **Smith, Neil**
200. **Snedden, Sheridan**
201. **Song, Daniel**
202. **Spahn, Gay Ann**
203. **Strauss, Mike**
204. **Timm, Catherine**
205. **White, Stacey**
206. **Zecher, Michael**

Research Tip:
Type any name or subject in the Google search at the top of this webpage. That will show you any relevant links within the sites that we have been following and investigating in the *Leader v. Facebook* case. Vigilance everyone! Our American Republic is at risk.

HOW TO FILE A FRAUD COMPLAINT AGAINST A UNIVERSITY

The following universities were announced as participants in Ohio State Provost Joseph A. Steinmetz's corrupt MOOC education initiative named "University Innovation Alliance" (UIA). We have identified the instructions and online forms you need to file a complaint with the participants. MOOC stands for "Massive Open Online Course."

You should complain about:

(1) the intellectual property theft of social networking source code from Leader Technologies, Columbus, Ohio that is the software engine running the UIA;

(2) the corruption at Ohio State University and OSU's collusion with Battelle Memorial Institute which helped steal the software being used by UIA; and

(3) the mistreatement of OSU Marching Band Director Jon Waters regarding fabricated Title IX charges that were used to pave the way for Steinmetz to announce UIA.

Universities pride themselves on protection of intellectual property.

Therefore, these universities cannot participate in this abuse of inventor copyrights, patents and trade secrets by The Ohio State Trustees and Administration. If these universities participate knowingly with Ohio State in its theft of intellectual property, then they are aiding and abetting the theft of intellectual property on a "massive" scale... Massive Open Online Course (MOOC) also known as The Eclipse Foundation.

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
1	(n)Code Solutions	software
2	2000 customers (over) in 60 different countries	
3	3M	manufacturing
4	7 of the top 10 Fortune Global 1500 commercial bank	banking
5	7 of the top 10 Fortune Global 1500 pharmaceutical companies	pharmaceutical
6	8 of the top 10 e-governments worldwide	government
7	8 of the top 10 Fortune Global 1500 aerospace and defense companies	military
8	8 of the top 10 Fortune Global 1500 telecommunications companies	telecom
9	Accenture	professional services
10	Acxiom (Little Rock, AR, Rose Law Firm, Jerry C. Jones)	analytics
11	Adobe	software
12	AGBanco Nationale di Lavorno	banking
13	Alcatel (France)	telecom
14	AmikaNow! (Canada)	software
15	Andrew Pinder	director/officer
16	Anthony E. Hwang	director/officer
17	Aon Limited	insurance
18	Apple	computer
19	Applied Materials	electronics
20	APWG (Anti-Phishing Working Group)	software
21	Arcadia Capital Advisors LLC	investment
22	Aristex Health Solutions Inc.	healthcare
23	Arkansas School of Law	law
24	Asia Digital Media	telecom
25	Authentify	software
26	Axent	manufacturing
27	Banca Nazionale del Lavoro (Italy)	banking
28	Banco Central del Ecuador	banking
29	Banco Santander (Spain)	banking
30	Banco Security (Chile)	banking
31	Bank of Bermuda	banking
32	Bank of New Zealand	banking
33	Baptist Medical Center	healthcare

APX 308

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
34	Bay Networks	information technology
35	BCE Emergis (Canada)	telecom
36	Bell Emergis (Canada)	telecom
37	Bell Nexxia (Canada)	telecom
38	BeTRUSTed (PricewaterhouseCoopers)	security
39	Blue Cross Blue Shield of Michigan	insurance
40	Boston College	education
41	Bradley N. Ross	director/officer
42	Brian O'Higgins	director/officer
43	Butler C. Derrick, Jr.	director/officer
44	CALA (Canadian Asia and Latin America)	government
45	Canadian Bank Note (Canada)	printing
46	Canadian High Performance Computing Virtual Lab	consulting
47	Canon	manufacturing
48	Capital One Bank	banking
49	Charles Russell Law (UK)	law
50	Charter Holding	banking
51	Chase Manhattan Bank	banking
52	Check Point	software
53	Christopher M. Stone	director/officer
54	Cisco	computer
55	Citibank	banking
56	Citrix	software
57	Colonial Bank Texas	banking
58	Columbia/HCA Healthcare	healthcare
59	Commercebank	banking
60	Compaq	computer
61	Countrywide	real estate
62	Credit Suisse (Switzerland)	banking
63	CrestCo	banking
64	CRISIL (India)	analytics
65	Cyclone Commerce	software
66	CygnaCom Solutions	security

APX 309

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
67	Czech Telecom (Czech Republic)	telecom
68	Dallas Citizens Council	government
69	Dallas Mavericks	sports
70	David L. Thompson	director/officer
71	David D. Archibald	director/officer
72	David Wagner	director/officer
73	Deloitte & Touche LLP	professional services
74	Developer Suite	software
75	Digital Medical Systems	software
76	DnB NOR (Norway)	banking
77	Documentum	software
78	Douglas Schloss	director/officer
79	E.G.G. (Entrust)	security
80	EDS	professional services
81	Edward J. Pillman	director/officer
82	Edward O. Vetter	director/officer
83	EMEA PS and Sales Engineering	software
84	enCommerce	software
85	Engyro Corporation (Microsoft)	software
86	Entrust China Aerospace New World	security
87	Entrust CygnaCom	security
88	Entrust CygnaCom	security
89	Entrust Entelligence	security
90	Entrust Entelligence Group Share	security
91	Entrust GetAccess	security
92	Entrust IdentityGuard	security
93	Entrust IdentityGuard Token	security
94	Entrust ISG	security
95	Entrust Rapid PKI	security
96	Entrust TransactionGuard	security
97	Entrust TruePass	security
98	Entrust.Net	security
99	Entrust/Access	security

APX 310

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
100	Entrust/Admin	security
101	Entrust/Alliance	security
102	Entrust/Authority	security
103	Entrust/AutoRA	security
104	Entrust/CBT	security
105	Entrust/CMS	security
106	Entrust/CommerceConnector	security
107	Entrust/Desktop Designer	security
108	Entrust/DeviceConnector	security
109	Entrust/Direct	security
110	Entrust/director/officery	security
111	Entrust/Engine	security
112	Entrust/Entelligence	security
113	Entrust/Express	security
114	Entrust/File Toolkit	security
115	Entrust/ICE	security
116	Entrust/IPSEC Negotiator Toolkit	security
117	Entrust/PKI	security
118	Entrust/PrivacyServer	security
119	Entrust/ProfileServer	security
120	Entrust/RA	security
121	Entrust/RA Toolkit	security
122	Entrust/RevocationCheck	security
123	Entrust/Session	security
124	Entrust/SignOn	security
125	Entrust/SNC	security
126	Entrust/Solo	security
127	Entrust/SSF	security
128	Entrust/Timestamp	security
129	Entrust/Toolkit	security
130	Entrust/Toolkit COM Edition	security
131	Entrust/Toolkit Java Edition	security
132	Entrust/Toolkit Java Edition for OS390	security

APX 311

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
133	Entrust/TrueDelete	security
134	Entrust/TruePass	security
135	Entrust/TruePass with Persistent	security
136	Entrust/Unity	security
137	Entrust/VPNConnector	security
138	Entrust/WAPConnector	security
139	Entrust/WebConnector	security
140	Entrust@YourService	security
141	Entrust-Ready	security
142	Ericsson	manufacturing
143	Ernst & Young	professional services
144	Eurofighter GmbH	aerospace
145	Eurogiro Network A/S	banking
146	Exide Technologies	power
147	Exodus	ISP
148	Expedia Inc.	travel
149	Experian	banking
150	F. William Conner	director/officer
151	F5	networks
152	Federal Express (FedEx)	shipping
153	Fidelity Investments	investment
154	FPKI-TWG (U.S. Government Federal Public Key Infrastructure Technical Working Group)	government
155	Frank A. Dunn	director/officer
156	Gemaltro (Netherlands)	security
157	getAccess	security
158	getAccess Mobile Server	security
159	Göteborg University	education
160	Government of Canada	government
161	Government of Canada Dept. of National Defense	government
162	Government of Canada Royal Canadian Mounted Police	police
163	Government of China Financial Certification Authority	government
164	Government of Norway Ministry of Defense	government
165	Government of Ontario	government

APX 312

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
166	Government of Saudi Arabia	government
167	Government of Singapore	government
168	Government of Slovenia	government
169	Government of Spain	government
170	Government of Sweden	government
171	Gwinnett Medical Center	healthcare
172	Hale and Dorr (Wilmer Hale) LLP	law
173	Hans Downer	director/officer
174	Hans Ydema	director/officer
175	Harvard Business School	education
176	Hewlett-Packard	computer
177	HSPD-12 Solutions	security
178	Hutchison 3G	ISP
179	i2 Technologies	supply chain
180	IBM (Lotus Corporation)	software
181	IBM Global Services	professional services
182	ICICI Bank (India)	banking
183	ICL-CFM	computer
184	IDX Systems Corp	software
185	IETF (Internet Engineering Task Force)	government
186	I-many Inc.	professional services
187	Industry Canada	government
188	ING DIRECT	insurance
189	Intel	electronics
190	International Business Machines (IBM)	computer
191	Internet Security Systems Inc.	software
192	Interpay	banking
193	ISO (the International Organization for Standardization)	government
194	ITNET	education
195	J. Alberto Yepez	director/officer
196	J.P. Morgan Chase	banking
197	James H. Dennedy	director/officer
198	Jawaid Ekram	director/officer

APX 313

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
199	Jerry C. Jones (Hillary Clinton, Rose Law Firm)	director/officer
200	Jetform (Canada)	software
201	John A. Ryan	director/officer
202	John F. Kennedy School of Government at Harvard	education
203	Juniper Networks	networks
204	Kevin Simzer	director/officer
205	Kevin Sullivan	director/officer
206	Kotak Mahindra Group (India)	banking
207	Kotak Securities Limited (India)	banking
208	KPMG	professional services
209	KPN (Netherlands)	telecom
210	L1	software
211	Lavoro (Italy)	engineering
212	Liener Termlin	advertising
213	Linux	software
214	Lloyds TSB (UK)	banking
215	Lotus Development Corp (IBM)	software
216	Lucent Technologies (Alcatel-Lucent, French-owned)	telecom
217	Mackenzie Financial	finance
218	Magellan Health Services	healthcare
219	marchFIRST	software
220	Marcus Schloss & Co. Inc.	broker
221	MCI Worldcom	telecom
222	Melchor Investment Company	investment
223	Metroplex Technology Business Council	government
224	Michael P. Ressner	director/officer
225	Microsoft	software
226	Milan Bekich	director/officer
227	Morgan Guaranty Trust	banking
228	Motorola	manufacturing
229	myEntrust.Net	security
230	NASA	aerospace
231	NaviSite Inc.	IT

APX 314

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
232	Neill Duff	director/officer
233	Nelson Mullins Riley and Scarborough LLP	law
234	Netscape	software
235	NETTRAK	IT
236	Network Associates	professional services
237	New York Life	insurance
238	New Zealand Ministry of Economic Development	government
239	Newbridge Networks	networks
240	Nokia (Finland)	telecom
241	Nortel (Canada)	telecom
242	Nortel Networks (Canada)	telecom
243	Northern Telecom Limited (Canada)	telecom
244	Novartis	pharmaceutical
245	Novell	software
246	Novell GroupWise	software
247	Novell Netware	software
248	OASIS (Organization for the Advancement of Structured Information Standards)	government
249	Oberthur	security
250	Ocean Systems Inc.	IT
251	Olympus Partners	investment
252	Open Solutions	software
253	Oracle	software
254	Orion Security Solutions	security
255	People's Bank of China	banking
256	PeopleSoft	software
257	Perot Systems	professional services
258	Personal Path Systems	IT
259	Peter Bellow	director/officer
260	Pharmacia UpJohn	pharmaceutical
261	Pittiglio Rabin Todd & McGrath (PRTM)	law
262	Powell Goldstein Frazer & Murphy LLP	law
263	PricewaterhouseCoopers	professional services
264	Princeton University	education

APX 315

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
265	PT Bank Mandiri (Indonesia)	banking
266	Queen's University in Kingston (Canada)	education
267	r3 Security Engineering AG (Switzerland)	security
268	Ray W. Washburne	director/officer
269	Research in Motion (RIM) (Canada)	manufacturing
270	Rexford Management Inc.	investment
271	Richard D. Spurr	director/officer
272	Robert S. Morris	director/officer
273	Rolls-Royce Motor Cars Ltd (UK)	automotive
274	Rose Law Firm (Little Rock, AR, Hillary Clinton, Jerry C. Jones)	law
275	Royal Bank of Scotland (UK)	banking
276	S.W.I.F.T.	banking
277	Sam Morcos	director/officer
278	SAP (German)	software
279	SAP R/3 (Germany)	security
280	Schlumberger	engineering
281	SchlumbergerSema	engineering
282	SCHUFA Holding AG	banking
283	Science Applications International (SAIC)	professional services
284	SECOM	security
285	SecureSummit	security
286	Shana Corp	security
287	Shiva	networks
288	Siemens (Germany)	engineering
289	Skanska	construction
290	Societe Generale (France)	banking
291	Southampton City Council (UK)	government
292	Southern Methodist University Tate Board	education
293	Sprint	telecom
294	St. Lawrence College (Canada)	education
295	State of Alaska Law Enforcement Information Sharing System (ALEISS)	police
296	State of California Highway Patrol	police
297	State of Illinois	government

APX 316

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
298	State of Kansas Bureau of Investigation	police
299	State of Tennessee Department of Revenue	government
300	Susquehanna Bancshares	banking
301	Swedish National Labor Market Administration (AMV)	government
302	Sybase (SAP)(Germany)	software
303	T. Rowe Price	investment
304	Tekelec	telecom
305	Teledenmark (Denmark)	telecom
306	Telenor (Norway)	telecom
307	Telia (Sweden)	telecom
308	Terdema Ussery II	director/officer
309	Terrell B. Jones	director/officer
310	The Business Software Alliance (BSA)	government
311	Thomas E. Noonan	director/officer
312	Thomas Group (The)	marketing
313	Thomson Consumer Electronics	electronics
314	TimeStep	networks
315	Tokyo Institute of Technology (Japan)	education
316	Toro Company (The)	manufacturing
317	Travelocity	travel
318	Trustgenix	security
319	U.S. American National Standards Institute (ANSI)	government
320	U.S. Bureau of Census	government
321	U.S. Business Software Alliance Information Security Governance Task Force	government
322	U.S. Coast Guard	military
323	U.S. Department of Commerce	government
324	U.S. Department of Defense (DoD)	government
325	U.S. Department of Energy (DoE)	government
326	U.S. Department of State (DoS)	government
327	U.S. Department of Treasury	government
328	U.S. Federal Bureau of Investigation (FBI)	government
329	U.S. Federal Deposit Insurance Corporation (FDIC)	government
330	U.S. General Services Administration (GSA)	government

APX 317

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
331	U.S. Joint Chiefs of Staff ("Joint Forces Advisory Board")	military
332	U.S. Marine Corps (USMC)	military
333	U.S. National Cyber Security Partnership (NCSP)	government
334	U.S. National Cyber Security Partnership's Corporate Governance Task Force	government
335	U.S. National Institute of Standards and Technology (NIST)	government
336	U.S. National Institute of Standards and Techology (NIST)	government
337	U.S. National Security Agency (NSA)	government
338	U.S. National Voluntary Laboratory Accreditation Program	government
339	U.S. Patent and Trademark Office (USPTO)	government
340	U.S. Postal Service (USPS)	government
341	UK Customs & Excise	government
342	UK Land Registry	government
343	UK Ministry of Defence	military
344	UK Post Office	government
345	UK Royal Mail	shipping
346	Unisys	computer
347	University of Ottawa (Canada)	education
348	US Bank	banking
349	Vejle County (Denmark)	government
350	Vericept Corporation	security
351	Victorian Business Master Key (VBMK) (Australia)	security
352	Vignette	software
353	Vodafone (UK)	telecom
354	Wesley K. Clark	director/officer
355	Wharton School of the University of Pennsylvania.	education
356	William G. McGee	director/officer
357	Williams Communications	telecom
358	Williams & Jensen Washington	law

APX 318

No.	*ENTRUST (ENTU 1998-2009) 10-K. (Accessed Sep. 13, 2018). Material Relationships Disclosed Customer, Partner, Director, Officer, Dependent, Subsidiary. Source: SEC Edgar. Alpha Industry Sort. See *.xlsx raw data file attached to this PDF.*	*Industry/Title*
1	Liener Termlin	advertising
2	Eurofighter GmbH	aerospace
3	NASA	aerospace
4	Acxiom (Little Rock, AR, Rose Law Firm, Jerry C. Jones)	analytics
5	CRISIL (India)	analytics
6	Rolls-Royce Motor Cars Ltd (UK)	automotive
7	7 of the top 10 Fortune Global 1500 commercial bank	banking
8	AGBanco Nationale di Lavorno	banking
9	Banca Nazionale del Lavoro (Italy)	banking
10	Banco Central del Ecuador	banking
11	Banco Santander (Spain)	banking
12	Banco Security (Chile)	banking
13	Bank of Bermuda	banking
14	Bank of New Zealand	banking
15	Capital One Bank	banking
16	Charter Holding	banking
17	Chase Manhattan Bank	banking
18	Citibank	banking
19	Colonial Bank Texas	banking
20	Commercebank	banking
21	Credit Suisse (Switzerland)	banking
22	CrestCo	banking
23	DnB NOR (Norway)	banking
24	Eurogiro Network A/S	banking
25	Experian	banking
26	ICICI Bank (India)	banking
27	Interpay	banking

APX 319

28	J.P. Morgan Chase	banking
29	Kotak Mahindra Group (India)	banking
30	Kotak Securities Limited (India)	banking
31	Lloyds TSB (UK)	banking
32	Morgan Guaranty Trust	banking
33	People's Bank of China	banking
34	PT Bank Mandiri (Indonesia)	banking
35	Royal Bank of Scotland (UK)	banking
36	S.W.I.F.T.	banking
37	SCHUFA Holding AG	banking
38	Societe Generale (France)	banking
39	Susquehanna Bancshares	banking
40	US Bank	banking
41	Marcus Schloss & Co. Inc.	broker
42	Apple	computer
43	Cisco	computer
44	Compaq	computer
45	Hewlett-Packard	computer
46	ICL-CFM	computer
47	International Business Machines (IBM)	computer
48	Unisys	computer
49	Skanska	construction
50	Canadian High Performance Computing Virtual Lab	consulting
51	Andrew Pinder	director/officer
52	Anthony E. Hwang	director/officer
53	Bradley N. Ross	director/officer
54	Brian O'Higgins	director/officer
55	Butler C. Derrick, Jr.	director/officer
56	Christopher M. Stone	director/officer
57	David L. Thompson	director/officer

APX 320

58	David D. Archibald	director/officer
59	David Wagner	director/officer
60	Douglas Schloss	director/officer
61	Edward J. Pillman	director/officer
62	Edward O. Vetter	director/officer
63	F. William Conner	director/officer
64	Frank A. Dunn	director/officer
65	Hans Downer	director/officer
66	Hans Ydema	director/officer
67	J. Alberto Yepez	director/officer
68	James H. Dennedy	director/officer
69	Jawaid Ekram	director/officer
70	Jerry C. Jones (Hillary Clinton, Rose Law Firm)	director/officer
71	John A. Ryan	director/officer
72	Kevin Simzer	director/officer
73	Kevin Sullivan	director/officer
74	Michael P. Ressner	director/officer
75	Milan Bekich	director/officer
76	Neill Duff	director/officer
77	Peter Bellow	director/officer
78	Ray W. Washburne	director/officer
79	Richard D. Spurr	director/officer
80	Robert S. Morris	director/officer
81	Sam Morcos	director/officer
82	Terdema Ussery II	director/officer
83	Terrell B. Jones	director/officer
84	Thomas E. Noonan	director/officer
85	Wesley K. Clark	director/officer
86	William G. McGee	director/officer
87	Boston College	education

APX 321

88	Göteborg University	education
89	Harvard Business School	education
90	ITNET	education
91	John F. Kennedy School of Government at Harvard	education
92	Princeton University	education
93	Queen's University in Kingston (Canada)	education
94	Southern Methodist University Tate Board	education
95	St. Lawrence College (Canada)	education
96	Tokyo Institute of Technology (Japan)	education
97	University of Ottawa (Canada)	education
98	Wharton School of the University of Pennsylvania.	education
99	Applied Materials	electronics
100	Intel	electronics
101	Thomson Consumer Electronics	electronics
102	Lavoro (Italy)	engineering
103	Schlumberger	engineering
104	SchlumbergerSema	engineering
105	Siemens (Germany)	engineering
106	Mackenzie Financial	finance
107	8 of the top 10 e-governments worldwide	government
108	Butler C. Derrick, Jr.	government
109	CALA (Canadian Asia and Latin America)	government
110	Dallas Citizens Council	government
111	FPKI-TWG (U.S. Government Federal Public Key Infrastructure Technical Working Group)	government
112	Government of Canada	government
113	Government of Canada Dept. of National Defense	government
114	Government of China Financial Certification Authority	government
115	Government of Norway Ministry of Defense	government
116	Government of Ontario	government
117	Government of Saudi Arabia	government

APX 322

118	Government of Singapore	government
119	Government of Slovenia	government
120	Government of Spain	government
121	Government of Sweden	government
122	IETF (Internet Engineering Task Force)	government
123	Industry Canada	government
124	ISO (the International Organization for Standardization)	government
125	Metroplex Technology Business Council	government
126	New Zealand Ministry of Economic Development	government
127	OASIS (Organization for the Advancement of Structured Information Standards)	government
128	Southampton City Council (UK)	government
129	State of Illinois	government
130	State of Tennessee Department of Revenue	government
131	Swedish National Labor Market Administration (AMV)	government
132	The Business Software Alliance (BSA)	government
133	U.S. American National Standards Institute (ANSI)	government
134	U.S. Business Software Alliance Information Security Governance Task Force	government
135	U.S. Department of Defense (DoD)	government
136	U.S. Department of Energy	government
137	U.S. Department of State	government
138	U.S. Department of Treasury	government
139	U.S. Department of Commerce	government
140	U.S. Federal Deposit Insurance Corporation (FDIC)	government
141	U.S. Federal Bureau of Investigation (FBI)	government
142	U.S. General Services Administration (GSA)	government
143	U.S. National Cyber Security Partnership (NCSP)	government
144	U.S. National Cyber Security Partnership's Corporate Governance Task Force	government
145	U.S. National Institute of Standards and Technology (NIST)	government
146	U.S. National Institute of Standards and Techology (NIST)	government
147	U.S. National Security Agency (NSA)	government

APX 323

148	U.S. National Voluntary Laboratory Accreditation Program	government
149	U.S. Patent and Trademark Office (USPTO)	government
150	U.S. Postal Service (USPS)	government
151	UK Customs & Excise	government
152	UK Land Registry	government
153	UK Post Office	government
154	Vejle County (Denmark)	government
155	Aristex Health Solutions Inc.	healthcare
156	Baptist Medical Center	healthcare
157	Columbia/HCA Healthcare	healthcare
158	Gwinnett Medical Center	healthcare
159	Magellan Health Services	healthcare
160	Bay Networks	information technology
161	Aon Limited	insurance
162	Blue Cross Blue Shield of Michigan	insurance
163	ING DIRECT	insurance
164	New York Life	insurance
165	Arcadia Capital Advisors LLC	investment
166	Fidelity Investments	investment
167	Melchor Investment Company	investment
168	Olympus Partners	investment
169	Rexford Management Inc.	investment
170	T. Rowe Price	investment
171	Exodus	ISP
172	Hutchison 3G	ISP
173	NaviSite Inc.	IT
174	NETTRAK	IT
175	Ocean Systems Inc.	IT
176	Personal Path Systems	IT
177	Arkansas School of Law	law

APX 324

178	Charles Russell Law (UK)	law
179	Hale and Dorr (Wilmer Hale) LLP	law
180	Nelson Mullins Riley and Scarborough LLP	law
181	Pittiglio Rabin Todd & McGrath (PRTM)	law
182	Powell Goldstein Frazer & Murphy LLP	law
183	Rose Law Firm (Little Rock, AR, Hillary Clinton, Jerry C. Jones)	law
184	Williams & Jensen Washington	law
185	3M	manufacturing
186	Axent	manufacturing
187	Canon	manufacturing
188	Ericsson	manufacturing
189	Motorola	manufacturing
190	Research in Motion (RIM) (Canada)	manufacturing
191	Toro Company (The)	manufacturing
192	Thomas Group (The)	marketing
193	8 of the top 10 Fortune Global 1500 aerospace and defense companies	military
194	U.S. Coast Guard	military
195	U.S. Joint Chiefs of Staff ("Joint Forces Advisory Board")	military
196	U.S. Marine Corps (USMC)	military
197	UK Ministry of Defence	military
198	F5	networks
199	Juniper Networks	networks
200	Newbridge Networks	networks
201	Shiva	networks
202	TimeStep	networks
203	7 of the top 10 Fortune Global 1500 pharmaceutical companies	pharmaceutical
204	Novartis	pharmaceutical
205	Pharmacia UpJohn	pharmaceutical
206	Government of Canada Royal Canadian Mounted Police	police
207	State of Alaska Law Enforcement Information Sharing System (ALEISS)	police

APX 325

208	State of California Highway Patrol	police
209	State of Kansas Bureau of Investigation	police
210	Exide Technologies	power
211	Canadian Bank Note (Canada)	printing
212	Accenture	professional services
213	Deloitte & Touche LLP	professional services
214	EDS	professional services
215	Ernst & Young	professional services
216	IBM Global Services	professional services
217	I-many Inc.	professional services
218	KPMG	professional services
219	Network Associates	professional services
220	Perot Systems	professional services
221	PricewaterhouseCoopers	professional services
222	Science Applications International (SAIC)	professional services
223	Countrywide	real estate
224	Gemaltro (Netherlands)	security
225	BeTRUSTed (PricewaterhouseCoopers)	security
226	CygnaCom Solutions	security
227	E.G.G. (Entrust)	security
228	Entrust China Aerospace New World	security
229	Entrust CygnaCom	security
230	Entrust CygnaCom	security
231	Entrust Entelligence	security
232	Entrust Entelligence Group Share	security
233	Entrust GetAccess	security
234	Entrust IdentityGuard	security
235	Entrust IdentityGuard Token	security
236	Entrust ISG	security
237	Entrust Rapid PKI	security

APX 326

238	Entrust TransactionGuard	security
239	Entrust TruePass	security
240	Entrust.Net	security
241	Entrust/Access	security
242	Entrust/Admin	security
243	Entrust/Alliance	security
244	Entrust/Authority	security
245	Entrust/AutoRA	security
246	Entrust/CBT	security
247	Entrust/CMS	security
248	Entrust/CommerceConnector	security
249	Entrust/Desktop Designer	security
250	Entrust/DeviceConnector	security
251	Entrust/Direct	security
252	Entrust/director/officery	security
253	Entrust/Engine	security
254	Entrust/Entelligence	security
255	Entrust/Express	security
256	Entrust/File Toolkit	security
257	Entrust/ICE	security
258	Entrust/IPSEC Negotiator Toolkit	security
259	Entrust/PKI	security
260	Entrust/PrivacyServer	security
261	Entrust/ProfileServer	security
262	Entrust/RA	security
263	Entrust/RA Toolkit	security
264	Entrust/RevocationCheck	security
265	Entrust/Session	security
266	Entrust/SignOn	security
267	Entrust/SNC	security

APX 327

268	Entrust/Solo	security
269	Entrust/SSF	security
270	Entrust/Timestamp	security
271	Entrust/Toolkit	security
272	Entrust/Toolkit COM Edition	security
273	Entrust/Toolkit Java Edition	security
274	Entrust/Toolkit Java Edition for OS390	security
275	Entrust/TrueDelete	security
276	Entrust/TruePass	security
277	Entrust/TruePass with Persistent	security
278	Entrust/Unity	security
279	Entrust/VPNConnector	security
280	Entrust/WAPConnector	security
281	Entrust/WebConnector	security
282	Entrust@YourService	security
283	Entrust-Ready	security
284	getAccess	security
285	getAccess Mobile Server	security
286	HSPD-12 Solutions	security
287	myEntrust.Net	security
288	Oberthur	security
289	Orion Security Solutions	security
290	r3 Security Engineering AG (Switzerland)	security
291	SAP R/3 (Germany)	security
292	SECOM	security
293	SecureSummit	security
294	Shana Corp	security
295	Trustgenix	security
296	Vericept Corporation	security
297	Victorian Business Master Key (VBMK) (Australia)	security

APX 328

298	Federal Express (FedEx)	shipping
299	UK Royal Mail	shipping
300	L1	software
301	(n)Code Solutions	software
302	Adobe	software
303	AmikaNow! (Canada)	software
304	APWG (Anti-Phishing Working Group)	software
305	Authentify	software
306	Check Point	software
307	Citrix	software
308	Cyclone Commerce	software
309	Developer Suite	software
310	Digital Medical Systems	software
311	Documentum	software
312	EMEA PS and Sales Engineering	software
313	enCommerce	software
314	Engyro Corporation (Microsoft)	software
315	IBM (Lotus Corporation)	software
316	IDX Systems Corp	software
317	Internet Security Systems Inc.	software
318	Jetform (Canada)	software
319	Linux	software
320	Lotus Development Corp (IBM)	software
321	marchFIRST	software
322	Microsoft	software
323	Netscape	software
324	Novell	software
325	Novell GroupWise	software
326	Novell Netware	software
327	Open Solutions	software

APX 329

328	Oracle	software
329	PeopleSoft	software
330	SAP (German)	software
331	Sybase (SAP)(Germany)	software
332	Vignette	software
333	Dallas Mavericks	sports
334	i2 Technologies	supply chain
335	Asia Digital Media	telecom
336	8 of the top 10 Fortune Global 1500 telecommunications companies	telecom
337	Alcatel (France)	telecom
338	BCE Emergis (Canada)	telecom
339	Bell Emergis (Canada)	telecom
340	Bell Nexxia (Canada)	telecom
341	Czech Telecom (Czech Republic)	telecom
342	KPN (Netherlands)	telecom
343	Lucent Technologies (Alcatel-Lucent, French-owned)	telecom
344	MCI Worldcom	telecom
345	Nokia (Finland)	telecom
346	Nortel (Canada)	telecom
347	Nortel Networks (Canada)	telecom
348	Northern Telecom Limited (Canada)	telecom
349	Sprint	telecom
350	Tekelec	telecom
351	Teledenmark (Denmark)	telecom
352	Telenor (Norway)	telecom
353	Telia (Sweden)	telecom
354	Vodafone (UK)	telecom
355	Williams Communications	telecom
356	Expedia Inc.	travel
357	Travelocity	travel

APX 330

THE HILL

Officials prepare for potential claims of election interference

BY JACQUELINE THOMSEN - 10/24/18 06:00 AM EDT

69 SHARES SHARE TW

© Getty

State and federal officials say they are well prepared for the possibility of a cyberattack on American election systems Nov. 6, but experts warn that even a false claim of interference by foreign actors on Election Day could undermine the public's faith in the voting process.

The top cyber official at the Department of Homeland Security (DHS) said it's a very real possibility that groups will announce they successfully hacked certain election results. That would require swift action from federal authorities to decisively refute any unsubstantiated declarations of election meddling, analysts say.

"I could absolutely envision a scenario where someone claims to have had access or claims to have hacked" an election, Christopher Krebs, the undersecretary of the National Protection and Programs Directorate (NPPD), told reporters last week.

Krebs said if such a claim were made, federal officials would contact the state and local officials running the election to see if they could verify it. If the allegation is shown to be false, he said federal officials would do their best to help spread the word.

"If they need independent verification, my teams are ready to go," he said. "The FBI and the Department of Justice are ready to help out as well."

Another cybersecurity official at DHS, Jeanette Manfra, said Tuesday that a hacker could undermine the legitimacy of a race just by misrepresenting

Just In...

Uber to offer $10 off ride to the polls on Election Day
TECHNOLOGY — 3M 35S AGO

Pelosi to appear on 'Late Show' one week before midterms
IN THE KNOW — 3M 53S AGO

Dem analysis: More than 15 million could lose coverage if Trump-backed lawsuit succeeds
HEALTHCARE — 10M 55S AGO

NY governor says suspicious device sent to his Manhattan office
NEWS — 16M 43S AGO

Apple's Tim Cook: Being gay is 'God's greatest gift to me'
TECHNOLOGY — 17M 2S AGO

Dems hold 6 point lead on generic ballot ahead of midterms
WHAT AMERICA'S THINKING — 17M 33S AGO

Trump vs Obama: The economic tale of the tape
OPINION — 18M 23S AGO

$2 million ad buy targets Republicans on entitlements
HEALTHCARE — 20M 37S AGO

VIEW ALL

the results posted on a state's website.

"Are they actually manipulating the vote tally? No, but could you have then confusion or concern?" said Manfra, undersecretary for cybersecurity and communications at NPPD.

She said DHS will be in close contact with the media on Election Day to ensure accurate information is being shared and reported.

But widespread worries of a potential election hack could make false claims of meddling more effective than they otherwise might be, even if they're rebuked by election officials, experts said.

"I think no matter what happens, I think there are going to be parties who are going to claim they've broken into systems and did something to monkey with the results in one shape or form," said Paul Kurtz, CEO of the threat intelligence firm TruSTAR who served on the White House's National Security and Homeland Security councils under former Presidents Clinton and George W. Bush.

Clint Watts, a former FBI agent who has testified before the Senate on Russian disinformation campaigns, said a hacker only needs to get into a voter database and then publicly claim that they changed votes in order to raise concerns about the veracity of election results.

He said even if officials can disprove the claim with evidence, people who want to believe an election was hacked will probably do just that.

"That's the crazy thing about influence," Watts said. "You don't actually have to change any votes, you don't actually have to break into any systems. You just have to create the perception of it."

Officials across all levels of government say they are significantly more prepared this time around to counter any election interference compared with 2016, when Russia was determined to have meddled in the election.

But fears of election interference were amplified Friday when the Justice Department unsealed its first charge against a Russian national tied to the midterm elections. About the same time, several U.S. agencies released a statement warning of ongoing influence campaigns from countries such as Russia, North Korea and Iran that are designed to sow distrust in the American political systems.

Kurtz said he didn't believe a foreign actor like Russia would openly admit to interfering in U.S. elections since doing so would likely be met with severe penalties like sanctions.

"I don't see a nation-state owning up to hacking the United States," he said. "On the other hand, I can see more ambiguous statements about hacking to kind of create trouble when they have not hacked."

Josh Geltzer, former senior director for counterterrorism at the National Security Council during the Obama administration who is now executive director of Georgetown Law's Institute for Constitutional Advocacy and Protection, said the 2018 midterms could give a cyber actor like Russia the chance to test using a false claim of a hack as a possible tool to influence elections. If it's successful, he said, they could use it during the 2020 presidential election.

"The overarching goal would be to continue to make democracy seem vulnerable and leading us to cast doubt on the vibrancy of our own

Related News by |

US-led coalition strikes another Syrian mosque...

Skin Doctors Tell All: "Forget Botox, Do This...
Sponsored | www.liftandtighten.com

Ex-adviser worries McCain was last...

Top Dem calls on Kavanaugh to take a lie...

system," Geltzer said.

To effectively counter an unsubstantiated claim of election interference, state and local officials would need to act quickly to prevent the spread of misinformation, experts said, adding that many states have systems in place that could be used to fact-check a fake interference claim, such as a paper trail for ballots cast on digital voting machines.

But states such as Delaware, Georgia, Louisiana, New Jersey and Pennsylvania rely on digital systems for voting, without a verified paper record for every ballot cast.

"Those states, they can't even go back and count the ballots, to say 'Hey look, we counted the ballots. We know what the total is. Here's what it is,' " said Jake Braun, a DHS liaison in the Obama White House who's now an organizer of the Def Con Voting Village. "It would have a devastating impact on voter confidence, and that's with them changing not one vote."

SHARE TWEET

THE HILL

THE HILL 1625 K STREET, NW SUITE 900 WASHINGTON DC 20006 | 202-628-8500 TEL | 202-628-8503 FAX
THE CONTENTS OF THIS SITE ARE ©2018 CAPITOL HILL PUBLISHING CORP., A SUBSIDIARY OF NEWS COMMUNICATIONS, INC.