NO. 16-

IN THE

Supreme Court of The United States

DIANNE BLUMSTEIN, NANCY GOODMAN,
DONNA SOODALTER-TOMAN
Petitioners, Pro Se
v.

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.

On Petition for a Writ of Mandamus to the United States Court of Appeals For the First Circuit

---

EMERGENCY PETITION FOR WRIT OF MANDAMUS

QUESTIONS PRESENTED

I. Did the Appeals Court Err by Requiring Petitioners to Provide Legal Precedent for their "Novel Constitutional Claim" in Light of the Expert Evidence Provided?

II. Did the Appeals Court Err by Not Issuing a Declaratory Finding that U.S. Officials Exercised their Powers in an Unconstitutional Manner While Performing 2016 Inauguration Duties?

III. Did the Appeals Court Err by Not Issuing a Writ of Mandamus Prohibiting the Inauguration of Donald J. Trump and Mike Pence Based Upon 2016 Presidential Election Outcomes?

IV. Did the Appeals Court Err by Failing to Find that 17 U.S. Intelligence Agencies Under the Executive Branch of Government Concluded that Russia Invaded U.S. Cyber Territory in 2016 to Influence Election Outcomes?

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES CITED

CONSTITUTIONAL PROVISIONS AND STATUTES

OTHER AUTHORITIES CITED

IN THE
Supreme Court of The United States

DIANNE BLUMSTEIN, NANCY GOODMAN, DONNA SOODALTER-TOMAN

Petitioners, Pro Se

v

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

On Petition for a Writ of Mandamus to the United States Court of Appeals For the First Circuit

---

EMERGENCY PETITION FOR WRIT OF MANDAMUS

Petitioner Seeks to Prove:

The United States had an obligation to protect the States against cyber invasions during the 2016 elections pursuant to Article IV § 4.

The United States knew that a foreign adversary was invading U.S. cyberspaces and intruding into State election systems.

The United States failed to take sufficient actions to prevent cyber intrusions into State election systems during the 2016 elections.

No one can identify with certainty the extent to which cyber intrusions determined election outcomes.

Congressional leaders and the President of the United States took an oath of office to defend the Constitution of the United States "against all enemies foreign and domestic."

The manner in which U.S. elected officials exercised their powers during the 2016 Inauguration is in conflict with their oath-of-office pledge.

Permitting a foreign adversary to help select America's most powerful leaders is likely to have a catastrophic consequence.

Contrary to well-settled law, the U.S. Supreme Court can provide injunctive relief and declaratory relief—non-political remedies—under Article IV § 4 pursuant to the Court's powers of judicial review.

There has never been a more urgent need for the Court to provide injunctive and declaratory relief in order to compel the Executive Branch and Legislative Branch to hold new presidential and congressional elections.

JURISDICTION

This court has jurisdiction and authority to provide injunctive relief and declaratory relief under the following statutes and laws: 28 U.S.C. § 1331, 42 U.S.C. § 1983.

Petitioners were faced with overcoming longstanding, well-settled precedent in its original Petition for Writ of Mandamus filed with The United States Court of Appeals for the First Circuit:

> Is the Non-political Remedy of Permanent Injunctive Relief and [Declaratory Relief] Available to the Court Under Article IV § 4 (The Guarantee Clause)?

Petitioners argued that 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. Petitioners assert that the remedies they seek are judicial in nature (injunctive relief and declaratory relief) and *are not* within the authority of the Executive Branch or Legislative Branch to grant.

ARTICLE III STANDING

The U.S. Court of Appeals for the First Circuit labeled Pro Se Petitioners' case a "novel constitutional claim."

Petitioners were registered voters in a national election held on November 8, 2016, whereby Donald J. Trump and Mike Pence were selected as President and Vice President of the United States. Several other candidates were selected to serve in the U.S. House of Representatives and the U.S. Senate. Petitioner is challenging the constitutionality and lawfulness of current federal officials' exercise of power (*Flast v. Cohen*) in accordance with the Twelfth Amendment and Article II of the U.S. Constitution, beginning on January 3, 2017, and culminating soon after Friday, January 20, 2017.

During the referenced timeframe, representatives of the political branches of government will have unwittingly participated in cyber terrorists' scheme to subvert the U.S. election process and the "people's" republican form of government.

RELIEF SOUGHT

There exists compelling evidence that operatives acting on behalf of a third party (named as the Government of Russia) illegally and repeatedly *invaded* U.S. election systems, extracted voter records, and engaged in other criminal acts of cyber terrorism, yet to be discerned, during the 2016 election cycle to materially influence congressional and presidential election outcomes.

While it cannot be ascertained—due to the nature of clandestine cyber-attacks[1]—the degree to which cyber invasions w*ere* or *were not* determinative of election results, there exists clear and convincing evidence that some elected officials who prevailed in the 2016 elections were "selected" by a foreign power rather than "elected" in accordance with states' electoral voting processes.

Petitioners request:

The Court permanently enjoin all U.S. officials, including judges, the President of the Senate, Members of the U.S. Senate, Members of the U.S. House, and other persons from:

1) Swearing Donald J. Trump into the Office of the U.S. President on January 20, 2017;
2) Swearing Mike Pence into the Office of Vice President on January 20, 2017;
3) Procuring and or issuing public servant performance bonds to President Donald J. Trump and Mike Pence; and
4) Engaging in all other acts that would be in accordance with the peaceful transition of power as defined in the U.S. Constitution.

Petitioners also seek declaratory relief and request the Court find that persons who *exercised* inauguration-related powers in accordance with Amendment 12 and Article II following the 2016 elections acted unconstitutionally by violating the spirit and intent of the U.S. Constitution and their oath of office.

---

[1] FBI Cyber Crime website:https://www.fbi.gov/investigate/cyber

ARGUMENT

I. Did the Appeals Court Err by Requiring Petitioners to Provide Legal Precedent for Their "Novel Constitutional Claim" in Light of the Expert Testimony Provided?

Petitioners assert that the Guarantee Clause (Article IV § 4) imposes upon the United States Government an obligation to protect a State's cyber territory against invasions.

While Petitioners were not able to identify precedent in support of its "novel constitutional claim," Petitioners did provide fact-based evidence from cyber experts confirming a State's right to control its cyber infrastructure and the cyber activities within its cyber territory. The publication, *The Tallinn Manual Sovereignty by Martin Wells* (June 12, 2015), is published by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in collaboration with distinguished international law scholars and practitioners.

The Tallinn manual sets forth non-binding standards governing a nation-state's sovereignty and right to exercise jurisdiction and control over its cyberspace. It states:

> Although no state may claim sovereignty over cyberspace per se, states may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure. . . .

Petitioners make a key distinction between a cyber invasion and a cyber intrusion. 18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers[2] describes the importance of protecting cyber boundaries and the damaging effects of cyber intrusions. The statute outlines the criminal nature of intrusions into systems under the jurisdiction and control of another party. The FBI Cyber Division investigates cybercrimes.[3]

A cyber invasion, however, involves a cyber act by a foreign terrorist or nation-state intent on undermining the stability of the United States or harvesting U.S. trade or other secrets. During an act of cyber terrorism, a foreign actor invades U.S. cyberspace and intrudes into systems operated by the Government or other entities. The intent of a cyber invader is often very different from the intent of a cyber intruder.

Petitioners find support for their distinctions. U.S. government security expert Richard A. Clarke, in his book *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."

Petitioners note that the nomenclature (cyber attacks, cyberwarfare, cyber terrorists, etc.) used to define cyber invasions is analogous to the nomenclature that would be used to characterize other hostile acts of war taken by an adversary against the United State or a U.S. territory, i.e., U.S. airspace, U.S. waters, and U.S. land territories.

---

[2] https://www.law.cornell.edu/uscode/text/18/1030

[3] https://www.fbi.gov/investigate/cyber

II. Did the Appeals Court Err by Not Issuing a Declaratory Finding that U.S. Officials Exercised Their Powers in an Unconstitutional Manner While Performing 2016 Inauguration Duties?

The hacking of the U.S. elections in 2016 was unprecedented in scope and contaminated the election process to such an extent that it is impossible to ascertain if cyber terrorists determined election outcomes for the highest offices in our nation.

Expert testimony confirms that no one except for the invader can know the degree to which the invader impacted systems, records, or outcomes, given the number of election systems deployed on Election Day in the U.S. (Appendix B).

Expert testimony also confirms the existence of multiple access points and vulnerabilities a third party can exploit in order to determine election outcomes (Appendix B).

News reports, Senate hearings, and reports from the U.S. Intelligence Community confirm that a third party invaded U.S. cyber space in 2016 and intruded into U.S. election systems.

News reports and details from press conferences confirm that the political branches of the U.S. Government knew of the cyberspace invasions, but failed to take the extraordinary precautions needed to protect State election systems from intrusion during the 2016 election cycle.

Associate Director of *the International Security and Defense Policy Center,* Christopher S. Chivvis, who is also a senior political scientist, says there are ways to render attempts at cyber invasions ineffective. He states:

> [T]he United States could seek simply to make such operations impossible by developing highly effective cyber-network defenses—a strategy akin to what was sometimes called active defense.

While FBI alerts[4] indicate the United States took some action to prevent election cyber invasions during the 2016 elections, actions taken by the United States were not sufficient to prevent cyber terrorists from significantly influencing U.S. election outcomes.

The Twelfth Amendment to the U.S. Constitution provides a list of requirements Secretaries of State, the President of the U.S. Senate (Vice President of the United States), Members of the Congress, and Members of the Executive Branch must complete to accomplish a peaceful transition of power.

In 2016, political leaders charged with transition-of-power responsibilities were forced to make a difficult choice: Comply with Amendment 12 of the U.S. Constitution and ratify electoral votes significantly determined by hackers or comply with their oath of office to uphold the Constitution and thereby refuse to help perfect the criminal acts of

[4] https://www.fbi.gov/investigate/cyber

cyber terrorists. Never has the Court's counterbalancing influence been more needed.

III. Did the Appeals Court Err by Not Issuing a Writ of Mandamus Prohibiting the Inauguration of Donald J. Trump and Mike Pence Based Upon 2016 Presidential Election Outcomes?

Deputy Director of the Central Intelligence Agency (CIA), Mark J. Morell, labeled Russia's meddling in the U.S. presidential election to help President-elect Donald Trump as "the political equivalent of 9/11." The quote, which Petitioners observed Morell reiterate on CNN, was also publicized in numerous online and print publications.[5]

The extraordinary nature of a Writ of Mandamus renders it the perfect instrument for remedying an egregious terrorist act that threatens to obliterate the integrity of our Nation's foundational structure. In 2016, cyber terrorists invaded U.S. cyberspace and launched a highly public, pervasive, and unprecedented attack on the U.S. voting process—the root from which all political power in this nation stems.

IV. Did the Appeals Court Err by Failing to Find that 17 U.S. Intelligence Agencies Under the Executive Branch of Government All Concluded that Russia Invaded U.S.

[5] http://www.politico.com/story/2016/12/michael-morell-russia-us-elections-232495

Cyber Territory in 2016 to Influence Election Outcomes?

The United States Intelligence Community (IC) is a coalition of 17 agencies and organizations, including the ODNI, which is in the Executive Branch. The intelligence agencies work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities.[6] The Coalition is headed by the Director of National Intelligence (DNI).

On January 5, 2017, following the submission of Petitioners' original Writ of Mandamus to the Appeals Court, DNI James Clapper reaffirmed a finding issued by the IC on October 7, 2016. Clapper stated that all 17 U.S. intelligence agencies had concluded that Russia directed the election interference that occurred during the 2016 elections.

FACTS PRESENTED

Pro Se Petitioners Sought to Find a Path to the U.S. Supreme Court's Door.

Petitioners began by filing an Extraordinary Petition for Writ of Mandamus in a Federal Court of Appeals on January 5, 2017. Petitioners argued:

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;

[6] Intelligence Community: https://www.dni.gov/index.php

2. The non-political remedy of permanent injunctive relief is available to the courts under Article IV § 4 (The Guarantee Clause);
3. The United States failed to protect States from invasion during the 2016 elections as required by Article IV § 4;
4. The Court is required to uphold the rule of law without regard to political consequence; and
5. The hacking of the 2016 election enlisted Congressional leaders who ratified the election results 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:

1. Swearing in on January 3, 2017, persons newly elected to the U.S. House of Representatives and the U.S. Senate;
2. Ratifying on January 6, 2017, electoral votes cast by state electors and transmitted to the President of the U.S. Senate;
3. Swearing in of Donald J. Trump on January 20, 2017;
4. Procuring and issuing performance bonds to persons elected to federal office on November 8, 2016; and

5. All other acts commensurate to the peaceful transition of power following a valid election.

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).

REASONS WRIT SHOULD ISSUE

Officials overseeing the political branches of government (Legislative Branch and Executive Branch) were aware of cyber terrorists' invasions into U.S. election systems long before November 8, 2016. Yet U.S. Government officials failed to sufficiently protect systems against invasion or implement revised voting processes to mitigate the threat. As a result, a foreign adversary invaded U.S. cyberspace and intruded into election systems to materially influence—and perhaps determine—U.S. 2016 election outcomes.

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 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 constitutional duties by swearing into office newly elected leaders—some of whom were materially helped by a third party invader—and ratifying electoral votes that were impacted by a foreign cyber invader;
>
> or
>
> 2) Refuse to perform transition-of-power duties and thereby uphold their oath of office pledge to protect our nation against enemies, foreign and domestic.

At the same time, all 17 U.S. intelligence agencies, comprising the U.S. Intelligence Community (IC), were reaffirming 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 invasions began in 2015 and included multiple cyber intrusions into State election databases and the extraction of emails from the Democratic and Republican National Committee members' email accounts. Numerous states also reported cyber intrusions. The Cyber

Division of the FBI reported that election databases in at least 12 states were hacked.[7]

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

While the U.S. President has responded by taking steps to retaliate against Russia for the cyber invasions, including expelling 35 Russian diplomats, the President's acts do little to redress the impact of the hacks on states, electors, voters, and the nation as a whole.

The leaders of our government have enormous influence. They determine national and international policy, oversee military and intelligence assets, manage our economy, oversee our government's vast resources, and chart our future. The extraordinary risks of allowing such an openly tainted election to stand are incalculable and undermine our nation's position and image on the world stage.

CONCLUSION

Petitioners request the Court issue an Extraordinary Writ of Mandamus permanently enjoining the inauguration of Donald J. Trump as President and Mike Pence as Vice President of the United States.

Petitioners also request that the U.S. Supreme Court declare unconstitutional the acts of Senate

---

[7] http://thehill.com/blogs/blog-briefing-room/news/293636-fbi-foreign-hackers-penetrated-state-election-databases

President Joseph Biden and other officiants involved in the 2016 inauguration process, since such acts unwittingly enlists U.S. officials in cyber terrorists' scheme to undermine the U.S. Government.

The Supreme Courts in Austria and the Ukraine ordered new elections after cyber terrorists invaded their elections. The citizens of this great nation are asking our Supreme Court to declare the 2016 election results unconstitutional in order to pave the way for a new election.

APPENDICES

APPENDIX A

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. S*ee 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

APPENDIX B

Limited Number of Election Hack Scenarios
by Brian J. 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 California Association of Voting officials (CAVO) and pioneered the initial OS vote tabulation systems.