In The
Supreme Court of The United States

DIANNE BLUMSTEIN

NANCY GOODMAN

DONNA SOODALTER-TOMAN

Petitioners,
Pro Se

Case No. _____

vs.

JOSEPH A. BIDEN, PRESIDENT OF U.S. SENATE (114TH CONGRESS)

MEMBERS OF THE U.S. HOUSE OF REPRESENTATIVES (114TH CONGRESS)

MEMBERS OF THE UNITED STATES SENATE (114TH CONGRESS)

PRESIDENT-ELECT DONALD J. TRUMP

VICE PRESIDENT-ELECT MIKE PENCE

DIRECTOR, U.S. OFFICE OF PERSONNEL MANAGEMENT (OPM)

Respondents,

EMERGENCY MOTION FOR STAY PENDING REVIEW OF PETITION FOR A WRIT OF MANDAMUS AND FOR A TEMPORARY ADMINISTRATIVE STAY PENDING FULL CONSIDERATION OF THIS MOTION

INTRODUCTION

Pro Se Petitioners request that the U.S. Supreme Court deploy its powers of judicial review, declaratory relief, and injunctive relief to prevent cyber terrorists from perfecting a sinister scheme to undermine the U.S. government and its citizens. Beginning in 2015, cyber terrorists—said to be working on behalf of Russia—engaged in a yearlong criminal effort to materially determine 2016 congressional and presidential election outcomes.[1]

The U.S. Constitution prescribes the inaugural process that must be carried out to accomplish a peaceful transition of power. The process encompasses several official acts that include swearing in newly elected Senators and Members of the House of Representatives, ratifying electoral votes, and swearing into office the President and Vice President of the United States.

During Congressional swearing-in ceremonies, members of Congress raise their right hand and recite the Congressional Oath of Office, as required by Article VI § 3. The oath, enacted into law by Congress in 1884, reads:

> I do solemnly swear (or affirm) that I will support and defend the Constitution of the United States against all enemies, foreign and domestic; that I will bear true faith and allegiance to the same; that I take this

[1] *FBI/DHS Summary Report: GRIZZLY STEPPE–Russian Malicious Cyber Activity:* https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

obligation freely, without any mental reservation or purpose of evasion; and that I will well and faithfully discharge the duties of the office on which I am about to enter: So help me God.

In 2017, existing members of the 114th Congress were confronted with a constitutional conflict. They could either:

1. Fulfill their constitutionally mandated transition-of-power duties and ratify electoral votes on January 6, 2017, that were materially determined by a foreign cyber invader; and

   Swear into office on January 3, 2017, newly elected leaders—some of whom were materially helped by a third party invader; or

2. Refuse to perform transition-of-power duties on January 3 and January 6 in order to uphold their oath of office pledge to protect our nation against enemies, foreign and domestic.

During that period, all 17 U.S. intelligence agencies comprising the U.S. Intelligence Community (IC) were reconfirming to the President of the United States and Congressional leaders their findings that Russia had intervened in the 2016 U.S. elections for the explicit purpose of determining election outcomes.

The IC reported that the cyber invasion began in 2015 and included multiple cyber intrusions into State election data bases, and hacking and exfiltration of emails from the Democratic and Republican National Committee members' email accounts. Numerous states also reported cyber intrusions: Illinois reported that a third party extracted more than 200,000 records from voter registration files. The Cyber Division of the FBI reported that election data bases in at least 12 states were hacked.

Cyber security experts acknowledged they cannot know for sure the degree to which hackers partly or wholly determined U.S. presidential or congressional election outcomes (Appendix A).

America Is a Nation-State with Many Boundaries, Including a Cyber Territory

America is a sovereign nation-state that has a government, territories, and population. With the advent of computing, new territorial boundaries emerged in the form of cyber territory:

> It is the sovereignty that a state enjoys over territory that gives it the right to control cyber infrastructure and cyber activities within its territory. Accordingly, cyber infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic

waters, or national airspace is subject to the sovereignty of the territorial state.[2]

New nomenclature emerged such as cyber warfare, cyber intrusions, cyberattacks, and cyber invasions—all of which are similar to terms used to characterize encroachments upon other types of U.S. territories such as air, land, and sea. While these terms are often used interchangeably, Petitioners note that the intent of a cyber invader is often very different from a cyber intruder.

The nature of cyber intrusions is spelled out in *18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers,*[3] which also describes the damaging effects of cyber intrusions[4] and the need to protect against them. A cyber invader, however, generally acts on behalf of a nation-state such as Russia that is intent on undermining the stability of a government such as the United States by harvesting trade or other secrets from its target or disrupting affairs.

Petitioners find support for their distinctions in several books written by U.S. government security experts. Richard A. Clarke, in his book titled *Cyber War* (May 2010) defines "cyberwarfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

---

[2] *Tallinn Manual Sovereignty* by Martin Walls (June 12, 2015): http://insct.syr.edu/wp-content/uploads/2015/06/Tallinn-Manual-Sovereignty.pdf

[3] Legal Information Institute: https://www.law.cornell.edu/uscode/text/18/1030

[4] FBI—What We Investigate, Cyber Crimes: https://www.fbi.gov/investigate/cyber

Some governments have made cyberwarfare an integral component of their overall military strategy.[5,6] and have adopted a warfighting strategy[7] for preventing cyberattacks that involves:[8] 1) Preventing cyberattacks against critical infrastructure; 2) Reducing national vulnerability to cyberattacks; and 3) Minimizing damage and recovery time from cyberattacks." Nations also employ offensive national level cyber strategies in conjunction with officially declared wars and undeclared secretive operations."

The Federal Government and States Have Long Known State Voting Systems Are Vulnerable

Voting is the bedrock of the U.S. electoral process outlined in the Constitution's Twelfth Amendment. While the right to vote for electors may not be enshrined in the U.S. Constitution,[9)] voting is the mechanism by which citizens participate in our republic. Without the citizens' votes, Secretaries of State would be unable to determine which party's electors to seat for the Electoral College and, consequently, which electors are entitled to vote for the President and Vice President of the United States.

The American system of voting utilizes various methods to capture and count votes, including paper ballots, optical scan paper ballot systems, direct recording

---

[5] Clarke, Richard A. *Cyber War,* HarperCollins (2010) ISBN 9780061962233
[6] B Lynn, William J. III. "Defending a New Domain: The Pentagon's Cyberstrategy," Foreign Affairs, Sept/Oct. 2010, pp. 97–108
[7] USAF HQ, Annex 3–12 Cyberspace Ops, U.S. Air Force, 2011
[8] Clapper, James R. "Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, 26 February 2015 p. 1
[9] "[t]he individual citizen has no federal constitutional right to vote for electors for the President of the United States."] (*Bush* v. *Gore*)

electronic (DRE) systems, ballot marking devices and systems, punch card voting systems, mechanical lever voting machines, and online balloting by military and overseas Americans. Some electronic voting systems create a paper audit trail and some do not.

Computer experts, advocacy organizations, think tanks, and security experts have perpetually warned states and the federal government that state election laws, policies, processes, and machines that comprise America's voting system during a federal election are plagued by numerous vulnerabilities and irregularities that allow for voter suppression, manipulation, and invasion by third-party actors who have sinister intent.[10]

On multiple occasions throughout the 2016 election cycle, the U.S. Department of Homeland Security and the U.S. Intelligence Community, warned that a third-party actor—alleged to be Russia—was invading U.S. cyberspace and intruding into election systems.[11] The President of the United States acknowledged that he and Congressional leaders were briefed about the invasions throughout the 2016 election cycle. *FBI Alerts*[12] also reveal that Secretaries of State were made aware of the widespread election system breaches.

A CBS News website article titled *More State Election Databases Hacked Than Previously Thought,* dated September 28, 2016, reveals that government

---

[10] http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/

[11] *Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security*: (October 7, 2016): https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

[12]

officials were growing increasingly concerned about Russian efforts to disrupt or influence the 2016 election. The report also claimed that a total of about 10 states had their systems probed or breached by hackers, similar to the election systems breaches that had already occurred in Arizona and Illinois.[13]

The United States Failed to Protect States Against Invasions As Required by the Guarantee Clause (Article IV § 4)

The Guarantee Clause of the U.S. Constitution requires the United States to protect all its territories from invasion:

> The United States shall guarantee to every State in this Union a Republican Form of Government, and shall protect each of them against Invasion; and on Application of the Legislature, or of the Executive (when the Legislature cannot be convened), against domestic Violence.

While the Founding Fathers could not have envisioned today's technological society, the United States' obligation to protect States against invasion of all the nation's borders today would include a state's cyber territory.

> Protection against invasion was a continuation of an established centralized foreign policy and defense under the Articles of Confederation and Perpetual Union. The Framers understood that protection of the

[13] *More State databases hacked than previously thought*, *CBS News* (September 28, 2016): http://www.cbsnews.com/news/more-state-election-databases-hacked-than-previously-thought/

borders was essential to both the security of the people and the viability of the economy.[14]

U.S. leaders who were aware of ongoing cyber invasions in 2016 failed to stop the invasions into state election systems or develop stopgap measures that would have allowed for easy detection of terrorists' intrusions.[15]

STATEMENT OF THE CASE

Petitioners in the present action before the U.S. Supreme Court filed their Extraordinary Petition for Writ of Mandamus on January 5, 2017, with the United States Court of Appeals for the Fifth Circuit (Appendix B). The writ asserts:

1. The hacking of the 2016 elections provides a new context for examining the intent of our Founding Fathers as it relates to the Guarantee Clause;

2. The non-political remedy of permanent injunctive relief and declaratory relief are available to the courts under Article IV § Section 4 (The Guarantee Clause);

3. The United States failed to protect States from invasion during the 2016 elections as required by Article IV § Section 4;

---

[14] *What does Article IV, Section 4 really mean?* The American View: http://www.theamericanview.com/q-what-does-article-iv-section-4-really-mean/

[15] *FBI/DHS Summary Report: GRIZZLY STEPPE–Russian Malicious Cyber Activity:* https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

4. The Court is required to uphold the rule of law without regard to political consequence; and

5. Members of Congress who ratified the 2016 federal electoral votes participated de facto in a scheme orchestrated by an invader.

The Petition for Writ of Mandamus also requested the Court permanently enjoin the President of the U.S. Senate, Members of the U.S. Senate, Members of the U.S. House, and other persons in the U.S. Government from swearing in newly elected congressional members on January 3, ratifying electoral votes on January 6, and inaugurating Donald J. Trump President and Mike Pence Vice President on January 20, 2017. The petition also requested the Office of Personnel Management be enjoined from issuing public official performance bonds to members of Congress and the executive branch who were elected on November 8, 2016.

Almost all of the scheduled inauguration activities had been completed by January 6, 2017—the day on which the Appeals Court rendered its decision (Appendix B) dismissing Petitioners' action.

ARGUMENT

Legal Standard for Granting a Stay Pending Appeal

In determining whether to grant a stay pending appeal, the Court considers four factors: "1) whether stay applicants have made a strong showing that they are likely to succeed on the merits; 2) whether the applicant will be irreparably injured absent a stay; 3) whether issuance of the stay will substantially injure the other parties interested in the proceeding; and 4) where the public interest lies." *Nken v. Holder*, 556 U.S. 418, 434 (2009) [internal quotation marks omitted]; see also Washington *Metro. Area Transit Comm'n v. Holiday Tours, Inc.*, 559F.2d 841, 842-43 & n.1 (D.C. Cir. 1977); D.C. Cir. R. 8(a)(1). "The [probability of success]" element "is inversely proportional to the degree of irreparable injury evidenced." *Cuomo v. NRC* 772 F.2d 972, 974(D.C. Cir. 1985) [*per curriam*]. "A stay may be granted with either a high probability of success and some injury or vice versa." Id.

In accordance with precedent, Courts judge the four criteria on a sliding scale *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291 (D.C. Cir. 2009). They also "balance the strengths of the requesting party's arguments in each of the four required areas," such that "[i]f the movant's showing is particular strong in one area, [a stay] may issue even if the showing in the "other areas are rather weak," *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 297, (D.C. Cir. 2006).

Petitioners Have a Substantial Likelihood of Success on the Merits

The decision from the United States Court of Appeals for the First Circuit states that Pro Se Petitioners introduced "novel constitutional arguments" in their original Petition for Writ of Mandamus. The Court also did not reject Petitioners' argument that Article IV § 4 is justiciable as follows:

1. The Court has the power of judicial review as it relates to the Executive and Legislative Branches;
2. The Court can review the manner in which members of the Executive Branch or Legislative Branch *exercise their powers*; and
3. The Court can provide injunctive and declaratory relief on the basis of Article IV § 4 in accordance with its powers of judicial review.

Petitioners' case, in addition to presenting a "novel constitutional issue," purports to contribute to an area of law where precedent is almost non-existent (Court's authority to order a special election). It also promises to unify the limited precedent that does exist as it relates to key matters pertaining to special elections:

1. *Fladell v. Election Canvassing Commission,* stating that a revote was constitutionally impermissible.
2. *Donohue v. Board of Elections*, in which the District Court ruled it had the authority to order a new election.

3. *Political Question doctrine*, which holds that courts cannot direct either of the co-equal branches of government to carry out a specific act.
4. Article II, Section 1, requirement [3 U.S.C. Sec 1], that the presidential election take place on a particular Tuesday in early November.

Petitioners and Their Nation Will Suffer Incalculable Long-term Harm Absent a Stay

The hacking of the U.S. elections in 2016 was unprecedented in scope. It contaminated the election process to such an extent, it is impossible to determine to what degree election outcomes for the highest offices in our Nation, i.e., President, Vice President, and Congress, were determined by the people of the United States.

There is no disputing that an "emergency stay" and a "stay pending review of petition for writ of mandamus and for a temporary administrative stay pending full consideration of this motion" will have a temporary seismic effect and significant disruption throughout the United States. But the incalculable harm to U.S citizens and our democracy of being presided over by officials selected by a foreign adversary is far weightier than our nation can bear.

A Ruling Granting Injunctive Relief Will Have Positive Unintended Consequences

A ruling granting the remedy sought, permanent injunctive relief and declaratory relief, will have the unintended consequence of causing the President and members of the Legislative Branch—many of whom were beneficiaries of the cyber hacks—to join together, devise procedures for holding new elections, enact revote legislation, and implement measures to ensure state and federal elections are tamper-free in the future. Without such remedies, the door to undermining America's democracy will remain wide open.

Public Interest Favors Granting a Stay

The hijacking of U.S. 2016 elections may have allowed one of the nation's fiercest adversaries to accomplish the ultimate coup by helping to "elect" leaders at the highest levels of the U.S. Government.

Granting a stay to allow Petitioners to defend their claim of an unconstitutional election while affording them an opportunity to demonstrate the need for injunctive and declaratory relief "advances 'broader' public interests in the observance of law . . . ." (*Upjohn*, 449 U.S. 389).

A favorable granting of the relief petitioners ultimately seek will have unintended positive consequence. The 2016 elections revealed a gaping hole in our democracy, which is the inability to quickly hold new elections in the face of an

attack or national disaster. There exists a clear need for a Supreme Court-invoked process for holding new presidential and congressional elections.

A ruling from the High Court granting permanent injunctive relief and declaratory relief will have the unintended consequences of causing the President and Legislative Branch to join together, devise procedures for holding new elections, speedily enact revote legislation with public input, and implement measures to ensure state and federal elections are tamper-free in the future. Without such remedies, the door to undermining America's democracy will remain wide open.

CONCLUSION

During the 2016 election cycle, the United States was humiliated nationally and internationally as the world observed our voting processes undermined. The U.S. Supreme Court can help reestablish faith in our election process and our democracy by demonstrating that—like the Ukraine and Austria—this Nation will engage in extraordinary measures to protect our right to vote and preserve the strength and stability of our Union.

A stay will provide the Court an opportunity to determine if elected officials in the Executive Branch and Legislative Branch *exercised their vast powers* in a manner that was inconsistent with the U.S. Constitution in both spirit and intent and thus determine if this election rises to the intent set forth in the U.S. Constitution.

January 18, 2017

Respectfully Submitted:

APPENDIX A

Limited Number of Election Hack Scenarios

by Brian Fox-CAVO (California Association of Voting Officials)

SCENARIO I—Hack Early, Reap Later

In this scenario, a machine has its software changed during the primary elections. The goal of the change is to install software that will run during the general election, and will change the way the votes are counted during that election. This type of attack often generates a sense of safety and security among the election officials, because when they hand count and otherwise audit the results of the primary election, the results match perfectly. Election officials then believe that the machines are working and have not been tampered with. When the votes are tallied for the general election, **the hack is activated**, and the counts are skewed.

This type of attack can be carried out by an individual who shows up to vote at a precinct.

SCENARIO II— Hack and Reap

In this scenario, the election equipment is used as normal, but, at tally time, the memory card associated with the tally is modified (this can be done in seconds, but not likely by a voter). Once again, the counts are skewed, and the election results are different than they would have been. However, after this has happened, ballots are either destroyed or discarded, so that there is no record or auditable verification of the false count.

Because of the way our Electoral College works, in both of these scenarios, the place to attack is within states that are expected to vote about 50/50 between the two major parties. In those states, find a couple of larger precincts to hack, where you expect the vote to be overwhelmingly for the candidate that you do **not** want to win. Steal 10% of the votes cast there for your candidate, and you've not changed the precinct results, but you have changed enough votes to change the state's results.

About the Author—Brian J. Fox

Brian J Fox is an American computer programmer, entrepreneur, consultant, author, and free software advocate. He was the original author of the GNU Bash shell, which he announced as a beta in June 1989. He continued as the primary maintainer for Bash until at least early 1993.

In 1985, Fox and Richard Stallman began Stallman's newly created Free Software Foundation. At the FSF, Fox authored GNU Bash, GNU Makeinfo, GNU Info, GNU Finger, and the readline and history libraries. He was also the maintainer of Emacs for a time, and made many contributions to the software that was created for the GNU Project between 1986 and 1994. He is founder of CAVO and pioneered the initial OS vote tabulation systems.

APPENDIX B

United States Court of Appeals for the First Circuit

January 6, 2017, Decision

United States Court of Appeals
For the First Circuit

No. 17-1029

IN RE: DIANE BLUMSTEIN; NANCY GOODMAN; DONNA,

Petitioners.

Before

Lynch, Kayatta and Barron,
Circuit Judges.

JUDGMENT

Entered: January 6, 2017

Mandamus is an extraordinary remedy reserved for those occasions when a petitioner demonstrates a clear entitlement to relief. See In re Sterling-Suarez, 306 F.3d 1170, 1172 (1st Cir. 2002). Petitioner cites no precedent legitimately supporting her novel constitutional claim, and we see no basis for concluding that there is a clear entitlement to relief. See California v. United States, 104 F.3d 1086, 1091 (9th Cir. 1997)("For this Court to determine that the United States has been 'invaded' when the political branches have made no such determination would disregard the constitutional duties that are the specific responsibility of other branches of government, and would result in the Court making an ineffective non-judicial policy decision.").

For this reason, the motion for a stay is **denied** and the emergency petition for a writ of mandamus is **dismissed**.

By the Court:

/s/ Margaret Carter, Clerk

cc: Diane Blumstein