

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CASE NO. 17-22568-CIV-COOKE/GOODMAN**

**ARTHENIA JOYNER; MIKE SUAREZ;
JOSHUA A. SIMMONS; BRENDA SHAPIRO;
LUIS MEURICE; THE AMERICAN CIVIL
LIBERTIES UNION OF FLORIDA, INC.;
FLORIDA IMMIGRANT COALITION, INC.,**

Plaintiffs,

vs.

**PRESIDENTIAL ADVISORY COMMISSION
ON ELECTION INTEGRITY; MICHAEL
PENCE**, in his official capacity as Chair of the
Presidential Advisory Commission on Election
Integrity; **KRIS KOBACH**, in his official capacity
as Vice Chair of the Presidential Advisory
Commission on Election Integrity; **EXECUTIVE
OFFICE OF THE PRESIDENT OF THE
UNITED STATES; EXECUTIVE OFFICE OF
THE VICE PRESIDENT OF THE UNITED
STATES; TIM HORNE**, in his official capacity as
Administrator of the General Services
Administration; **MICK MULVANEY**, in his official
capacity as Director, Office of Management and
Budget; **KEN DETZNER**, in his official capacity as
Florida Secretary of State,

Defendants.

_____ /

**AMENDED COMPLAINT FOR
INJUNCTIVE AND DECLARATORY RELIEF**

I. PRELIMINARY STATEMENT

1. This action is brought on behalf of Florida voters and organizations involved and interested in the fair conduct of elections in Florida and elsewhere throughout the United States. This litigation challenges the legality of the actions of

the Presidential Advisory Commission on Election Integrity and the legality of its directive requesting and collecting voter registration information of state-registered voters in Florida and throughout the United States.

2. This suit proceeds pursuant to the Administrative Procedure Act (“APA”) (5 U.S.C. §§ 551-706), the Federal Advisory Committee Act (“FACA”) (5 U.S.C. app. 2), the Paperwork Reduction Act (“PRA”) (44 U.S.C. § 3501), the Declaratory Judgment Act (28 U.S.C. § 2201, *et seq.*), and the United States Constitution, seeking injunctive and declaratory relief, and other appropriate relief to prevent the unauthorized collection of state voter information data and to prohibit the Florida Secretary of State and other similarly situated officials of other states from providing state voter data to the Presidential Advisory Commission on Election Integrity (the “Presidential Advisory Commission” or “Commission”) and any other person or entity acting pursuant to the request or directives of the Presidential Advisory Commission.

3. At issue in this lawsuit is the request by the Presidential Advisory Commission to collect, aggregate, and potentially disseminate a massive volume of state-maintained voter information and voting history, including personal identification information and private data. Much of this information is gathered from citizens who are required by law to furnish the information to state officials solely to pursue their First Amendment constitutional right to vote. The challenged requests made to state elections officials infringe voters’ First Amendment rights. The requests also constitute an unjustified invasion of privacy not authorized under

the Constitution and laws of the United States or the individual states. The actions of the Presidential Advisory Commission have occurred in the absence of a required Privacy Impact Assessment. Importantly, the Presidential Advisory Commission's request for voter information preceded any authorized meeting of the Commission. The continued maintenance, access, and use of this information by the Presidential Advisory Commission, in secret and without authorization, constitutes a further infringement of the rights of Florida voters.

4. At issue in this lawsuit is the secrecy under which the Commission operates and the secrecy of its use of the voter data it has collected and continues to collect. The data collected includes Floridians' individual voter history and election information. The data has been uploaded to a secretive "White House Computer System" to which only select members (not all members) of the Commission have been given access. Many states have uploaded the data to this computer system. The public has been shut out on what the Commission is doing with this data at the White House.

II. JURISDICTION, STANDING, AND VENUE

5. This court has jurisdiction under its general federal question jurisdiction, 28 U.S.C. § 1331, and specific jurisdiction over claims arising under the Administrative Procedure Act, 5 U.S.C. §§ 702 & 704.

6. The Court has jurisdiction over claims for violations of the Paperwork Reduction Act. *See Livestock Mktg. Ass'n v. U.S. Dep't of Agriculture*, 132 F. Supp. 2d 817, 831 (D.S.D. 2001); *see also Alabama-Tombigbee Rivers Coal. v. Dep't of Interior*,

26 F. 3d 1103 (11th Cir. 1994) (holding that “[a]bsent the clearest command to the contrary from Congress, federal courts retain their equitable power to issue injunctions in suits over which they have jurisdiction” because it is inappropriate “to allow the government to use the product of a tainted procedure” in violation of federal statutes) (internal citation omitted).

7. The Declaratory Judgment Act (28 U.S.C. § 2201) authorizes courts to issue declaratory judgments.

8. This court has personal jurisdiction over all defendants.

9. Plaintiffs have standing to commence this action under the Administrative Procedure Act (“APA”), which confers standing to any party adversely affected by government action. 5 U.S.C. § 702 (1988).

10. Plaintiffs also have standing pursuant to the Federal Advisory Committee Act (5 U.S.C. app. 2). *Miccosukee Tribe of Indians of Fla. v. S. Everglades Restoration Alliance*, 304 F.3d 1076, 1080-81 (11th Cir. 2002); *Public Citizen v. U.S. Dept. of Justice*, 491 U.S. 440, 459 (1989).

11. Plaintiffs are authorized to seek compliance with the Separation of Powers. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 637-38 (1952) (Jackson, J., concurring). *See also Muller Optical Co. v. E.E.O.C.*, 743 F.2d 380, 386 (6th Cir. 1984) (“The President may not circumvent the constitution by attempting to legislate by Executive Order”); *County of Santa Clara v. Trump*, 2017 WL 1459081, at *21 (N.D. Cal. Apr. 25, 2017) (entering preliminary injunction as against executive order, where enforcement would invade Congress’s Article I power).

12. Plaintiffs have standing for a private cause of action for violation of the Paperwork Reduction Act of 1995, in that, “[t]he protection provided by this section may be raised in the form of a complete defense, bar, *or otherwise at any time* during the agency administrative process or judicial action applicable thereto.” (emphasis added). 44 U.S.C. § 3512(b); *see Livestock Mktg. Ass’n*, 132 F. Supp. 2d at 831 (holding that there is a private right of action under the Paperwork Reduction Act because the court “[could] not imagine language that would be more expansive.”).

13. Plaintiffs’ privacy interests are also adversely affected by the federal government action that is the subject of this complaint.

14. Venue is proper in the Southern District of Florida under 5 U.S.C. § 703 and 28 U.S.C. § 1391 as a place where the challenged conduct is occurring with respect to Florida voters.

15. All conditions precedent to bringing this action have occurred, have been waived, or would be a useless act and are accordingly waived.

III. PARTIES

16. Plaintiff Senator Arthenia Joyner (retired) is a resident and voter of Hillsborough County, Florida, and a member in good standing of The Florida Bar. She sues in her individual capacity. Senator Joyner formerly served as a member of the Florida House of Representatives, representing the 59th House District from 2000 through 2006, and as a member of the Florida Senate representing the 19th Senate District from 2006 through 2016. As a member of the Florida Senate from 2014 through 2016, Senator Joyner served as the Florida Senate Minority Leader. Senator Joyner has long been a passionate advocate for civil rights and justice during the

entirety of her political and legal careers, and within her private life. Senator Joyner is concerned about the disclosure of private information and how such disclosures violate the law and the civil rights of all people. She opposes the dissemination, collection, and uploading of her voting history, voter data, and identity information on to a secretive White House computer system. She fears what is being done or what may be done with her data at the White House. She fears this White House computer system is unsecure, could be subject to hacking, and that her data may be disseminated to unknown entities for unknown purposes.

17. Plaintiff Councilman Mike Suarez, is a resident and voter of Hillsborough County, Florida. He sues in his individual capacity. Councilman Suarez represents District 1 in the Tampa City Council and is the immediate past Chair of the Tampa City Council, having served in that position from 2016 through 2017. Councilman Suarez is a third-generation Tampa resident who is concerned about the protection of personal voter and identification information and privacy rights for himself as a registered voter, and for his constituents throughout the City of Tampa. He is a Florida voter. He opposes the dissemination, collection, and uploading of his voting history, voter data, and identity information to a secretive White House computer system. He fears what is being done or what may be done with his data at the White House. He fears this White House computer system is unsecure, could be subject to hacking, and that his data may be disseminated to unknown entities for unknown purposes.

18. Plaintiff Joshua A. Simmons is a resident and voter in Broward County,

Florida, in the Southern District of Florida. He sues in his individual capacity. He is a Florida voter. He opposes the dissemination, collection, and uploading of his voting history, voter data, and identity information on to a secretive White House computer system. He fears what is being done or what may be done with his data at the White House. He fears this White House computer system is unsecure, could be subject to hacking, and that his data may be disseminated to unknown entities for unknown purposes.

19. Plaintiff Brenda Shapiro is a resident and voter in Miami-Dade County, Florida, in the Southern District of Florida. She sues in her individual capacity. She is an active voter, a practicing attorney, and has been a leader in civic affairs in Miami, where she has served as Chair of both the City of Miami's Community Relations Board and the City of Miami's Civilian Investigative Panel. She is concerned about the circulation of her voting history and her personal information, and she is especially concerned about the misuse of that information. She opposes the dissemination, collection, and uploading of her voting history, her voter data, and identity information on to a secretive White House computer system. She fears what is being done or what may be done with her data at the White House. She fears this White House computer system is unsecure, could be subject to hacking, and that her data may be disseminated to unknown entities for unknown purposes.

20. Plaintiff Luis Meurice is a resident and voter in Miami-Dade County, Florida, in the Southern District of Florida. He is a 38-year member of the International Longshoremen's Association, its Florida Legislative Director, and

President of ILA Local 2062. He is also District Vice President of South Florida AFL-CIO. He is active in Movimiento Democracia, a non-profit organization advocating for freedom and democracy for all people. He opposes the dissemination, collection, and uploading of his voting history, voter data, and identity information on to a secretive White House computer system. He fears what is being done or what may be done with his data at the White House. He fears this White House computer system is unsecure, could be subject to hacking, and that his data may be disseminated to unknown entities for unknown purposes.

21. Plaintiff The American Civil Liberties Union of Florida, Inc. (“ACLU of Florida” or “ACLU”) is a non-profit, §501(c)(3) membership organization. The ACLU is dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws, including laws protecting access to the right to vote. Since 1965, the ACLU, through its Voting Rights Project, has litigated more than 300 voting rights cases and has a direct interest in ensuring that all eligible citizens are able to access the franchise and are not removed from voter rolls, and in empowering those targeted by vote suppression. The ACLU of Florida has over 50,000 members and has litigated numerous cases, either through direct representation or as amicus curiae, to protect the fundamental right to vote. ACLU of Florida members include registered voters who vote in Florida. ACLU Florida members could sue in their own right for the actions complained of here. The interests that ACLU of Florida seeks to protect here are germane to the organization’s purpose. The claims asserted here and relief sought does not require the participation of individual members in the lawsuit.

ACLU of Florida has dedicated resources to challenge Defendants, resources that could have been used elsewhere. ACLU of Florida is an historical champion of the right to vote. The ACLU of Florida is a state affiliate of the national American Civil Liberties Union and is domiciled in the State of Florida, with its principal place of business in Miami-Dade County, Florida, within the Southern District of Florida.

22. Plaintiff Florida Immigrant Coalition, Inc. (“FLIC”) is a non-profit membership organization and coalition of more than 65 membership organizations and over 100 allies. FLIC was founded in 1998 and formally incorporated in 2004. More than an organization, “FLIC” is a strategic multi-racial, intergenerational social movement working for the fair treatment of all people, including immigrants. FLIC promotes citizenship, the right to vote, and assists immigrants in becoming citizens along with that sacred right to vote. FLIC members include registered voters who vote in Florida. FLIC members could sue in their own right for the actions complained of here. The interests that FLIC seeks to protect here are germane to the organization’s purpose. The claims asserted here and relief sought does not require the participation of individual members in the lawsuit. FLIC has dedicated resources to challenge Defendants, resources that could have been used elsewhere. FLIC is domiciled in the State of Florida, with its principal place of business in Miami-Dade County, Florida, within the Southern District of Florida. Its members are residents of Florida and elsewhere.

23. Defendant Presidential Advisory Commission is an advisory commission of the United States government within the meaning of the Federal Advisory

Committee Act (5 U.S.C. app. 2 § 10). It is a subcomponent of the Executive Office of the President of the United States. The Office of Management and Budget and the General Services Administration, along with the Presidential Advisory Commission are agencies or the equivalent thereof within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

24. Defendant Michael Pence is the Vice President of the United States and the Chair of the Presidential Advisory Commission. He is sued in his official capacity as Chair of the Presidential Advisory Commission.

25. Defendant Kris Kobach is the Secretary of State of Kansas, and the Vice Chair of the Presidential Advisory Commission. Vice Chair Kobach has a lengthy history of attempting to suppress the right to vote within his home state of Kansas. On the Kansas Secretary of State official website, Vice Chair Kobach proclaims that he was elected to stop voter fraud. State of Kansas, Office of the Secretary of State, http://www.kssos.org/about/about_news_biography.html. But, in *League of Women Voters of United States v. Newby*, 838 F.3d 1, 13 (D.C. Cir. 2016), the U.S. Court of Appeals for the District of Columbia Circuit rejected Secretary Kobach's arguments that proof of citizenship should be required when registering to vote because there is "precious little record evidence" that failure to present citizenship leads to fraudulent registration by non-citizens. Similarly, in *Fish v. Kobach*, 840 F.3d 710 (10th Cir. 2016), the U.S. Court of Appeals for the Tenth Circuit upheld the district court's injunction against Secretary Kobach, requiring him to register voters whose voter registrations were rejected for failure to provide documentary proof of citizenship.

The Tenth Circuit explained that Mr. Kobach's actions and the Kansas statutory scheme amounted to a "mass denial of a fundamental constitutional right" for more than 18,000 voters. Moreover, the Tenth Circuit explained that Secretary Kobach's "assertion that the 'number of aliens on the voter rolls is likely to be in the hundreds, if not thousands' is pure speculation." *Id.* at 755. He is sued in his official capacity as Vice Chair of the Presidential Advisory Commission.

26. Defendant Executive Office of the President of the United States ("EOP") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

27. Defendant Office of the Vice President of the United States ("OVP") is a subcomponent of EOP and constitutes an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

28. Defendant Tim Horne is the Administrator of the U.S. General Services Administration ("GSA"), an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The GSA is charged with providing the Presidential Advisory Commission "such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission" (Exhibit A). Exec. Order. No. 13,799, 82 Fed. Reg. 22,389, 22,390 (May 11, 2017). He is sued in his official capacity.

29. Defendant Mick Mulvaney is the Director of the Office of Management and Budget ("OMB"), an office within the Executive Office of the President of the United States. The OMB Director reports to the President, Vice President, and the

White House Chief of Staff. The OMB is tasked with promulgating the Federal Regulations to effectuate the mandates of the Paperwork Reduction Act. He is sued in his official capacity.

30. Defendant Ken Detzner is the Florida Secretary of State, charged with the statutory responsibilities of maintaining and securing Florida voter information. He is sued in his official capacity.

IV. FACTS

The President and His Administration Propagate Baseless Accusations About Widespread Voter Fraud

31. President Trump has a long history of propagating baseless conspiracy theories about voter fraud, ostensibly in order to suppress the right to vote. As a presidential candidate and now as President, Mr. Trump repeatedly, and baselessly, spoke about widespread voter fraud across the country, including supposed votes cast by dead people, people voting multiple times, people voting in multiple states, and, supposed votes cast by “illegal immigrants.”¹

32. In August 2016, then-Candidate Trump told an audience that:

The only way they can beat me, in my opinion, and I mean this 100 percent, is if in certain sections of the state, they cheat, OK . . . So I hope you people can sort of not just vote . . . (but also) go around and look and watch other polling places and make sure that it's 100 percent fine.

Sachelle Saunders, *Donald Trump wants to fight voter fraud with observers*, Orlando News 6 (August 17, 2017), <http://www.clickorlando.com/news/politics/trumps-call-for->

¹ Attached as Exhibit B is a compilation of public statements by or on behalf of the President promoting the existence of voter fraud in connection with the 2016 election, despite no legitimate supportive facts or evidence.

poll-observers-could-cause-trouble. Similarly, on October 1, 2017, then-Candidate Trump told an audience to:

watch your polling booths because I hear too many stories about Pennsylvania, certain areas. . . . We can't lose an election because of, you know what I'm talking about.

Robert Farley, *Trump's Bogus Voter Fraud Claims*, FactCheck.org (October 19, 2016), <http://www.factcheck.org/2016/10/trumps-bogus-voter-fraud-claims/>. These are just two examples, of many, of Mr. Trump encouraging people to go to polling sites to intimidate voters.

33. As another example, on October 17, 2016, then-Candidate Trump stated:

They even want to try to rig the election at the polling booths. And believe me, there's a lot going on. Do you ever hear these people? They say there's nothing going on. People that have died 10 years ago are still voting. Illegal immigrants are voting. I mean, where are the street smarts of some of these politicians? ... So many cities are corrupt, and voter fraud is very, very common.

Tribune news services, *Trump wrongly insists voter fraud is 'very, very common,'* Chicago Tribune (Oct. 17, 2016), <http://www.chicagotribune.com/news/nationworld/politics/ct-donald-trump-voter-fraud-20161017-story.html>.

34. On November 27, 2016, shortly after the election, the President-Elect continued his baseless accusations about voter fraud, claiming without evidence that he actually won the national popular vote if "illegal" votes were deducted from the total. The President-Elect tweeted:

In addition to winning the Electoral College in a landslide, I won the

popular vote if you deduct the millions of people who voted illegally.

Donald J. Trump (@realDonaldTrump), Twitter (Nov. 27, 2016, 3:30 p.m.), <https://twitter.com/realDonaldTrump/status/802972944532209664>. ABC News declared this statement “False,” because “Trump offered no proof to back up this claim, and ABC News, which monitored all 50 states for voting irregularities on election night, has found no evidence of widespread voter fraud.” Lauren Pearle, *Fact-Checking Trump’s Claims About ‘Serious Voter Fraud,’* ABC News (Nov. 28, 2016), <http://abcnews.go.com/Politics/fact-checking-trumps-claims-voter-fraud/story?id=43820475>.

35. Soon after the inauguration, on January 25, 2017, President Trump tweeted:

I will be asking for a major investigation into VOTER FRAUD, including those registered to vote in two states, those who are illegal and....

even, those registered to vote who are dead (and many for a long time). Depending on results, we will strengthen up voting procedures!

Donald J. Trump (@realDonaldTrump), Twitter (Jan. 25, 2017, 7:10 am), <https://twitter.com/realDonaldTrump/status/824227824903090176>; Donald J. Trump (@realDonaldTrump), Twitter (Jan. 25, 2017, 7:13 am), <https://twitter.com/realDonaldTrump/status/824228768227217408>.

36. With these tweets, the President stated his intention to create what would later become the Presidential Advisory Commission.

**The Presidential Advisory Commission
Seeks to Collect State Voter Information – Including Florida’s**

37. Under the Federal Advisory Committee Act (“FACA”), the Presidential

Advisory Commission was established by Executive Order No. 13,799 on May 11, 2017 (the “Executive Order”). 82 Fed. Reg. 22,389 (Exhibit A). Its Charter is attached as Exhibit C.

38. The Executive Order instructs the Presidential Advisory Commission to “study the registration and voting processes used in Federal elections.” (Exhibit A). 82 Fed. Reg. at 22,389. The Executive Order does not contain any authority to amass a national voter database, collect personal voter data, to initiate investigations, or to seek the disclosure of state voter data. It says nothing about uploading voter’s data and information to a White House computer.

39. On June 23, 2017, the Commission filed its Charter – as FACA requires. The Charter says nothing about amassing a national voter database, collecting personal voter data, initiating investigations, or seeking the disclosure of state voter data. And like the Executive Order, it says nothing about uploading individuals’ voting history and data to a White House computer.

40. On June 28, 2017, the Vice Chair of the Commission – Kobach – initiated a process to collect detailed voter information, including personal identifying information, from all 50 States and the District of Columbia. This request had never occurred before, notwithstanding the existence of the U.S. Election Assistance Commission created by the Help America Vote Act of 2002. 52 U.S.C. §§ 20921-20930.²

² The U.S. Election Assistance Commission is empowered to conduct periodic studies of election administration including, among other things “[n]ationwide statistics and methods of identifying, deterring, and investigating voting fraud in elections for

41. On June 28, 2017, prior to all Commission's members being publicly named and sworn in, and before any duly noticed meetings, Vice Chair Kobach stated during a phone call with Commission members that "a letter w[ould] be sent today to the 50 States and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls. . . ." (Exhibit D). Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017).

42. The conference call—which took place mere hours before the letters were sent—was the first time Commission members were informed of the letters requesting voter information. The timing of this disclosure deprived commission members of the opportunity to consult with other members of the Commission or to formulate and express their views as to the legality or propriety of this action. See Complaint filed in *Matthew Dunlap v. Presidential Advisory Commission on Election Integrity*, 1:17-cv-02361-CKK at ¶ 44 (D.D.C. Nov. 9, 2017).

43. Similarly, the public had no meaningful opportunity to formulate and express their views as to the legality or propriety of this action.

44. According to the U.S. Census, state voter rolls include the names, addresses, and other personally identifiable information of as many as 157 million registered voters nationwide. U.S. Census Bureau, *Voting and Registration in the*

Federal office" and "[m]ethods of voter registration, maintaining secure and accurate lists of registered voters (including the establishment of a centralized, interactive, statewide voter registration list linked to relevant agencies and all polling sites), and ensuring that registered voters appear on the voter registration list at the appropriate polling site." 52 U.S.C. § 20981.

Election of November 2016 at tbl. 4a (May 2017), <https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html>.

45. Florida law makes certain voter information confidential and exempt from disclosure under any circumstances. Social security numbers, driver's license numbers, and the source of voter registration application cannot be released under any circumstances. § 97.0585, Florida Statutes (2016). Additionally, other voter information is confidential under certain circumstances. For instance, victims of domestic violence and stalking who are participants in the Attorney General's Address Confidentiality Program are exempt from public disclosure of voter registration information. § 97.0585(3). Also, categories of high-risk professionals can be exempt from disclosure of personal information including address, photograph, and date of birth.

46. The Florida Department of State, Division of Elections, is required to redact all protected exempt information for any requests for production of voter information.

47. One of the Vice Chair's hastily sent letters on June 28, 2017 was sent to Florida Secretary of State Ken Detzner. (Exhibit E).³

³ That same day of June 28, 2017, the U.S. Department of Justice sent a letter to every state covered by the National Voter Registration Act, 52 U.S.C. § 20501 ("NVRA") seeking "all statutes, regulations, written guidance, internal policies, or database user manuals that set out the procedures" each state has relating to various programs including, among other things, removing voters from voter registration rolls. The letter also discusses coordination between "state voter registration lists with state agency records on felony status and death." However, the DOJ letter does

48. These letters include a request for voter identifying information, including the “full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.” *Id.*

49. The Vice Chair’s letters also sought “[w]hat evidence or information [the state had] regarding instances of voter fraud or registration fraud” and “[w]hat convictions for election related crimes ha[d] occurred in [the] state since the November 2000 federal election.” (Exhibit E).

50. According to the Presidential Advisory Commission, “any documents that are submitted to the full Commission w[ould] also be made available to the public.” (Exhibit E).

51. According to the letters, the states’ responses to the Presidential Advisory Commission were due by July 14, 2017. (Exhibit E).⁴

not appear to specifically request information about specific identifiable voters. A copy of the letter sent to Washington Secretary of State Kim Wyman is attached as Exhibit F and is representative of the letters to all states covered by the NVRA. Given the nearly identical timing and subject matter of the DOJ’s letter and the Presidential Advisory Commission’s letter, it appears that the Presidential Advisory Commission exists to obtain records that would be otherwise unavailable to the DOJ for the purpose of enacting policies and procedures to suppress the vote across the entire country.

⁴ The URL provided by the Presidential Advisory Commission for the transmission of voter registration data and information at that time was a non-secure site, subjecting voters to having personal identifying information made available on the Internet and

**Opposition by States to Presidential Advisory Commission's
Demand for Voter Identifying Information**

52. As of the date of this lawsuit was filed, at least 9 states refused to provide any voter data. Other states issued no decision. *Responses to the "Voter Fraud" Commission's Voter File Data Request*, Brennan Center for Justice, NYU School of Law. <https://www.brennancenter.org/latest-updates-fraud-commission>. Philip Bump & Christopher Ingraham, *Trump Says States Are "Trying to Hide Things" from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017), <https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-tohide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/>.

53. California Secretary of State Alex Padilla announced his state would "not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud" Press Release, *Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters* (June 29, 2017), <http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds->

thus making them potential victims of identity theft. Visitors to this URL were informed that the "connection is not secure" and are warned about "your information . . . being stolen."

presidential-election-commission-request-personal-data-california-voters/.

54. Kentucky Secretary of State Alison Lundergan Grimes stated that “Kentucky w[ould] not aid a commission that is at best a waste of taxpayer money and at worst an attempt to legitimize voter suppression efforts across the country.” Bradford Queen, *Secretary Grimes Statement on Presidential Election Commission’s Request for Voters’ Personal Information*, Kentucky (last accessed July 3, 2017) <http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prld=129>.

55. Outgoing Virginia Governor Terry McAuliffe had “no intention of honoring [the] request.” Terry McAuliffe, *Governor McAuliffe Statement on Request from Trump Elections Commission* (June 29, 2017), <https://governor.virginia.gov/newsroom/newsarticle?articleid=20595>.

56. Mississippi Secretary of State Delbert Hosemann said, of the Vice Chair’s first letter: “My reply would be: They can go jump in the Gulf of Mexico, and Mississippi is a great state to launch from. Mississippi residents should celebrate Independence Day and our state’s right to protect the privacy of our citizens by conducting our own electoral processes.” Tal Kopan, *Pence-Kobach voting commission alarms states with info request*, CNN (July 1, 2017), <http://www.cnn.com/2017/06/30/politics/kris-kobach-voter-commission-rolls/index.html>.

57. Public opposition to the Presidential Advisory Commission’s requests and actions is mounting. Voting technology professionals wrote state election officials to warn that “[t]here is no indication how the information will be used, who will have

access to it, or what safeguards will be established.” Letter from EPIC to Nat’l Ass’n of State Sec’y’s (July 3, 2017), <https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf>.

58. After public opposition to the Presidential Advisory Commission’s request began to mount, the Vice Chair wrote an article for Breitbart News, in which he conceded that “information like the last four numbers of a voter’s social security number” is “private,” but that “[t]he Commission didn’t request that information. Thus, there is no threat that the Commission’s work might compromise anyone’s privacy.” Kris W. Kobach, *Kobach: Why States Need to Assist the Presidential Commission on Election Integrity*, Brietbart News (July 3, 2017), <http://www.breitbart.com/big-government/2017/07/03/kobach-why-states-need-to-assist-the-presidential-commission-on-election-integrity/>. (Exhibit G). To the contrary, the Vice Chair’s June 28, 2017 letter to the 50 States and the District of Columbia specifically requests, among other things, the “last four digits of social security number[s].” (Exhibit E).

59. The President also responded to the news that numerous states were objecting to the production of voter data to the Presidential Advisory Commission, tweeting:

Numerous states are refusing to give information to the very distinguished VOTER FRAUD PANEL. What are they trying to hide?

Donald J. Trump (@realDonaldTrump), Twitter (July 1, 2017, 6:07am), <https://twitter.com/realDonaldTrump/status/881137079958241280>.

Effects on Florida and its Voters

60. Florida already has one of the highest rates of fraud and identity theft in the country, making it imperative that its voters' data be held secure.

61. Additionally, after intensive scrutiny into election security caused at least in part by then-Candidate Trump's repeated unfounded statements about voter fraud, Florida officials stated, in response to media inquiries about possible data breaches during the 2016 election, that "Florida's online elections databases and voting systems remained secure in 2016," and Florida has "secured its databases and put in firewalls to protect information, and the state has 'no indication that any unauthorized access occurred.'" Jeff Pegues, *Election databases in several states were at risk during 2016 presidential campaign*, CBS News (June 13, 2017), <http://www.cbsnews.com/news/election-databases-in-several-states-were-at-risk-during-2016-presidential-campaign/>.

62. Florida is also in the process of implementing a new online voter registration platform. There has been considerable legislative debate about the platform's implementation, specifically to address security concerns to protect the public. Amy Sherman, *Is online voter registration more secure? Florida state senator says yes*, Politifact (Jan. 23, 2015), <http://www.politifact.com/florida/statements/2015/jan/23/jeff-clemens/online-voter-registration-more-secure-florida-stat/>.

63. Florida's efforts to secure voter registration data and, therefore, its voters (including the Plaintiffs), from among other things, identity theft, is now

threatened and undermined now that personalized voter data has been amassed and centralized on a White House computer, the security of which is an open question.

Florida Uploads Voter Data to a White House Computer

64. Two days after a hearing denying a preliminary injunction seeking to enjoin certain Commission activities on a related case in Washington, D.C., the Commission – on July 26, 2017 – met again, in secret and without public notice, and again without the full input and participation of all Commission members. That day, Vice Chair Kobach sent a second letter again asking States to upload voter data. This time, states were directed to “transmit the data to the White House computer system.” Like the first letter, the public had no opportunity whatsoever to comment contemporaneously. The specific letter to Florida Secretary of State Detzner is attached (Exhibit H).

65. Wasting no time, Florida Secretary of State Ken Detzner uploaded the data that very day to the White House computer. <http://www.miamiherald.com/news/politicsgovernment/article164232182.html>.

66. Secretary Detzner’s Disclosure remained subject to limitations under Florida law that this Court had in place since a July 20, 2017 ruling on Plaintiff’s Motion for Temporary Restraining Order. [DE 31]. The White House computer system was an unknown matter at the time of that hearing. That twist came along just six days later.

The Commission’s Public Meetings Say Nothing About its White House Database

67. To date, the Commission has held two public meetings, on July 19, 2017

and September 12, 2017. The September 12 meeting took place after Vice Chair Kobach began rounding up voter data and directing that States upload it to a White House computer. At that meeting, there is nothing whatsoever on the Agenda about the White House computer system or what the Commission is doing with or intends to do with the voter data it has. (PACEI Agenda , September 12, 2017, Exhibit I). During that meeting, *the subject was not even discussed.* <https://www.youtube.com/watch?v=gSXN-uq2Ju8>.

**Commission Member and Maine Secretary of State Matthew Dunlap
Sounds the Alarm on the Secretive Nature of the Commission**

68. Mathew Dunlap is the Maine Secretary of State. He is also a member of the Commission.

69. Secretary Dunlap has sounded the alarm on the secretive nature of the Commission. He has blown the whistle, exposing the corrupt nature of this Commission. The Secretary has called the Commission out for its hidden agenda, as well as the Commissions violations of the sunshine and transparency that FACA requires.

70. On November 9, 2017, Secretary Dunlap sued the very Commission on which he serves. *See Matthew Dunlap v. Presidential Advisory Commission on Election Integrity*, 1:17-cv-02361-CKK (D.D.C.).⁵

⁵ Secretary Dunlap's Complaint cites to the instant lawsuit as one of several earlier-filed lawsuits "seeking to enjoin the Commission's collection of data." *See* Document Entry 1 at ¶ 45 in *Matthew Dunlap v. Presidential Advisory Commission on Election Integrity*, 1:17-cv-02361-CKK in the United States District Court for the District of Columbia.

71. Secretary Dunlap's revelations include, among other things:

(a) The purported bi-partisanship of the Commission is a facade, hiding the reality of the Commission's actual work.

(b) Secretary Dunlap has no access to the White House Computer systems or its contents, and does not know what Vice Chair Kobach, the Vice President, other Commission members, and perhaps others at the White House are doing with the data.

(c) Dunlap and other Commission members have no idea what the purpose of the Commission's voter database is and for what purpose its information has been gathered.

(d) The Commission has obstructed Dunlap and other Commission members from participating in the substantive process of the Commission's work.

(e) Vice Chair Kobach's letters asking States for voter data was a surprise to Dunlap and other Commission members who received the notification just hours before the letters were sent, leaving no time for consultation between members or any real opportunity to comment on it.

(f) The Commission blocked information access to Dunlap and other Commission members.

(g) Dunlap and other Commission members have been deprived of access to documents and information prepared by, viewed by, and obtained by other Commissioners.

(h) Dunlap and other Commission members have been blocked from participating in the preparation of the Commission's public meetings – including agenda preparation, selection of discussion topics, choosing participants for meetings, and selection of prepared testimony.

(i) The Commission has blocked Secretary's Dunlap's request for documents that FACA requires be shared with him, including communications among Commission members.

(j) The exclusion of Secretary Dunlap and other Commission members and the obstruction of providing documents violate FACA. *See* FACA, §10 (b), USCA App. 2; *see also Cummock v. Gore*, 180 F.3d 282 (D.C. Cir. 1999).

(k) The Commission's legitimacy, any findings it may purport to make, what the Commission does with the voter data on the White House computer are all compromised. This affects Plaintiffs.

72. The procedures employed by the Commission and the other federal Defendants leave the Plaintiffs and, in the case of the organizational Plaintiffs, their members, open to fraud and identity theft, and Plaintiffs have no knowledge over the aims of this Commission or the ultimate use of and disposition of their voter data on the White House Computer.

73. The federal Defendants' ongoing actions further compound this problem now that Florida's and other states' voter data, have been uploaded to the White House.

74. It is well known that Vice Chair Kobach employs a deeply flawed

computer program called “Crosscheck” that targets people with same names and labels them fraudulent voters.⁶

75. By secretly tinkering with the data *behind closed White House doors*, the Commission has up-ended FACA’s very soul of openness and transparency. Plaintiffs and the public have no idea what is behind being done with their data. Or for what purpose.

76. Plaintiffs and the public are deeply aggrieved by this and other secretive actions that the Commission has undertaken.

Absence of Privacy Impact Assessment

77. Under the E-Government Act of 2002 (18 Pub. L. 107-347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note)), every agency “initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual” is required to complete a Privacy Impact Assessment (“PIA”) before initiating such collection. 44 U.S.C. § 3501 note (“Privacy Impact Assessments”).

78. The agency must “(i) conduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or

⁶ “The GOP’s Stealth War Against Voters” (describing the “Crosscheck” program, started by Kris Kobach), <http://www.rollingstone.com/politics/features/the-gops-stealth-war-against-voters-w435890>; *see also* The Washington Post, “This Anti-Voter-Fraud Program gets it Wrong Over 99% of the Time. The GOP Wants to Take it Nationwide.” https://www.washingtonpost.com/news/wonk/wp/2017/07/20/this-anti-voter-fraud-program-gets-it-wrong-over-99-of-the-time-the-gop-wants-to-take-it-nationwide/?utm_term=.5c8850ff66f5

equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.” *Id.*

79. The Presidential Advisory Commission is an agency subject to the E-Government Act because it is an “establishment in the executive branch of the Government,” a category that “includ[es] the Executive Office of the President.” 44 U.S.C. § 3502(1).

80. A Privacy Impact Assessment for a “new collection of information” must be “commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information.” § 3501 note (“Privacy Impact Assessments”). The PIA must specifically address “(I) what information is to be collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured” *Id.*

81. Under FACA, “records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [an] advisory committee shall be available for public inspection and copying at a single location in the offices of the advisory committee or

the agency to which the advisory committee reports until the advisory committee ceases to exist.” 5 U.S.C. app. 2 § 10(b).

82. The Commission has not conducted a Privacy Impact Assessment for its collection of state voter data.

83. The Commission has not ensured review of a PIA by any Chief Information Officer or equivalent official.

84. The Commission has not published a PIA or made such an assessment available for public inspection.

Current and Former National Security Officials Warn that Commission is Exposing Voter Data to Cyber Hacking Threat

85. The U.S. Congress has made no finding of a problem that would warrant creation of a nationwide voter database. There has been no congressional finding of a systemic and nationwide problem with voter registration files and voter history, including evidence of voter fraud, to justify the collection of state voter history and voter registration information by the federal government.

86. Since the inception of the activities of the Presidential Advisory Commission, significant new information has been developed by the United States Congress identifying serious national security and cybersecurity implications of database breaches, and the coordination of intrusion efforts by foreign governments. Collected in the Amicus Brief of Former National Security and Technology Officials in *Common Cause v. Presidential Advisory Commission on Election Integrity*, U.S.D.C. Case No. 17-Cv-01398-RCL (D.D.C) (DE38-1), are warnings from current and former government security officials that Russia and other foreign adversaries

have sought to intervene and will intervene in future United States elections, and that such behavior is likely to escalate. This Amicus Brief is attached as Exhibit J, and its contents, documents, and citations are incorporated in this Amended Complaint.

87. That Amicus Brief relates that Admiral Michael Rogers, director of the National Security Agency, recently testified before Congress that “[w]e have seen states seeking to shape the policies and attitudes of democratic peoples, and we are convinced such behavior will continue for as long as autocratic regimes believe they have more to gain than to lose by challenging their opponents in cyberspace.”

88. As the Amicus Brief explains, James Clapper, the former Director of National Intelligence, similarly testified that Russia is now “emboldened to continue” its election interference activities, “and to do so even more intensely.”

89. Members of Congress, too, have repeatedly expressed concerns about future election interference and the adequacy of existing measures to protect against further attacks, including potential tampering with voter registration systems.⁷

90. The former national security officials in the Amicus Brief described the likelihood of hostile nation-states attempting to breach the Presidential Advisory

⁷ See, e.g., Video Recording, Hrg. before the Senate Comm. on Homeland Security and Governmental Affairs (Sept. 27, 2017) at 01:41:45 – 01:42:33 (questions from Sen. Claire McCaskill to Elaine Duke, Acting Secretary of DHS, and Christopher Wray, Director of the FBI, concerning measures to prevent interference in future elections); id. at 01:49:55 – 01:50:22 (question from Sen. James Lankford expressing concerns about tampering with voter registration lists), available at <https://www.c-span.org/video/?434411-1/senior-officials-testify-homelandsecurity-threats&start=6178>.

Commission's database for espionage purposes not directly related to election interference. The Justice Department, in *United States v. Dokuchaev*, U.S.D.C. Case No. 3:17-cr-103, ECF No. 1 (N.D. Cal. Feb. 28, 2017), charged two officers belonging to the Russian Federal Security Service (as well as two other individuals) with orchestrating a massive breach of Yahoo's networks and accessing information regarding more than 500 million Yahoo user accounts.¹⁷ The indictment alleges the conspirators used this information to target particular victims of interest to Russian intelligence as well as to orchestrate various scams.¹⁸ It has also been reported that other hacked files pertaining to American citizens are being used by foreign intelligence services, including in China and Russia, to assemble and cross-index databases that could be used to identify and even blackmail U.S. intelligence operatives.

91. Based in part on the testimony of these former national security officials who operated at the highest levels of the U.S. Government, the Amicus Brief details the serious compromise to privacy, national security, and voter information resulting from the Presidential Advisory Commission's conduct. The Amicus Brief recognizes that the "stated mission of the Presidential Advisory Commission on Election Integrity is to ensure the integrity of our electoral systems. But given the advanced cyber threats posed by foreign adversaries, there is a serious risk that the Commission's activities will ultimately make U.S. election systems more susceptible to compromise and abuse. The Commission has aggregated and continues to aggregate large volumes of data about American voters, including names, addresses,

partial social security numbers, and voting history, into one centralized database stored, operated, and maintained by the White House. That database may be a compelling target for foreign adversaries seeking to interfere in future elections through a variety of means, as well as for cyber criminals and other malicious actors. Yet, despite this grave vulnerability, the Commission chose to move the database from a network administered by the Department of Defense to an ad hoc system built by White House personnel. Amici, who have a wealth of experience as national security and cybersecurity officials, have authored this brief in order to highlight the substantial risks that assembling and maintaining such a database could create.” (Exhibit J, page 2).

92. The Amicus Brief further explains that “[f]or all of the vulnerabilities demonstrated during last year’s elections, one feature of our state-based election system that poses challenges to would-be attackers is the extent of its decentralization—including the degree to which information that could be used to exploit potential vulnerabilities is widely dispersed across numerous systems, formats, and regions. That strength is critically undermined by the Commission’s conduct and will continue to be undermined so long as the Commission’s database is maintained. Because the Commission’s maintenance of this database could enable malicious actors to inflict significant harms on the nation’s electoral process as well as on individual voters, amici seek to inform the Court’s understanding of these potential harms as it evaluates Plaintiffs’ complaint and the Government’s motion to dismiss. (Exhibit J, page 2-3).

COUNT I

**Violations of the Federal Advisory Committee Act,
5 U.S.C. App. 2, *et seq.***

**Against Presidential Advisory Commission, Pence, Kobach,
Executive Office of the President, Executive Office of the Vice
President, Horne, and Mulvaney**

93. Plaintiffs restate and incorporate paragraphs 1-92.

94. The Executive Order specifically contemplates that the Presidential Advisory Commission is governed by the Federal Advisory Committee Act, 5 U.S.C. App. 2, *et seq.* (“FACA”). *See* Executive Order 82 Fed. Reg. 22,389 at § 7(c) (Exhibit A). The Presidential Advisory Commission’s Charter also states that the Commission “is established in accordance with . . . the Federal Advisory Committee Act.” (Exhibit C at ¶ 2). The first notice of any meeting of the Presidential Advisory Commission published in the Federal Register, which was published on July 5, 2017, also states that the Commission was “established in accordance with the Federal Advisory Committee Act (FACA), 5 U.S.C. App. . . .” 82 Fed. Reg. 31,063 (Exhibit K) (the “First Meeting Notice”).

95. However, Defendant Presidential Advisory Commission and the other federal Defendants have failed to comply with numerous of the FACA’s clear requirements. Among other things, these Defendants (a) failed to properly notice and conduct meetings, (b) failed to provide opportunities for public participation and input, (c) failed to make its membership fully known, (d) failed to make documents available to the public, (e) conducted unlawful business not authorized by the Executive Order or any statute prior to all of the Commission’s members being

appointed and sworn in and without input or participation from the public or even most of the Commission's members; and (f) have shut out select Commission members from the workings, preparations, strategy, and goals of this Commission.

96. "Because FACA's dictates emphasize the importance of openness and debate, the timing of such observation and comment is crucial to compliance with the statute. Public observation and comment must be contemporaneous to the advisory committee process itself. . . . If public commentary is limited to retrospective scrutiny, the Act is rendered meaningless." *See Alabama-Tombigbee Rivers Coal. v. Dep't of Interior*, 26 F.3d 1103, 1106 (11th Cir. 1994).

97. According to the Eleventh Circuit, "injunctive relief [is] the only vehicle that carries the sufficient remedial effect to ensure future compliance with FACA's clear requirements." *Id.* at 1107. It is the responsibility of the courts to see that the FACA is followed, even where there are only "minor transgressions" of the FACA and where "the subject matter is serious" and "the objective is worthy." *Id.* at n.9. "Because the matters are so serious and of such great concern to so many with differing interests, it is absolutely necessary that the procedures established by Congress be followed to the letter." *Id.*

98. "[T]o allow the government to use the product of a tainted procedure would circumvent the very policy that serves as the foundation of the Act." *Id.*

99. *First*, the Presidential Advisory Commission and the other federal Defendants, including the Vice President and the Vice Chair on behalf of the Commission, began conducting official business prior to ever holding a meeting for

which a notice was published in the Federal Register, prior to the appointment and swearing in of all of its members, and prior to any public participation or input being permitted.

100. The first meeting of the Commission for which a notice was published in the Federal Register is presently scheduled to take place on July 19, 2017. At that meeting, the Commission's members will be sworn in.

101. Yet, on June 28, 2017, the Vice Chair issued letters to the chief elections officials of all 50 States and the District of Columbia seeking personal information about every registered voter in the country, the effect of which would be to amass and centralize a federal voter database not authorized by the Executive Order or any statute, thereby indicating one or more earlier meetings of the Commission have taken place without any notice published in the Federal Register.

102. At that June 28 meeting, certain Commission members, including Secretary Dunlap, were shut out of the preparations for this meeting and the concept of amassing a national voter database. Secretary Dunlap and others had no opportunity to comment or study the intent behind this unprecedented request – one that has already affected Plaintiffs and the Public.

103. According to the Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017), attached as Exhibit D, additional telephonic meetings, for which there was no notice published in the Federal Register, were unlawfully held. During the conference call with the Commission's members, the Vice Chair told the

other members about the letters he sent to the 50 States and the District of Columbia on behalf of the Commission requesting voter data.

104. Thus, the Vice President and the Vice Chair acted unilaterally on behalf of the Presidential Advisory Commission, without the consent or participation of the public or even the majority of the members of the Commission, in sending the letters seeking voter registration and personal information about every registered voter in the country, in violation of the FACA.

105. In fact, the Vice Chair's June 28, 2017 letter to each of the 50 States and the District of Columbia, which is printed on Presidential Advisory Commission letterhead and which bears the Seal of the President of the United States, requests that each jurisdiction receiving the letter respond by July 14, 2017, which is prior even to the first meeting of the Commission for which notice was published in the Federal Register, which is scheduled for July 19, 2017.

106. *Second*, the Presidential Advisory Commission and the other federal Defendants failed to name all of its members before it began conducting business, in violation of the FACA.

107. Pursuant to 5 U.S.C. App. 2 § 2(b)(5), "the Congress and the public should be kept informed with respect to the number, purpose, membership, activities, and cost of advisory committees."

108. By July 9, 2017, various news reports have indicated that 11 members of the Commission had been appointed, including the Vice President as Chair, and including the Vice Chair. News reports also indicate that one of the members has

since resigned from the Commission, leaving the Commission with 10 members as of that date. Pursuant to the Executive Order, the Commission will have “no more than 15 additional members” besides the Vice President, for a maximum possible total of 16 members. As of the time the Commission began conducting official business, the Commission’s makeup was uncertain and non-final.

109. In fact, the Commission’s members’ swearing-in ceremony did not take place until approximately July 19, 2017, even though the Commission had already begun conducting business in violation of the FACA.

110. *Third*, the Presidential Advisory Commission and the other federal Defendants have failed to comply with the FACA’s requirements regarding advance notice of meetings or transparency of their intentions.

111. Pursuant to 41 C.F.R. § 101-6.1015(b), a regulation implementing the FACA:

(b) *Committee meetings*. (1) The agency or an independent Presidential advisory committee shall publish at least 15 calendar days prior to an advisory committee meeting a notice in the FEDERAL REGISTER, which includes:

- (i) The exact name of the advisory committee as chartered;
- (ii) The time, date, place, and purpose of the meeting;
- (iii) A summary of the agenda; and
- (iv) A statement whether all or part of the meeting is open to the public or closed, and if closed, the reasons why, citing the specific exemptions of the Government in the Sunshine Act (5 U.S.C. 552(b)) as the basis for closure.

(2) In exceptional circumstances, the agency or an independent Presidential advisory committee may give less than 15 days notice, provided that the reasons for doing so are included in the committee meeting notice published in the FEDERAL REGISTER.

112. The Presidential Advisory Commission and its affiliated federal

Defendants have violated 41 C.F.R. § 101-6.1015(b) in multiple regards, by holding meetings that were not noticed in the Federal Register whatsoever and taking action based upon those un-noticed meetings, including:

a. Holding one or more meetings consisting solely of the Vice Chair and/or the Vice President (and possibly other members of the Trump administration, but not including the majority of the members of the Presidential Advisory Commission) that were not noticed in the Federal Register, which led to the Vice Chair sending out letters seeking voter information from all 50 States and the District of Columbia on June 28, 2017, all without the participation or input of the public or even the majority of the Commission's members; and

b. Holding one or more telephonic meetings that were not noticed in the Federal Register and that did not allow for public participation or input.

113. The meetings of the Commission referenced in the preceding paragraph violate 41 C.F.R. § 101-6.1015(b) for failing to provide any notice in the Federal Register whatsoever.

114. The Presidential Advisory Commission and its affiliated federal Defendants have also violated 41 C.F.R. § 101-6.1015(b) with regard to the first meeting for which a notice was published in the Federal Register, because the notice is legally deficient.

115. The first notice of any meeting of any kind of the Presidential Advisory

Commission was published in the Federal Register on July 5, 2017, giving notice of an open meeting to take place on July 19, 2017. 82 Fed. Reg. 31,063 (Exhibit K) (the “First Meeting Notice”). Accordingly, even this First Meeting Notice violates 41 C.F.R. § 101-6.1015(b) in that it provides less than 15 days’ notice of the meeting and provides no reasons or exceptional circumstances for doing so, in violation of the FACA.

116. *Fourth*, the Presidential Advisory Commission and the other federal Defendants have failed to comply with the FACA’s requirement that members of the public be permitted to attend one or more of the Commission’s open meetings in person.

117. Pursuant to 41 C.F.R. § 101-6.1021(b), a regulation implementing the FACA:

The agency head, or the chairperson of an independent Presidential advisory committee, shall ensure that— . . . (b) The meeting room size is sufficient to accommodate advisory committee members, committee or agency staff, and interested members of the public[.]

118. The Presidential Advisory Commission and its affiliated federal Defendants have violated 41 C.F.R. § 101-6.1021(b) with regard to its earlier un-noticed meetings in multiple regards, including by:

a. Holding one or more meetings of the Commission that were not noticed in the Federal Register, in which the meeting room was not sufficient to accommodate interested members of the public (and in which the majority of the Commission’s members were not even in attendance); and

b. Holding one or more telephonic meetings of the Commission that

were not noticed in the Federal Register, in which the meeting room was necessarily not sufficient to accommodate interested members of the public because the meetings took place by telephone, and thus there was no meeting room.

119. The Presidential Advisory Commission and its affiliated federal Defendants have also violated 41 C.F.R. § 101-6.1021(b) with regard to the first meeting for which a notice was published in the Federal Register, because the notice is legally deficient.

120. The First Meeting Notice states that the meeting “will be open to the public through livestreaming on <https://www.whitehouse.gov/live>.” This indicates that interested members of the public will not be permitted to attend and observe the meeting in person, in violation of 41 C.F.R. § 101-6.1021(b).

121. *Fifth*, the Presidential Advisory Commission and the other federal Defendants, including the Vice President, have failed to comply with the FACA’s requirements to provide reasonable public participation in the Commission’s activities.

122. Pursuant to 41 C.F.R § 101-6.1011(b), a regulation implementing the FACA, “[t]he chairperson of an independent Presidential advisory committee shall comply with the Act and this subpart and shall: . . . (b) [f]ulfill the responsibilities of an agency head as specified in paragraphs (d), (h) and (j) of §101–6.1009” 41 C.F.R. § 101-6.1009(h), referenced therein, provides that:

The head of each agency that uses one or more advisory committees shall ensure: . . . (h) The opportunity for reasonable public participation in

advisory committee activities[.]

123. Thus, the Presidential Advisory Commission's refusal to allow in-person attendance at its meetings, along with the Commission having taken action by, at a minimum, sending letters to all 50 States and the District of Columbia seeking voter data to amass and centralize a federal voter database, without any public participation or input, violates the Vice President's obligations as the Chair of the Commission under the FACA to provide for reasonable public participation in the Commission's activities.

124. The Vice President's and Vice Chair's unilateral actions on behalf of the Presidential Advisory Commission, without even the input of the majority of the Commission's members, in seeking to collect voter data from all 50 States and the District of Columbia to amass and centralize a federal voter database without first (a) making known the final makeup of the Commission's members, (b) holding any meetings for which notice(s) were published in the Federal Register, (c) swearing in the Commission's members, or (d) providing any opportunity for public comment, participation, or input, necessarily violates the FACA because "[p]ublic observation and comment must be contemporaneous to the advisory committee process itself." *See Alabama-Tombigbee Rivers Coal.*, 26 F.3d at 1106.

125. *Sixth*, the Presidential Advisory Commission and the other federal Defendants have failed to make available for public inspection a privacy impact assessment for the collection of voter data, and have also failed to comply with numerous transparency and openness provisions of FACA.

126. *Seventh*, the Presidential Advisory Commission and the other federal Defendants have failed to comply with FACA provisions requiring that advisory commissions not be partisan. FACA guards against the use of advisory committees to lend a false imprimatur of bipartisanship and legitimacy to their findings and recommendations. Membership of commissions must be “fairly balanced in terms of the points of view represented.” 5 U.S.C. app. 2 § 5(b)(2). Additionally, there must be “a clearly defined purpose for the advisory committee” and the Commission cannot be “inappropriately influenced by the appointing authority or by any special interest.” *Id.* at §§ 5(b)(1) & (3). “To the extent they are applicable, [these provisions] shall be followed by the President, agency heads, or other Federal officials in creating an advisory committee.” *Id.* at § 5(c).

127. Yet, the Presidential Advisory Commission is, in reality, mainly comprised of and controlled by individuals who wish to suppress the right to vote, including of particular note, Vice Chair Kobach and the Vice President. Any members, like Secretary Dunlap, who do not wish to suppress the right to vote are left out of important decision-making and are not privy to numerous documents, systems, information, communications, and are otherwise obstructed and blocked from meaningful participation in the Commission. The purported bi-partisanship of the Commission is a facade, hiding the reality of the Commission’s actual work, which is to suppress the right to vote in Florida and nationwide.

128. *Eighth*, the Commission and the other federal Defendants continue to violate the FACA by storing their materials on unapproved mediums and in darkness

from the public and otherwise in direct contravention of FACA.

129. On July 28, 2017 Vice Chair Kobach sent a second letter asking for States to upload voter data to a “White House Computer System.” (Exhibit H). That very day, Florida complied.

130. Again, this was done without public notice, without the public’s right of contemporaneous comment, and without the full inclusion of certain Commission members who have been locked out of this effort to amass and centralize a national voter database.

131. And now, Secretary (and Commissioner) Dunlap has blown the whistle, exposing the corrupt nature of this Commission

132. *Ninth*, for these reasons and other reasons not yet known to the public, the Commission’s and the other federal Defendants’ FACA violations of transparency and openness are flagrant. The Commission’s ongoing defiance of the law is detrimental to Plaintiffs and the Public. The Eleventh Circuit holds:

“Because FACA’s dictates emphasize the importance of openness and debate, the timing of such observation and comment is crucial to compliance with the statute. Public observation and comment must be contemporaneous to the Advisory committee process itself.” A simple “excuse us” cannot be sufficient. It would make FACA meaningless, something Congress certainly did not intend.”

(T)o allow the government to use the product of a tainted (FACA) procedure would circumvent the very policy that serves as the foundation of the Act.

It is simply insufficient for the government to contend that . . . courts should not interfere or be concerned with (what it claims are) minor transgressions. Quite the contrary. Because the matters are so serious and of such great concern to so many with differing interests, *it is absolutely necessary that the procedures*

*established by Congress be followed to the letter. Congress outlined in detail exactly what procedures were to be used and it is the responsibility of the courts to see that such laws are carried out.*⁸

Alabama-Tombigbee Rivers Coalition v. Department of Interior, 26 F.3d

1103, 1106-07 n.9 (11th Cir 1994).

133. These violations are all injurious to Plaintiffs. Their right to vote is threatened. Their data is threatened as it is tinkered with in secret by only a select number on the Commission and perhaps unknown others. The data is threatened because there is no assurance of security in this particular White House.

134. The Defendants have failed to comply with the Federal Advisory Committee Act, FACA, 5 U.S.C. App. 2; §§ 1-10, by committing, among other things, the following acts and omissions:

(a) Failing to comply with the requirement that “the records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by each advisory committee shall be available for public inspection and copying at a single location in the offices of the advisory committee or the agency to which the advisory committee reports until the advisory committee ceases to exist.” This violates FACA, §§1 (5), 10 (b), 5 U.S.C.A. App. 2.

(b) Failing to provide public notice, opportunity of contemporaneous comment, openness and transparency of its meeting that culminated with

⁸ *Id.* at 107 and FN 9.

same-day letters on June 28 and July 26, 2017 to the States and the District of Columbia directing that voter data be uploaded to a White House Computer System. This violates FACA, §§1 (5), 10(a) (1)-(3)(b), 5 U.S.C.A. App. 2.

(c) Shutting or severely restricting Secretary Dunlap and other Commission members who would otherwise provide input and balance on the initiative, purpose and need for the amassing of a nationwide voter database on a White House Computer System. This violates FACA, 5 U.S.C.A. App. 2, § 5 (b) (1-3).

(d) Amassing a National voter database, with Floridian and other state voter data, on a White House Computer System, behind closed White House Doors and with no ability for Plaintiffs, the Public, or even Congress to see what the Commission is doing with that data. This violates FACA, 5 U.S.C.A. App. 2, §§1 (5)10 (b).

(e) Eliminating FACA's requirement of balance, and only permitting a select few Commissioners to control the agenda, invite participants, and select prepared testimony for Public meetings to the exclusion of Secretary Dunlap and others on the Commission. This violates FACA. 5 U.S.C.A. App. 2, §5 (b)(2), §10 (b); *see also Cummock v. Gore*, 180 F.3d 282 (D.C. Cir. 1999).

(f) Failing to inform the public in public meeting the purpose of the voter database, what is being done with it, and otherwise carrying on a secret agenda that is not disclosed to the Public or even members of the Commission. This violates FACA. 5 U.S.C.A. App. 2, §§1 (5), 5 (b)(2), 10 (b). *See also*

Cummock v. Gore, 180 F.3d 282 (D.C. Cir. 1999).

(g) Running or considering running Crosscheck or similar voter elimination programs in secret at the White House on Plaintiffs, Floridians and other voter data that Vice Chair Kobach and the Commission have obtained. This violates FACA. 5 U.S.C.A. App. 2, §§1 (5), 5 (b)(2), 10 (b).

(h) Exceeding the Scope of the Executive Order, which does not empower the Commission to amass and centralize a federal database of voters on a White House computer. This violates FACA. 5 U.S.C.A. App. 2, § (9)(a-b).

(i) Exceeding the Scope of the Commission's Charter, which does not empower the Commission to amass and centralize a federal database of voters on a White House computer. This violates FACA. 5 U.S.C.A. App. 2, § (9)(a-c).

(j) Continuing to operate in the darkness at nearly all levels, in violation of the letter and spirit of FACA for reasons stated herein and also for those reasons not yet known.

135. Defendants may have committed additional violations of the FACA not presently known to the Plaintiffs, especially in light of the Defendants' various violations of the FACA that have kept the public in the dark about the Presidential Advisory Commission's conduct.

136. Plaintiffs are, individually and in their representative capacities, adversely affected and aggrieved by the Defendants' actions and inaction.

137. The FACA transgressions are blatant and continuing in nature. Neither the Presidential Advisory Commission nor any of the federal Defendants should be

permitted to utilize any of the documents, materials, or information they received in violation of FACA; they should not be permitted to author or present any reports or the like, including but not limited to the President or anyone, in any official or unofficial capacity; and any reports or the like that it has already authored or prepared, or that it will author or prepare should not be permitted to be utilized. *See Alabama-Tombigbee Rivers Coal. v. Dep't of Interior*, 26 F. 3d 1103 (11th Cir. 1994).

138. Unless the Court declares the actions of the Presidential Advisory Commission, the Vice President, the Vice Chair, and the other federal Defendants to be illegal and enters an order or orders granting injunctive relief to require the Defendants to follow all legal requirements, Plaintiffs, individually and in their representative capacities, will be subjected to unknown manipulation and use of their data at the White House, the purpose of which use has not been explained—controlled by the whims of certain Commission's directors, that is not authorized by any statute, the Executive Order, the Commission's Charter, and that is the product of numerous violations of the FACA.

COUNT II

Breaches and Violations of Constitutional Separation of Powers and Article II

Against Presidential Advisory Commission, Pence, Kobach, Executive Office of the President, Executive Office of the Vice President, Horne, and Mulvaney

139. Plaintiffs restate and incorporate paragraphs 1-92.

140. Pursuant to the U.S. Constitution, the powers of the three branches are separated.

141. The Framers of the Constitution placed Congress's power in Article I. Executive power follows in Article II.

142. Under the U.S. Constitution, Congress is given the power to enforce and protect, through legislation, the right to vote and the election system. The U.S. Constitution gives no power to the Executive Branch concerning the election system or its integrity. Any power the Executive does have to enforce the right to vote or to protect the electoral process is its general enforcement power and its obligation to execute and enforce Congressional acts and laws – *faithfully*.

143. Under Article I, Congress is given the exclusive federal power to make laws and regulate elections: “The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations . . .” Art. I, § 4, U.S. Const.

144. Under the 14th, 15th, 19th, 24th, and 26th Amendments to the U.S. Constitution, the right to vote was secured for African-Americans, women, and 18-

year olds, and poll taxes were eliminated. In each Amendment, Congress was given the power to enforce these rights with legislation. Each of these Amendments conclude with nearly identical language: “The Congress shall have power to enforce, by appropriate legislation, the provisions of this article.” The Executive is not mentioned.

145. Using its Article I Powers, Congress has created the exclusive legal regime over the enforcement of elections and the right to vote, to safeguard the integrity of the voting systems, and to otherwise regulate the integrity of elections. Such legislation includes, *inter alia*: The Voting Rights Act of 1965; The National Voter Registration Act of 1993 (Motor Voter Law); and the Help America Vote Act of 2002. These laws are aimed at protecting election integrity and the right to vote. The U.S. Court of Appeals for the Eleventh Circuit explained that the Help America Vote Act “represents Congress’s attempt to strike a balance between promoting voter access to ballots on the one hand and preventing voter impersonation fraud on the other.” *Fla. State Conference of N.A.A.C.P. v. Browning*, 522 F.3d 1153, 1168 (11th Cir. 2008).

146. The Executive Branch has limited, enumerated powers under Article II of the U.S. Constitution.

147. Nowhere in the Constitution or through Acts of Congress is the Executive granted or delegated any power to amass and centralize a national database of voters that includes party affiliation, voting history, social security numbers, military history, criminal history, address, or any other of the personal data

the Presidential Advisory Commission requested.

148. To the extent the Executive has implied or express powers through the enforcement and execution of Congressional Acts – including its limited and delegated authority to establish *sunshine, transparent, out-in-the-open* commissions under FACA – nowhere does Congress or the Constitution contemplate that the Executive can amass and centralize a national voter database at the White House, where it can tinker with the data in private.

149. The Commission's acts here are unprecedented.

150. One of the Executive's duties is that "he shall take care that the laws be faithfully executed." The Executive – through the Presidential Advisory Commission – is not faithful to the execution of any law. Rather, the Executive is pursuing a widely disputed complaint that millions voted illegally in the 2016 election.

151. The creation and the activities of the Executive's Presidential Advisory Commission unconstitutionally intrude into the Article I powers of Congress over the electoral system, its authority over the protection of the vote, and its authority over the integrity of the election system. The presidential creation of the Presidential Advisory Commission and its ongoing activities violate the separation of powers of the U.S. Constitution.

152. These actions have exceeded the scope of the Executive's Article II powers and have otherwise breached Article II.

153. These transgressions of Separation of Powers principles as well as Article II limitations and duties include, *inter alia*, the following acts and omissions:

a. Using the Presidential Advisory Commission to amass and centralize a federal database *at the White House* or elsewhere with personal and private information of voters.

b. Creating a commission that is not tied to any of the Executive's enumerated Article II powers or to any congressional enactment or authorization.

c. Creating the Presidential Advisory Commission based on a myth of voter fraud and without any legitimate factual finding to support its purported mission.

d. Creating the Presidential Advisory Commission as a ruse to do what the Executive cannot otherwise do – amass and centralize a federal database at the White House with personal and private voter information.

e. Failing to faithfully execute FACA or any other law by allowing the Commission to carry out a secret agenda, to the exclusion of Commission members that are not faithful to the President's belief of voter fraud.

f. Failing to faithfully execute FACA or any other law by allowing the Commission to upload Data to a White House computer system where the Data can be tinkered with behind closed doors and without public knowledge or input.

g. Failing to faithfully execute any law through the creation

of and workings of the Presidential Advisory Commission.

h. Failing to prevent the commission from exceeding its purported authority and purpose as set forth in Section 5 of the Executive Order. That is, by creating a federal database, the Presidential Advisory Commission is duplicating the work of existing government entities, namely the states and other existing, independent election commissions such as the U.S. Election Assistance Commission and Federal Election Commission.

i. Failing to prevent the Presidential Advisory Commission from exceeding its purported authority and purpose as set forth in the Executive Order. The Order does not direct the Presidential Advisory Commission to amass and centralize a federal database at the White House of voters' personal and private information.

j. Failing to prevent the Presidential Advisory Commission from exceeding its own Charter. The Charter does not call on the Presidential Advisory Commission to amass and centralize a federal database at the White House of voters' personal and private information.

k. Failing to prevent the Presidential Advisory Commission from not disclosing its work materials and full membership as required under the Federal Advisory Committee Act, and to otherwise adhere to the FACA disclosure and sunshine requirements as more fully set forth

in Count I.

l. Failing to prevent the commission from exceeding its purported authority and purpose as set forth in Section 5 of the Executive Order. That is, by creating a commission whose goal, *in the written word*, is to protect voting integrity through study of the registration process and voting processes in Federal Elections, the Presidential Advisory Commission is duplicating the work of existing government entities, namely the states and other existing, independent election commissions such as the U.S. Election Assistance Commission and Federal Election Commission.

m. The creation and the activities of the Presidential Advisory Commission unconstitutionally intrude into the Article I powers of Congress over the electoral system, its authority over the protection of the vote, and its authority over the integrity of the election system. The Presidential Advisory Commission's actions violate the separation of powers delineated in the U.S. Constitution.

COUNT III

Violation of The Paperwork Reduction Act, 44 U.S.C. § 3501, *et seq.*

Against Presidential Advisory Commission, Pence, Kobach, Executive Office of the President, Executive Office of the Vice President, Horne, and Mulvaney

154. Plaintiffs restate and incorporate paragraphs 1-92.

155. The Paperwork Reduction Act of 1995 (“PRA”) was designed for multiple purposes, but most notably was intended to minimize the burden on the public and on state governments, to ensure the “greatest possible public benefit from and maximize the utility of information created, collected, maintained, used, shared and disseminated by or for the Federal Government.” 44 U.S.C. § 3501 (2017).

156. For purposes of the PRA, “the term ‘agency’ means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency” 44 U.S.C. § 3502 (2017). The Presidential Advisory Commission is not otherwise specifically excluded. More particularly, the Executive Office of the President is specifically included as an agency bound by the requirements of the PRA.

157. Agencies, such as the Presidential Advisory Commission, when seeking information from more than 10 respondents, must receive approval from the Office of Management and Budget (“OMB”) prior to the collection of information.

158. The OMB is tasked with promulgating the Federal Regulations to effectuate the mandates of the PRA.

159. Prior to its collection of information directed at more than ten respondents, namely each of the 50 States and the District of Columbia, the Presidential Advisory Commission must strictly comply with statutory prerequisites. *See* 44 U.S.C. § 3506 (2017).

160. This includes, in part, preparing for the Director of the OMB a review that identifies the plan for collection of information, inventory, and control numbers for each item, and that:

- (iii) informs the person receiving the collection of information of –
 - (I) the reasons the information is being collected;
 - (II) the way such information is to be used;
 - (III) an estimate, to the extent practicable, of the burden of the collection;
 - (IV) whether responses to the collection of information are voluntary, required to obtain benefit, or mandatory; and
 - (V) the fact that an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number.

44 U.S.C. § 3506(c)(1)(B)(iii).

161. The Commission failed to prepare a review identifying the plan for collection of information, inventory, and control numbers for each item, and that “informs the person receiving the collection of information of” “the reasons the information is being collected;” “the way such information is to be used;” “an estimate, to the extent practicable, of the burden of the collection;” and/or “whether responses to the collection of information are voluntary, required to obtain benefit, or mandatory,” among other things. 44 U.S.C. § 3506(c)(1)(B)(iii).

162. The PRA also requires that the agency must “provide 60-day notice in the Federal Register, and otherwise consult with members of the public and affected

agencies concerning each proposed collection of information,” 44 U.S.C. § 3506(c)(2)(A), and to solicit comments from the public in order to, in pertinent part:

- (i) evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility;
- (ii) evaluate the accuracy of the agency’s estimate of the burden of the proposed collection of information;
- (iii) enhance the quality, utility, and clarity of the information to be collected; and
- (iv) minimize the burden of the collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology[.]

163. Defendants fail to “provide 60-day notice in the Federal Register, and otherwise consult with members of the public and affected agencies concerning each proposed collection of information,” and solicit comments about whether “the proposed collection of information is necessary,” or “practical utility,” the “burden of the proposed collection of information;” and/or about “quality, utility, and clarity of the information to be collected;” and proper collection procedures that “minimize the burden of the collection of information.” 44 U.S.C. § 3506(c)(2)(A).

164. Defendants’ have not complied with, nor have they attempted to comply with, any of the required actions of the PRA.

165. Defendants’ collection of the information sought prior to complying with the requirements of the PRA is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(a) and short of statutory right under 5 U.S.C. § 706(2)(c).

166. The Commission is prohibited from collecting information unless in advance of the collection of information the agency has completed all prerequisites

pursuant to the prior sections and other items set forth in 44 U.S.C. § 3507.

167. Plaintiffs are, individually and in their representative capacities, adversely affected and aggrieved by Defendants' actions and inaction.

168. The only remedy that will grant full relief to Plaintiffs for these violations of the Paperwork Reduction Act is an order enjoining the Defendants to comply with the PRA prior to the collection of any information by the Presidential Advisory Commission.

COUNT IV

**Violation of Florida Statute § 97.0585:
Information Regarding Voters and
Voter Registration Confidentiality**

**Against Presidential Advisory Commission
and Detzner**

169. Plaintiffs restate and incorporate paragraphs 1-92.

170. The Florida Constitution guarantees the right of privacy to all persons,

Art. I, § 23, Florida Constitution:

Right of privacy.—Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.

171. Florida law provides for the confidentiality of certain voter information and voting registration data in § 97.0585, Florida Statutes:

Public records exemption; information regarding voters and voter registration; confidentiality.—

(1) The following information held by an agency as defined in s. 119.011 is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution and may be used only for purposes of voter registration:

(a) All declinations to register to vote made pursuant to ss. 97.057 and 97.058.

(b) Information relating to the place where a person registered to vote or where a person updated a voter registration.

(c) The social security number, driver license number, and Florida identification number of a voter registration applicant or voter.

(2) The signature of a voter registration applicant or a voter is exempt from the copying requirements of s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

(3) This section applies to information held by an agency before, on, or after the effective date of this exemption.

172. The Presidential Advisory Commission's request for voter identifying information includes information deemed confidential under Florida law.

173. The Florida Secretary of State is obligated by the Florida Constitution and laws to preserve and maintain the confidentiality of exempt voter registration information. The Florida Secretary of State must be prohibited from disclosing the private, protected confidential information to the Presidential Advisory Commission. Minimally, the Florida Secretary of State must be enjoined to comply with the requirements in Fla. Stat. § 119.07(1)(d) by redacting any private, protected confidential information to the Presidential Advisory Commission.

174. On July 6, 2017, Defendant Detzner issued a press statement indicating he would comply with the Commission's request for personal voter registration information from Florida's voter database. Defendant Detzner also stated that in doing so, he will comply with the restrictions set forth in § 97.0585 which prohibit the sharing of a voter's social security number and Driver's License number. To ensure Defendant Detzner complies with § 97.0585, and to prohibit the Commission from attempting to obtain that protected information from any other source, Plaintiffs seek an injunction pursuant to § 97.0585 to preclude disclosure of the social security numbers and Driver's License numbers of Florida voters.

175. At the time this lawsuit was first filed, it was not known whether the Florida Secretary of State had already transmitted the voter data to the Commission, and if so whether he had transmitted only that information permitted to be disclosed under Florida constitutional and statutory provisions cited above, nor whether the

transmission of data has been made using a secure method of transmission.

176. Subsequent to the lawsuit being filed, an order was entered in this case enjoining the Florida Secretary of State to comply with such laws.

177. The Defendants should continue to be bound to follow Florida privacy laws preliminarily and permanently.

178. To the extent the Presidential Advisory Commission seeks disclosure of private voter information, the request for information is contrary to Florida law.

179. Plaintiffs are, individually and in their representative capacities, adversely affected and aggrieved by Defendants' actions and inaction.

REQUESTED RELIEF ON ALL COUNTS

Plaintiffs request that this Court:

- A. Order expedited consideration;
- B. Declare that the Presidential Advisory Commission and its members have violated the FACA and enjoin the Presidential Advisory Commission and its members from conducting any business unless and until the FACA is fully complied with, and further enjoin all of the federal Defendants from utilizing the products of any materials or information obtained or produced in violation of the FACA;
- C. Declare and hold unlawful and set aside Defendants' authority to collect personal voter data from the states;
- D. Declare and hold unlawful and set aside Defendants' authority to collect and upload personal voter data from the states to a White House computer system;
- D. Order Defendants to halt collection of personal voter data;

E. Order Defendants to securely delete and properly disgorge any personal voter data collected or subsequently received;

F. Order Defendants to promptly conduct a privacy impact assessment prior to the collection of personal voter data;

G. Declare that the Presidential Advisory Commission and its members have violated the PRA and enjoin the Presidential Advisory Commission and its members from conducting any business unless and until the PRA is fully complied with, and further enjoin all of the federal Defendants from utilizing the products of any materials or information obtained or produced in violation of the PRA;

H. Order Defendant Florida Secretary of State to withhold voter-identifying information from the Presidential Advisory Commission, and to recall all private and public voter information already produced;

I. Award costs and reasonable attorney's fees incurred in this action; and

J. Grant such other relief as the Court may deem just and proper.

Dated: December 9, 2017

Respectfully submitted,

S/ H.K. Skip Pita

H.K. SKIP PITA

Florida Bar No. 101974

PITA WEBER DEL PRADO

9350 S. Dixie Hwy., Suite 1200

Miami, FL 33156

Tel: (305) 670-2889

Fax: (305) 670-6666

spita@pwdlawfirm.com

S/ Jason B. Blank

JASON B. BLANK

Florida Bar No. 28826

HABER BLANK, LLP

888 S. Andrews Ave., Suite 201

Fort Lauderdale, FL 33316

Tel: (954) 767-0300

Fax: (954) 949-0510

eservice@haberblank.com

jblank@haberblank.com

S/ Benedict P. Kuehne

BENEDICT P. KUEHNE

Florida Bar No. 233293

MICHAEL T. DAVIS

Florida Bar No. 63374

KUEHNE DAVIS LAW, P.A.

100 SE 2 Street, Suite 3550

Miami, FL 33131-154

Tel: (305) 789-5989

Fax: (305) 789-5987

ben.kuehne@kuehnelaw.com

mdavis@kuehnelaw.com

efiling@kuehnelaw.com

S/ Marc A. Burton

MARC A. BURTON

Florida Bar No. 95318

S/ Daniel J. Poterek

DANIEL J. POTEREK

Florida Bar No. 85204

THE BURTON FIRM, P.A.

2875 N.E. 191 Street, Suite 403

Miami, Florida 33180

Tel: (305) 705-0888

Fax: (305) 705-0008

mburton@theburtonfirm.com

dpoterek@theburtonfirm.com

pleadings@theburtonfirm.com

S/ Larry S. Davis

LARRY S. DAVIS

Florida Bar No. 437719

S/ Shana Korda

SHANA KORDA

Florida Bar No. 109504

**LAW OFFICE OF LARRY S. DAVIS,
P.A.**

1926 Harrison Street

Hollywood, FL 33020-5018

Tel: (954) 927.4249

Fax: (954) 927-1653

larry@larrysdavislaw.com

shana@larrysdavislaw.com

courtdocs@larrysdavislaw.com

S/ Freddy Funes

FREDDY FUNES

Florida Bar No. 87932

S/ Gerald Greenberg

GERALD GREENBERG

Florida Bar No. 440094

S/ Jarred L. Reiling

JARRED L. REILING

Florida Bar No. 93930

S/ Adam Schachter

ADAM SCHACHTER

Florida Bar No. 647101

**GELBER SCHACHTER &
GREENBERG, P.A.**

Cooperating Counsel

**American Civil Liberties Union
Foundation of Florida**

1221 Brickell Avenue, Suite 2010

Miami, FL 33131-3224
Tel: (305) 728-0950
Fax: (305) 728-0951
jreiling@gsgpa.com

S/ Nancy G. Abudu

NANCY G. ABUDU

Florida Bar No. 111881

Legal Director

AMERICAN CIVIL

LIBERTIES UNION OF

FLORIDA

4343 W. Flagler St., Suite 400

Miami, FL 33134

Tel: (786) 363-2707

Fax: (786) 363-1108

nabudu@aclufl.org

S/ Joseph S. Geller

JOSEPH S. GELLER

Florida Bar No. 292771

GREENSPOON MARDER, P.A.

200 E. Broward Blvd., Suite 1500

Fort Lauderdale, FL 33301-1874

Tel: (954) 491-1120

Fax: (954) 331-2037

joseph.geller@gmlaw.com

CERTIFICATE OF SERVICE

I certify on December 29, 2017, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record identified on the attached service list in the manner specified, either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner.

s/ Benedict P. Kuehne

BENEDICT P. KUEHNE

SERVICE LIST

H.K. SKIP PITA
PITA WEBER DEL PRADO
9350 S. Dixie Hwy., Suite 1200
Miami, FL 33156
Tel: (305) 670-2889
Fax: (305) 670-6666
spita@pwwlawfirm.com
lavarez@pwwlawfirm.com
Co-counsel for Plaintiffs

JASON B. BLANK
HABER BLANK, LLP
888 S. Andrews Ave., Suite 201
Fort Lauderdale, FL 33316
Tel: (954) 767-0300
Fax: (954) 949-0510
eservice@haberblank.com
jblank@haberblank.com
Co-counsel for Plaintiffs

BENEDICT P. KUEHNE
MICHAEL T. DAVIS
KUEHNE DAVIS LAW, P.A.
100 SE 2 Street, Suite 3550
Miami, FL 33131-154
Tel: (305) 789-5989
Fax: (305) 789-5987
ben.kuehne@kuehnelaw.com
mdavis@kuehnelaw.com
efiling@kuehnelaw.com
Co-counsel for Plaintiffs

MARC A. BURTON
DANIEL J. POTEREK
THE BURTON FIRM, P.A.
2999 N.E. 191 Street, Suite 805
Miami, Florida 33180
Tel: (305) 705-0888
Fax: (305) 705-0008
mburton@theburtonfirm.com
dpoterek@theburtonfirm.com
pleadings@theburtonfirm.com
Co-counsel for Plaintiffs

LARRY S. DAVIS
SHANA KORDA
LAW OFFICE OF LARRY S. DAVIS, P.A.
1926 Harrison Street
Hollywood, FL 33020-5018
Tel: (954) 927.4249
Fax: (954) 927-1653
larry@larrysdavislaw.com
shana@larrysdavislaw.com
courtdocs@larrysdavislaw.com
Co-counsel for Plaintiffs

FREDDY FUNES
GERALD GREENBERG
JARRED L. REILING
ADAM SCHACHTER
GELBER SCHACHTER &
GREENBERG, P.A.
Cooperating Counsel ACLU
Foundation of Florida
1221 Brickell Avenue, Suite 2010
Miami, FL 33131-3224
Tel: (305) 728-0950
Fax: (305) 728-0951
jreiling@gsgpa.com
Co-counsel for Plaintiffs

NANCY G. ABUDU
Legal Director
AMERICAN CIVIL LIBERTIES
UNION OF FLORIDA
4343 W. Flagler St., Suite 400
Miami, FL 33134
Tel: (786) 363-2707
Fax: (786) 363-1108
nabudu@aclufl.org
Co-counsel for Plaintiffs Co-counsel for
Plaintiffs

JOSEPH S. GELLER
GREENSPOON MARDER, P.A.
200 E. Broward Blvd., Suite 1500
Fort Lauderdale, FL 33301-1874
Tel: (954) 491-1120
Fax: (954) 331-2037
joseph.geller@gmlaw.com
Co-counsel for Plaintiffs

CHAD A. READLER
ELIZABETH J. SHAPIRO
CAROL FEDERIGHI
Senior Trial Counsel
KRISTINA A. WOLFE
JOSEPH E. BORSON
UNITED STATES DEPARTMENT
OF JUSTICE
Civil Division, Federal Programs
Branch
P.O. Box 883
Washington, DC 20044
Tel: (202) 514-1944
Fax: (202) 616-8460
carol.federighi@usdoj.gov
joseph.borson@usdoj.gov
Counsel for the Federal
Government Defendants

DAVID A. FUGETT
(FBN 835935)
General Counsel
david.fugett@dos.myflorida.com
FLORIDA DEPARTMENT OF
STATE
R.A. Gray Building, Suite 100
500 South Bronough Street
Tallahassee, Florida 32399-0250
Tel: (850) 245-6536
Fax: (850) 245-6127
Lead Counsel for the Florida
Secretary of State

EXHIBIT A

Federal Register

Vol. 82, No. 93

Tuesday, May 16, 2017

Presidential Documents

Title 3—

Executive Order 13799 of May 11, 2017

The President

Establishment of Presidential Advisory Commission on Election Integrity

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote fair and honest Federal elections, it is hereby ordered as follows:

Section 1. *Establishment.* The Presidential Advisory Commission on Election Integrity (Commission) is hereby established.

Sec. 2. *Membership.* The Vice President shall chair the Commission, which shall be composed of not more than 15 additional members. The President shall appoint the additional members, who shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience that the President determines to be of value to the Commission. The Vice President may select a Vice Chair of the Commission from among the members appointed by the President.

Sec. 3. *Mission.* 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.

Sec. 4. *Definitions.* For purposes of this order:

(a) The term "improper voter registration" means any situation where an individual who does not possess the legal right to vote in a jurisdiction is included as an eligible voter on that jurisdiction's voter list, regardless of the state of mind or intent of such individual.

(b) The term "improper voting" means the act of an individual casting a non-provisional ballot in a jurisdiction in which that individual is ineligible to vote, or the act of an individual casting a ballot in multiple jurisdictions, regardless of the state of mind or intent of that individual.

(c) The term "fraudulent voter registration" means any situation where an individual knowingly and intentionally takes steps to add ineligible individuals to voter lists.

(d) The term "fraudulent voting" means the act of casting a non-provisional ballot or multiple ballots with knowledge that casting the ballot or ballots is illegal.

Sec. 5. *Administration.* The Commission shall hold public meetings and engage with Federal, State, and local officials, and election law experts, as necessary, to carry out its mission. The Commission shall be informed by, and shall strive to avoid duplicating, the efforts of existing government entities. The Commission shall have staff to provide support for its functions.

Sec. 6. Termination. The Commission shall terminate 30 days after it submits its report to the President.

Sec. 7. General Provisions. (a) To the extent permitted by law, and subject to the availability of appropriations, the General Services Administration shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis.

(b) Relevant executive departments and agencies shall endeavor to cooperate with the Commission.

(c) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.) (the “Act”), may apply to the Commission, any functions of the President under that Act, except for those in section 6 of the Act, shall be performed by the Administrator of General Services.

(d) Members of the Commission shall serve without any additional compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

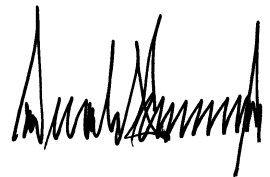
(e) Nothing in this order shall be construed to impair or otherwise affect:

(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.

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

(g) 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.



THE WHITE HOUSE,
May 11, 2017.

EXHIBIT B

**NON-EXHAUSTIVE COMPILATION OF STATEMENTS
BY OR ON BEHALF OF THE PRESIDENT
CONCERNING VOTER FRAUD IN THE 2016 ELECTION**

1. In August 2016, then-Candidate Trump told an audience that:

The only way they can beat me, in my opinion, and I mean this 100 percent, is if in certain sections of the state, they cheat, OK . . . So I hope you people can sort of not just vote . . . (but also) go around and look and watch other polling places and make sure that it's 100 percent fine.

Sachelle Saunders, *Donald Trump wants to fight voter fraud with observers*, Orlando News 6 (August 17, 2017),

[http://www.clickorlando.com/news/politics/trumps-call-for-poll-](http://www.clickorlando.com/news/politics/trumps-call-for-poll-observers-could-cause-trouble)

[observers-could-cause-trouble](http://www.clickorlando.com/news/politics/trumps-call-for-poll-observers-could-cause-trouble). Similarly, on October 1, 2017, then-Candidate Trump told an audience to:

watch your polling booths because I hear too many stories about Pennsylvania, certain areas. . . . We can't lose an election because of, you know what I'm talking about.

Robert Farley, *Trump's Bogus Voter Fraud Claims*, FactCheck.org

(October 19, 2016), [http://www.factcheck.org/2016/10/trumps-bogus-](http://www.factcheck.org/2016/10/trumps-bogus-voter-fraud-claims/)

[voter-fraud-claims/](http://www.factcheck.org/2016/10/trumps-bogus-voter-fraud-claims/). These are just two examples, of many, of Mr.

Trump encouraging people to go to polling sites to intimidate voters.

2. On October 17, 2016, then-Candidate Trump stated:

They even want to try to rig the election at the polling booths. And believe me, there's a lot going on. Do you ever hear these people? They say there's nothing going on. People that have died 10 years ago are still voting. Illegal immigrants are voting. I mean, where are the street smarts of some of these politicians? ... So many cities are corrupt, and voter fraud is very, very common.

Tribune news services, *Trump wrongly insists voter fraud is 'very, very common,'* Chicago Tribune (Oct. 17, 2016),

<http://www.chicagotribune.com/news/nationworld/politics/ct-donald-trump-voter-fraud-20161017-story.html>.

3. That same day (October 17, 2016), then-Candidate Trump also tweeted, with no evidence:

Of course there is large scale voter fraud happening on and before election day. Why do Republican leaders deny what is going on? So naive!

Donald J. Trump (@realDonaldTrump), Twitter (Oct. 17, 2016, 8:33am), <https://twitter.com/realDonaldTrump/status/787995025527410688>.

4. On October 19, 2016, now-Counselor to the President Kellyanne Conway, during the presidential campaign, indicated that she did not believe there would be voter fraud during the 2016 election, stating: "Absent overwhelming evidence that there is, it would not be

for me to say that there is[.]” “[W]hen pressed about specific instances of voter fraud, Conway appeared to suggest that the ‘rigged’ system was not meant to be taken literally, and was simply a rhetorical catch-all for what the campaign view[ed] as injustices in the American political system.” Conway added:

I think everyone is missing his larger point. . . . It is a rigged, corrupt system, whether you believe it’s rigged and corrupt at the polls or whether you believe it’s rigged and corrupt in that we have a \$19 trillion debt and people who are there for years and years, if not decades.

Maxwell Tani, *Donald Trump's campaign manager said she doesn't believe there will be voter fraud*, Business Insider (Oct. 19, 2017), <http://www.businessinsider.com/kellyanne-conway-donaldtrump-rigged-voter-fraud-2016-10>.

5. On November 27, 2016, shortly after the election, the President-Elect continued his baseless accusations about voter fraud, claiming without evidence that he actually won the national popular vote if “illegal” votes were deducted from the total. The President-Elect tweeted:

In addition to winning the Electoral College in a landslide, I won the popular vote if you deduct the millions of people who voted illegally.

Donald J. Trump (@realDonaldTrump), Twitter (Nov. 27, 2016, 3:30pm), <https://twitter.com/realDonaldTrump/status/802972944532209664>. ABC News declared this statement “False,” because “Trump offered no proof to back up this claim, and ABC News, which monitored all 50 states for voting irregularities on election night, has found no evidence of widespread voter fraud.” Lauren Pearle, *Fact-Checking Trump's Claims About ‘Serious Voter Fraud,’* ABC News (Nov. 28, 2016), <http://abcnews.go.com/Politics/fact-checking-trumps-claims-voter-fraud/story?id=43820475>.

6. That same day (November 27, 2016), the President-Elect also tweeted, without evidence, that:

Serious voter fraud in Virginia, New Hampshire and California - so why isn't the media reporting on this? Serious bias - big problem!

Donald J. Trump (@realDonaldTrump), Twitter (Nov. 27, 2016, 7:31pm), <https://twitter.com/realDonaldTrump/status/803033642545115140>. ABC News declared this statement “False,” because “Trump offered no proof to back up this claim, and ABC News found no evidence of widespread voter fraud in those states.” Lauren Pearle, *Fact-Checking Trump's Claims About ‘Serious Voter Fraud,’* ABC News (Nov.

28, 2016), <http://abcnews.go.com/Politics/fact-checking-trumps-claims-voter-fraud/story?id=43820475>.

7. On November 28, 2017, after another presidential candidate had requested a statewide recount in Wisconsin after the election, Spokesman for the Transition Team of the President-Elect, Jason Miller, stated, with no evidence, that:

If this much attention and oxygen is going to be given to a completely obnoxious, throwaway fundraising scheme by someone like [the opposing presidential candidate], then there should be actual substantive looks at overall examples of voter fraud and illegal immigrants voting in recent years.

Brent Griffiths, *Trump spokesman fails to back up Trump claim of voter fraud*, Politico (Nov. 28, 2016), <http://www.politico.com/story/2016/11/trump-voter-fraud-jason-miller-231883>. No evidence was provided in support of the assertions about “voter fraud and illegal immigrants voting in recent years.”

8. On November 30, 2017, Kansas Secretary of State and now-Vice Chair of the Presidential Advisory Commission on Election Integrity, Kris Kobach, stated, despite all legitimate evidence to the contrary, that:

I think the president-elect is absolutely correct when he says the number of illegal votes cast exceeds the popular vote margin

As reported by The Wichita Eagle, Secretary Kobach “had no tangible evidence to support that statement.” Secretary Kobach explained that:

This is the problem with aliens voting and registering. There’s no way you can look at the voter rolls and say this one’s an alien, this one’s a citizen[.] . . . Once a person gets on a voter roll, you don’t have any way of easily identifying them as aliens, so you have to rely on post-election studies.

Bryan Lowry, *Kobach backs Trump’s unsupported claim of millions illegally voting*, The Wichita Eagle (Nov. 30, 2016), <http://www.kansas.com/news/politics-government/election/article117933098.html>.

9. On December 2, 2016, now-Counselor to the President Kellyanne Conway stated, on ABC’s “Good Morning America,” that:

the president-elect has been talking to different people including Kris Kobach, [secretary of state] of Kansas, about voting irregularities or the number of illegal votes that may have been cast, and I believe that he bases his information on that.

and

Well, [the President-Elect has] been receiving information about the irregularities and about the illegal votes, particularly from sources, officials like Kris Kobach as I

mentioned, but he is messaging to his supporters and to the rest of the country the way he feels.

Emily Shapiro, *Kellyanne Conway Dodges Question on Trump's Claim That 'Millions' Voted Illegally*, ABC News (Dec. 2, 2016), <http://abcnews.go.com/Politics/kellyanne-conway-dodges-question-trumps-claim-millions-voted/story?id=43924056>.

10. Shortly after the inauguration, on or about January 23, 2017, the President claimed to members of Congress that people who are in the country illegally caused him to lose the popular vote by almost 3 million votes. When asked about the President's statement, White House Press Secretary Sean Spicer stated that "It was a comment that he made on a long-standing belief," and "He believes what he believes." David Jackson, *Spicer: Trump believes voter fraud claim despite lack of evidence*, USA Today (Jan. 24, 2017), <https://www.usatoday.com/story/news/politics/2017/01/24/donald-trump-sean-spicer-lindsey-graham/96994440/>.

11. On January 25, 2017, the President tweeted:

I will be asking for a major investigation into VOTER FRAUD, including those registered to vote in two states, those who are illegal and....

even, those registered to vote who are dead (and many for a long time). Depending on results, we will strengthen up voting procedures!

Donald J. Trump (@realDonaldTrump), Twitter (Jan. 25, 2017, 7:10 am), <https://twitter.com/realDonaldTrump/status/824227824903090176>; Donald J. Trump (@realDonaldTrump), Twitter (Jan. 25, 2017, 7:13 am), <https://twitter.com/realDonaldTrump/status/824228768227217408>.

12. On January 26, 2017, Counselor to the President Kellyanne Conway previewed the new administration's concern about voter fraud, stating about the President:

He knows there are dead people registered, there are illegal people registered, and he wants to get to the bottom of that without an election on the horizon. Usually, people get all exercised about electoral reform after something goes wrong or ballot integrity when we're about to have an election.

Transcript, *Kellyanne Conway on Trump's voter fraud claims, Mexico and the media*, PBS NewsHour (Jan. 26, 2017), <http://www.pbs.org/newshour/bb/kellyanne-conway-trumps-voter-fraud-claims-mexico-media/>. No evidence was provided.

13. Senior Advisor to the President Stephen Miller, claimed on February 12, 2017:

You have millions of people who are registered in two states or who are dead who are registered to vote. And you have 14

percent of noncitizens, according to academic research, at a minimum, are registered to vote, which is an astonishing statistic.

Madeline Farber, *White House's Stephen Miller Doubles Down on Voter Fraud Claim, But Gives No Evidence*, TIME (Feb. 12, 2017), <http://time.com/4668222/stephen-miller-voter-fraud-george-stephanopolos/>; Associated Press, *Fact check: Trump aide pushes false story of vote fraud*, Honolulu Star Advertiser (Feb. 13, 2017), <http://www.staradvertiser.com/2017/02/13/breaking-news/fact-check-trump-aide-pushes-false-story-of-vote-fraud/>. This statement, too, has been universally rejected by elections professionals.

EXHIBIT C

CHARTER

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY

1. **Committee's Official Designation.** Presidential Advisory Commission on Election Integrity ("Commission").
2. **Authority.** The Commission is established in accordance with Executive Order 13799 of May 11, 2017, "Establishment of a Presidential Advisory Commission on Election Integrity," ("Order") and the provisions of the Federal Advisory Committee Act ("FACA"), as amended (5 U.S.C. App.).
3. **Objectives and Scope of Activities.** The Commission will, consistent with applicable law and the Order, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President of the United States ("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 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.
4. **Description of Duties.** The Commission will function solely as an advisory body.
5. **Agency or Official to Whom the Committee Reports.** The Commission shall provide its advice and recommendations to the President.
6. **Agency Responsible for Providing Support.** The General Services Administration ("GSA") shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission, to the extent permitted by law and on a reimbursable basis. However, the President's designee will be responsible for fulfilling the requirements of subsection 6(b) of the FACA.
7. **Estimated Annual Operating Costs and Staff Years.** The estimated annual costs to operate the Commission are approximately \$250,000 in FY2017 and approximately \$250,000 in FY2018, as needed, including approximately three full-time equivalent employees (FTEs) over the duration of the Commission.
8. **Designated Federal Officer.** Pursuant to 41 CFR § 102-3.105 and in consultation with the chair of the Commission, the GSA Administrator shall appoint a full-time or part-time federal employee as the Commission's Designated Federal Officer ("DFO"). The DFO will approve or

call all Commission meetings, prepare or approve all meeting agendas, attend all Commission meetings and any subcommittee meetings, and adjourn any meeting when the DFO determines adjournment to be in the public interest. In the DFO's discretion, the DFO may utilize other Federal employees as support staff to assist the DFO in fulfilling these responsibilities.

9. **Estimated Number and Frequency of Meetings.** Meetings shall occur as frequently as needed, called, and approved by the DFO. It is estimated the Commission will meet five times at a frequency of approximately 30-60 days between meetings, subject to members' schedules and other considerations.

10. **Duration and Termination.** The Commission shall terminate no more than two (2) years from the date of the Executive Order establishing the Commission, unless extended by the President, or thirty (30) days after it presents its final report to the President, whichever occurs first.

11. **Membership and Designation.**

- (a) The Vice President shall chair the Commission, which shall be composed of not more than fifteen (15) additional members.
- (b) Members shall be appointed by the President of the United States and shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience determined by the President to be of value to the Commission. Members of the Commission may include both regular Government Employees and Special Government Employees.
- (c) The Vice President may select a Vice Chair from among those members appointed by the President, who may perform the duties of the chair if so directed by the Vice President. The Vice President may also select an executive director and any additional staff he determines necessary to support the Commission.
- (d) Members of the Commission will serve without additional compensation. Travel expenses will be allowed, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5701-5707), consistent with the availability of funds.

12. **Subcommittees.** The Chair of the Commission, in consultation with the DFO, is authorized to create subcommittees as necessary to support the Commission's work. Subcommittees may not incur costs or expenses without prior written approval of the Chair or the Chair's designee and the DFO. Subcommittees must report directly to the Commission, and must not provide advice or work products directly to the President, or any other official or agency.

13. **Recordkeeping.** The records of the Commission and any subcommittees shall be maintained pursuant to the Presidential Records Act of 1978 and FACA.

14. **Filing Date.** The filing date of this charter is June 23, 2017.

EXHIBIT D

the WHITE HOUSE



From the Press Office

[Speeches & Remarks](#)

[Press Briefings](#)

[Statements & Releases](#)

[Nominations & Appointments](#)

[Presidential Actions](#)

[Legislation](#)

[Disclosures](#)

The White House

Office of the Vice President

For Immediate Release

June 28, 2017

Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity

This morning, Vice President Mike Pence held an organizational call with members of the Presidential Advisory Commission on Election Integrity. The Vice President reiterated President Trump's charge to the commission with producing a set of recommendations to increase the American people's confidence in the integrity of our election systems.

"The integrity of the vote is a foundation of our democracy; this bipartisan commission will review ways to strengthen that integrity in order to protect and preserve the principle of one person, one vote," the Vice President told commission members today.

The commission set July 19 as its first meeting, which will take place in Washington, D.C.

Vice Chair of the Commission and Kansas Secretary of State Kris Kobach told members a letter will be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls and feedback on how to improve election integrity.



[HOME](#)

[BRIEFING ROOM](#)

[ISSUES](#)

[THE ADMINISTRATION](#)

[PARTICIPATE](#)

[1600 PENN](#)

[USA.gov](#)

[Privacy Policy](#)

[Copyright Policy](#)

EXHIBIT E

Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable Ken Detzner
Secretary of State
R.A. Gray Bldg., 500 S. Bronough, Ste. 100
Tallahassee, FL 32399

Dear Secretary Detzner,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity (“Commission”), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people’s confidence in the integrity of federal elections processes.

As the Commission begins its work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for Florida, including, if publicly available under the laws of your state, the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number

if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at <https://safe.amrdec.army.mil/safe/Welcome.aspx>. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

A handwritten signature in black ink, appearing to read "Kris Kobach". The signature is fluid and cursive, with the first name "Kris" and last name "Kobach" clearly distinguishable.

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

EXHIBIT F



U.S. Department of Justice

Civil Rights Division

*Voting Section - NWB
950 Pennsylvania Ave, NW
Washington, DC 20530*

The Honorable Kim Wyman
Secretary of State
Legislative Building
PO Box 40220
Olympia, WA 98504-0220

JUN 28 2017

Dear Secretary Wyman:

We write to you as the chief election official for the State of Washington to request information regarding the State's procedures for compliance with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 et seq. and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901 et seq. As part of our nationwide enforcement efforts, we are reviewing voter registration list maintenance procedures in each state covered by the NVRA.

The NVRA imposes several requirements on covered states that promote the maintenance of accurate statewide voter lists. Among other things, states must:

- "conduct a general program that makes a reasonable effort to remove the names of ineligible voters" from the statewide voter registration list due to the registrant's death or change of residence (Section 8(a)(4), 52 U.S.C. § 20507(a)(4));
- ensure that the state's general program complies with the requirements and protections imposed by Sections 8(b), (c), and (d) (52 U.S.C. § 20507(b)-(d));
- ensure that any change-of-address form submitted by a voter to a state's motor vehicle authority for driver's licensing purposes serves as a change of address for voter registration purposes, unless the voter states a contrary intention on the form (Section 5(d), 52 U.S.C. § 20504(d));
- ensure that when a registrar receives information that a registered voter has moved to a new address within the registrar's jurisdiction, the voter list is updated to reflect the new address (Section 8(f), 52 U.S.C. § 20507(f)); and
- maintain and make available for public inspection for at least two years "all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters" (Section 8(i), 52 U.S.C. § 20507(i)).

The NVRA imposes these requirements on the state itself. Thus, where a state tasks local election officials with implementing aspects of its list maintenance procedures, the state's chief elections official must "actively oversee the general program" and ensure that it is "reasonably conducted." *United States v. Missouri*, 535 F.3d 844, 850 (8th Cir. 2008).

HAVA also imposes certain list maintenance obligations on states as part of the uniform statewide database requirements of Section 303(a)(2) of HAVA, 52 U.S.C. § 21083(a)(2), including coordinating the state voter registration list with state agency records on felony status and death.

As well as reviewing states' procedures, our efforts to assess compliance with these provisions will also include an analysis of voter registration data reported by each state to the U.S. Election Assistance Commission ("EAC") as part of its biennial Election Administration and Voting Survey ("EAVS"). Data regarding confirmation notices, removals from the voter registration list, and active and inactive registered voters are of particular relevance and are among the categories of data for which reporting is required by EAC regulations. *See* 11 C.F.R. § 9428.7. However, such data for some states were not included in the 2014 EAVS report,¹ the most recent survey results published by the EAC. Thus, some states are receiving a request for any missing data as part of the information requested below. Similarly, we will review the forthcoming 2016 EAVS data when they are available.

To assist our efforts, we respectfully request that you provide us with the following information related to the above requirements:

- All statutes, regulations, written guidance, internal policies, or database user manuals that set out the procedures Washington has put in place relating to:
 - (A) the general program required by Section 8(a)(4) to remove voters from the voter registration list who have become ineligible due to death or change of residence;
 - (B) the requirement of Section 5(d) that motor vehicle changes of address generally serve as updates to voter registration records;
 - (C) any other process that election officials are authorized or required to follow to remove voters by reason of death or change in residence, such as challenge procedures or other list maintenance activities not part of the "general program"; and

¹ U.S. Election Assistance Commission, "The EAC 2014 Election Administration and Voting Survey Comprehensive Report: A Report to the 114th Congress," June 30, 2015, *available at* https://www.eac.gov/assets/1/1/2014_EAC_EAVS_Comprehensive_Report_508_Compliant.pdf.

-3-

- (D) the processes that the state follows for coordinating state databases under HAVA for list maintenance purposes, and any other database coordination or comparison that the state undertakes for list maintenance purposes.

If your state has relevant procedures in place that are not covered by these written materials, please provide a description of them.

- An explanation of which election officials are responsible for implementing Washington's general program of voter registration list maintenance, and for those responsible officials not employed by your office (such as a local election official), a description of the steps that you have taken to ensure that the State's list maintenance program has been properly carried out in full compliance with the NVRA.
- The following data relating to voter registration list maintenance that were requested as part of the EAC's 2014 EAVS and for which Washington's response appears to be incomplete, based on the datasets posted on the EAC's website² (please provide data for each of your state's local jurisdictions for which data were not provided to the EAC):
 - The number of confirmation notices sent to voters in the period between the close of registration for the November 2012 general election and the close of registration for the November 2014 general election (requested by question A10a of the 2014 EAVS Survey Instrument)
 - The number of voters removed from the voter registration rolls in your jurisdiction in the period between the close of registration for the November 2012 general election and the close of registration for the November 2014 general election due to failure to respond to notice sent and failure to vote in the two most recent Federal elections (requested by question A11g of the 2014 EAVS Survey Instrument)

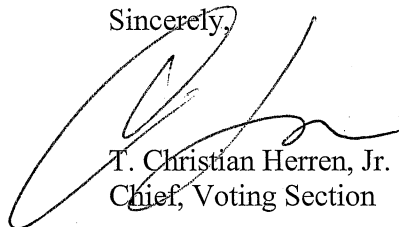
Please also indicate whether Washington is reporting similar data in response to the 2016 EAVS.

² See <https://www.eac.gov/research-and-data/2014-election-administration-voting-survey>; 2014 EAVS Survey Instrument, available at <https://www.eac.gov/assets/1/1/2014%20Election%20Administration%20and%20Voting%20SurveyFinal-2014-05-15.pdf>.

-4-

Please provide this information within 30 days of the date of this letter. The materials may be sent by email to voting.section@usdoj.gov or by FedEx or UPS to Voting Section, Civil Rights Division, Room 7254, U.S. Department of Justice, 1800 G Street NW, Washington, DC 20006. If you have any questions regarding this request, please contact Samuel Olier-Friedland at 202-353-6196 or David Cooper at 202-305-4733. We very much appreciate your cooperation in our nationwide efforts to monitor NVRA compliance.

Sincerely,

A handwritten signature in black ink, appearing to read 'T. Herren', is written over the typed name and title.

T. Christian Herren, Jr.
Chief, Voting Section

cc: Ms. Lori Augino, Director of Elections

EXHIBIT G

Kobach: Why States Need to Assist the Presidential Commission on Election Integrity

by [Kris W. Kobach](#) Jul 2017 5,685



[Irfan Khan/Los Angeles Times via Getty Images](#)

Last Thursday, the Presidential Commission on Election Integrity officially asked each state's chief election official for a copy of their state's publicly-available voter information, in order to better investigate voter fraud

across the nation. I'm the Vice Chair of that Commission, and the letter went out under my signature.

Immediately thereafter, several prominent Democrats declared that they would not comply with this request. California Secretary of State Alex Padilla stated, "California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud made by the President, the Vice President, and Mr. Kobach."

Similarly, Virginia Governor Terry McAuliffe fumed, "I have no intention of honoring this request. Virginia conducts fair, honest, and democratic elections, and there is no evidence of significant voter fraud in Virginia."

Governor McAuliffe's declaration was particularly amusing, because only three days earlier In Virginia, a college student had been convicted of fraudulently registering 18 dead people. Evidently, there's plenty of voter fraud in Virginia. Apparently, McAuliffe is ignorant of what's going on in his own state.

The hyperventilating on the Left about this request is particularly strange since the Commission only requested information that is *already publicly available*. Any person on the street can walk into a county election office and obtain a publicly-available copy of that state's voter rolls—which usually includes voter name, address, date of birth, and the recent elections in which the voter participated. During any campaign season, there are literally hundreds of candidates and campaign workers in every state who possess these same voter rolls. Voter rolls are also frequently obtained by journalists seeking to do election-related research.

Although private information like the last four numbers of a voter's social security number is sometimes included in a state's voter database, that information is usually *not* publicly available. The Commission didn't request

that information. Thus, there is no threat that the Commission's work might compromise anyone's privacy.

The Commission's primary objectives include measuring the amount of voter fraud and improper voter registration in the country. The voter rolls are the obvious starting point for the Commission's work.

Indeed just about every investigation that the Commission undertakes will require a copy of the publicly-available voter rolls for its work to be meaningful. For example, if a witness testifies before the Commission that a certain person voted fraudulently in a given state, the Commission needs to confirm that such a person even exists on the voter rolls and actually cast a ballot in the relevant election.

On a larger scale, the Commission is likely to look at the phenomenon of people registering and/or voting the names of the dead. As the recent Virginia conviction illustrates, this is very much a real problem.

Last year, the Pew Center on the States estimated that more than 1.8 million deceased individuals are still registered to vote. And Pew conceded that their estimate was likely on the low side. The Commission could determine the exact number (rather than relying on an estimate) by running the states' voter rolls against federal and state databases containing the names of deceased individuals.

More importantly, the Commission could answer the question of how many of those deceased individuals were recorded as actually casting a vote in the 2016 election. The number may be large, or it may be small. But the American people deserve to know what it is, either way.

Another important question is how many aliens are illegally registered to vote in the United States. And of those who are registered, how many have actually

voted?

During the Obama Administration, the federal government declined state requests to compare state voter rolls to federal databases of known (legal) aliens residing in the United States. But now the Commission may be able to finally conduct that research. If the same person appears on a state's voter rolls with the indication that he cast a ballot in 2016, and he also appears on the federal government's list of aliens living in the United States, then there is evidence that an alien has likely voted.

That research has never been done before. Many people would like to see just how big this problem is. The consequences are certainly important. Every time an alien votes, it effectively cancels out the vote of a United States citizen.

In my own state of Kansas, one academic expert has estimated that the number of aliens on the voter rolls may exceed 18,000. In a state such as California, that number is likely to be much, much larger. Is that why the California Secretary of State doesn't want the Commission to look at his state's voter rolls?

Finally, some of these opponents of the Commission have suggested that by studying the problem of voter fraud, the Commission will end up suppressing voter turnout in future elections. That is a truly baseless argument. How in the world can studying these statistics and providing information to the American public discourage someone from voting?

The Commission's work is an exercise in transparent government, enhancing the public debate by providing important statistical information. The Commission's report (which will not contain any voter's names) won't cause anyone to stay at home during the 2018 election. It might however, shine some light on voter fraud and encourage some fraudsters to reduce their

activity.

Maintaining the integrity of American elections is essential to the health of our republic. It's also crucial to giving voters confidence that elections will not be stolen.

The bottom line is that without these publicly-available copies of the voter rolls, the Commission will be unable to effectively measure the extent of voter fraud in America. Maybe that's the real objective of the officials who are standing in the way.

Kris W. Kobach is the elected Secretary of State of Kansas. An expert in immigration law and policy, he coauthored the Arizona SB-1070 immigration law and represented in federal court the 10 ICE agents who sued to stop Obama's 2012 executive amnesty. President Trump has named him Vice Chairman of the Presidential Commission on Election Integrity.

EXHIBIT H

Presidential Advisory Commission on Election Integrity

July 26, 2017

Office of the Secretary of State of Florida
The Honorable Ken Detzner, Secretary of State
R.A. Gray Bldg., 500 South Bronough Street
Tallahassee, FL 32399

Dear Secretary Detzner,

In my capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity, I wrote to you on June 28, 2017, to request publicly available voter registration records. On July 10, 2017, the Commission staff requested that you delay submitting any records until the U.S. District Court for the District of Columbia ruled on a motion from the Electronic Privacy Information Center that sought to prevent the Commission from receiving the records. On July 24, 2017, the court denied that motion. In light of that decision in the Commission's favor, I write to renew the June 28 request, as well as to answer questions some States raised about the request's scope and the Commission's intent regarding its use of the registration records. I appreciate the cooperation of chief election officials from more than 30 States who have already responded to the June 28 request and either agreed to provide these publicly available records, or are currently evaluating what specific records they may provide in accordance with their State laws.

Like you, I serve as the chief election official of my State. And like you, ensuring the privacy and security of any non-public voter information is a high priority. My June 28 letter only requested information that is already available to the public under the laws of your State, which is information that States regularly provide to political candidates, journalists, and other interested members of the public. As you know, federal law requires the States to maintain certain voter registration information and make it available to the public pursuant to the National Voter Registration Act (NVRA) and the Help America Vote Act (HAVA). The Commission recognizes that State laws differ regarding what specific voter registration information is publicly available.

I want to assure you that the Commission will not publicly release any personally identifiable information regarding any individual voter or any group of voters from the voter registration records you submit. Individuals' voter registration records will be kept confidential and secure throughout the duration of the Commission's existence. Once the Commission's analysis is

complete, the Commission will dispose of the data as permitted by federal law. The only information that will be made public are statistical conclusions drawn from the data, other general observations that may be drawn from the data, and any correspondence that you may send to the Commission in response to the narrative questions enumerated in the June 28 letter. Let me be clear, the Commission will not release any personally identifiable information from voter registration records to the public.

In addition, to address issues raised in recent litigation regarding the data transfer portal, the Commission is offering a new tool for you to transmit data directly to the White House computer system. To securely submit your State's data, please have a member of your staff contact Ron Williams on the Commission's staff at ElectionIntegrityStaff@ovp.eop.gov and provide his or her contact information. Commission staff will then reach out to your point of contact to provide detailed instructions for submitting the data securely.

The Commission will approach all of its work without preconceived conclusions or prejudgments. The Members of this bipartisan Commission are interested in gathering facts and going where those facts lead. We take seriously the Commissions' mission pursuant to Executive Order 13799 to identify those laws, rules, policies, activities, strategies, and practices that either enhance or undermine the integrity of elections processes. I look forward to working with you in the months ahead to advance those objectives.

Sincerely,

A handwritten signature in black ink, appearing to read "Kris Kobach". The signature is fluid and cursive, with the first name "Kris" and last name "Kobach" clearly distinguishable.

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

EXHIBIT I



Presidential Advisory Commission on Election Integrity

Agenda

Second Meeting of the Presidential Advisory Commission on Election Integrity

Tuesday, September 12, 2017, 10:00 a.m. EST

New Hampshire Institute of Politics, Saint Anselm College

1. **Welcome Remarks – Vice Chairman Kris Kobach; Secretary Bill Gardner; Former New Hampshire Governor and Chief of Staff to Former President George H.W. Bush, John H. Sununu**
2. **Panel One: Historical Election Turnout Statistics and the Effects of Election Integrity Issues on Voter Confidence**
 - Dr. Andrew Smith, Associate Professor of Political Science, University of New Hampshire
 - Kimball Brace, President, Election Data Services, Inc.
 - Dr. John Lott, President, Crime Prevention Research Center and Author, *Evidence of Voter Fraud and the Impact that Regulations to Reduce Fraud Have on Voter Participation Rates* (2006)
 - Q&A and Discussion – All Members
3. **Panel Two: Current Election Integrity Issues Affecting Public Confidence**
 - Donald Palmer, Former Secretary, Virginia State Board of Elections
 - Robert Popper, Director, Election Integrity Project, Judicial Watch
 - Ken Block, President, Simpatico Software Systems
 - Hans von Spakovsky, Senior Legal Fellow, Heritage Foundation and Member, PACEI
 - Q&A and Discussion – All Members
4. **Demonstration of Historic New Hampshire Voting Machines Still in Use Since 1892**
 - Thaire Bryant, Polling Place Moderator for Town of Eaton, New Hampshire
 - T. Patrick Hines, Polling Place Moderator for Town of Windsor, New Hampshire
5. **Panel Three: Electronic Voting Systems and Election Integrity – A Primer**
 - Dr. Andrew Appel, Professor of Computer Science, Princeton University
 - Dr. Ronald Rivest, Professor of Computer Science, Massachusetts Institute of Technology
 - Harri Hursti, Co-Founder of Nordic Innovation Labs
 - Q&A and Discussion – All Members
6. **Discussion and Other Business - All Members**
7. **Closing Remarks – Vice Chairman Kobach and Secretary Gardner**
8. **Adjourn**

EXHIBIT J

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

COMMON CAUSE,

ET AL.,

Plaintiffs,

v.

PRESIDENTIAL ADVISORY COMMISSION ON
ELECTION INTEGRITY,

ET AL.,

Defendants.

No. 1:17-cv-01398, Hon. Royce C.
Lamberth

**BRIEF OF FORMER NATIONAL SECURITY AND TECHNOLOGY
OFFICIALS AS AMICI CURIAE SUPPORTING PLAINTIFFS'
MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTION TO
DISMISS**

JOSHUA A. GELTZER (D.C. Bar No. 1018768)
INSTITUTE FOR CONSTITUTIONAL ADVOCACY
AND PROTECTION
Georgetown University Law Center
600 New Jersey Ave. NW
Washington D.C. 20001
Telephone: 202.661.6728
JG1861@Georgetown.edu

ROBERT S. LITT*
DAVID A. NEWMAN*
SOPHIA M. BRILL*
MORRISON & FOERSTER LLP
2000 Pennsylvania Avenue N.W.
Washington, D.C. 20006

ROBERT TAJ MOORE*
MORRISON & FOERSTER LLP
250 West 55th Street
New York, New York 10019

Counsel for Amici Curiae

* *pro hac vice* motions pending

TABLE OF CONTENTS

TABLE OF CONTENTS..... i

TABLE OF AUTHORITIES ii

INTEREST OF AMICI CURIAE 1

INTRODUCTION 2

ARGUMENT 3

I. THE COMMISSION’S AGGREGATION OF SENSITIVE VOTER DATA AND ITS STORAGE OF THAT DATA AT THE WHITE HOUSE CREATES SUBSTANTIAL CYBERSECURITY VULNERABILITIES 3

A. Aggregating Vast Amounts Of Personal Data Poses A Substantial Risk For Cyberattacks 3

1. Large-scale databases containing personal information are particularly attractive targets for malicious cyber actors..... 3

2. The Commission’s database would likely be targeted by hostile nation-states seeking to interfere in U.S. elections 6

3. The Commission’s database could also be targeted by criminal actors seeking to sell personal data for profit 11

B. Storing Sensitive Personal Data on White House Systems Introduces Heightened Vulnerabilities 12

II. THE COMMISSION’S CREATION OF THIS DATABASE RUNS CONTRARY TO THE PURPOSES OF THE PRIVACY ACT AND COULD CAUSE SIGNIFICANT ONGOING HARM..... 17

A. The Commission’s Conduct Runs Counter To The Privacy Act’s Purpose Of Ensuring That Personal Data Handled By The Federal Government Receives Appropriate Protections..... 17

B. The Commission’s Aggregation Of This Data Could Cause Ongoing Harms That Would Be Difficult To Remedy..... 20

CONCLUSION..... 21

APPENDIX: LIST OF AMICI CURIAE 22

CERTIFICATE OF SERVICE 23

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Am. Civil Liberties Union v. Dep’t of Justice</i> , 655 F.3d 1 (D.C. Cir. 2011).....	6
<i>Attias v. CareFirst, Inc.</i> , 865 F.3d 620 (D.C. Cir. 2017).....	11
<i>Ctr. for Nat’l Sec. Studies v. Dep’t of Justice</i> , 331 F.3d 918 (D.C. Cir. 2003).....	6
<i>Doe v. Dep’t of Justice</i> , 660 F. Supp. 2d 31 (D.D.C. 2009).....	19
<i>Remijas v. Nieman Marcus Group, LLC</i> , 794 F.3d 688 (7th Cir. 2015)	11
<i>United States v. Dokuchaev</i> , No. 3:17-cr-103 (N.D. Cal. Feb. 28, 2017).....	10
<i>United States v. Ferizi</i> , No. 1:16-cr-42 (E.D. Va. June 15, 2016).....	12
Statutes	
5 U.S.C. § 552a.....	17, 18
Executive and Congressional Materials	
Exec. Order No. 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (May 11, 2017)	14
“Federal Information Security Modernization Act of 2014: Annual Report to Congress for Fiscal Year 2016”	13
GAO, “Cybersecurity: Actions Needed to Strengthen U.S. Capabilities” (Feb. 2017)	13
GAO, “Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System” (Jan. 2016).....	13

“Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections” (Jan. 6, 2017).....	6, 7, 8
Memorandum from Jonathan R. Cantor, “DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information” (Apr. 27, 2017).....	19
S. Rep. No. 93-1183 (1974).....	18
Seena Gressin, “The Equifax Data Breach: What to Do,” Federal Trade Commission (Sep. 8, 2017).....	4
Statement of Adm. Michael S. Rogers, Commander, United States Cyber Command, before the Senate Comm. on Armed Services (May 9, 2017)	9
Statement of James R. Clapper before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism (May 8, 2017).....	10
Testimony of Colin Stretch before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism (Oct. 31, 2017)	7
Transcript, “Cybersecurity: Ensuring the Integrity of the Ballot Box,” Hrg. before the House Comm. on Oversight and Gov’t Reform, Subcomm. on Information Technology (Sept. 26, 2016)	9
Transcript, “OPM: Data Breach,” Hrg. before the House Comm. on Oversight and Gov’t Reform (June 16, 2015).....	20
United States Computer Emergency Readiness Team, “Securing Voter Registration Data” (last revised Sept. 30, 2016).....	5, 17
Video Recording, Hrg. before the Senate Comm. on Homeland SEcurity and Governmental Affairs (Sept. 27, 2017)	10
Video Recording, Hrg. before the Senate Select Comm. on Intelligence (Nov. 1, 2017)	7

Other Authorities

Associated Press, “How States Are Handling Trump’s Voter Information Request” (Aug. 2, 2017)	20
Brendan Pierson, “Anthem to Pay Record \$115 Million to Settle U.S. Lawsuits Over Data Breach,” <i>Reuters</i> (June 23, 2017).....	4
Brian Bennet & W.J. Hennigan, “China and Russia Are Using Hacked Data to Target U.S. Spies, Officials Say,” <i>Los Angeles Times</i> (Aug. 31, 2015).....	10
Daisuke Wakabayashi & Scott Shane, “Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election,” <i>N.Y. Times</i> (Sept. 27, 2017)	7

Dell Cameron, “Even a Novice Hacker Could Breach Network Hosting Kris Kobach’s Bogus Voter Fraud Program,” <i>Gizmodo.com</i> (Nov. 9, 2017)	17
Demetri Sevastopvlo, “Chinese Hack Into White House Network,” <i>Financial Times</i> (Nov. 6, 2008)	16
Devlin Barrett & Siobhan Gorman, “Gmail Hack Targeted White House,” <i>Wall St. J.</i> (June 3, 2011).....	16
Ellen Nakashima, “Hackers Breach Some White House Computers,” <i>Wash. Post</i> (Oct. 28, 2014)	16
George R. Lynch, “Website Creating Company Faces Data Breach Affecting Over 40 Million Users,” <i>Bloomberg BNA</i> (Oct. 24, 2016).....	4
Jaikumar Vijayan, “The Identity Underworld: How Criminals Sell Your Data on the Dark Web,” <i>Christian Science Monitor</i> (May 6, 2015).....	11
Jennifer Martinez, “White House Thwarts Hacker Attack on Unidentified Computer System,” <i>The Hill</i> (Oct. 1, 2012)	16
Jessica Huseman & Derek Willis, “The Voter Fraud Commission Wants Your Data—But Experts Say They Can’t Keep It Safe,” <i>ProPublica</i> , (Oct. 23, 2017)	17
Lillian Ablon, et al., <i>Markets for Cybercrime Tools and Stolen Data</i> , RAND Corporation (2014).....	11
Michael Chertoff, “Trump’s Voter Data Request Poses An Unnoticed Danger,” <i>Wash. Post</i> (July 15, 2017)	13
Michael Shear, “Technology Upgrades Get White House Out of the 20th Century,” <i>N.Y. Times</i> (Apr. 3, 2016).....	15
Sari Horowitz, et al., “DHS Tells States About Russian Hacking During 2016 Election,” <i>Wash. Post</i> (Sept. 22, 2017).....	9
Sasha Issenberg, <i>The Victory Lab: The Secret Science of Hidden Campaigns</i> (2013).....	6
Scott Shane, “These Are the Ads Russia Bought on Facebook in 2016,” <i>N.Y. Times</i> (Nov. 1, 2017)	7
Taylor Hatmaker, “Exposed GOP Database Demonstrates the Risks of Data-Hungry Political Campaigns,” <i>TechCrunch</i> (June 19, 2017)	8

INTEREST OF AMICI CURIAE

Amici curiae are former national security and technology officials who have a wealth of experience combatting cyber threats posed by foreign adversaries and other malicious actors.¹ Amici have worked at senior levels in administrations of both parties and share strong concerns about securing the integrity of our nation's electoral systems. This brief is intended to highlight for the Court a particular aspect of this litigation that has been referred to but not substantially discussed by either party: the potentially serious national security and cybersecurity implications of the Presidential Advisory Commission on Election Integrity's compilation of a massive database of personally identifiable information about American voters and its storage of that database on White House systems. Amici are uniquely positioned to provide the Court with information and insight about the risks that such a database could be breached, as well as the potential consequences of such a breach.

¹ No counsel for a party authored this brief in whole or in part, and no party or counsel for a party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than amici curiae, their members, or their counsel made a monetary contribution to the preparation or submission of this brief.

INTRODUCTION

Americans recently witnessed an unprecedented attack against our democracy by a hostile nation-state that sought to influence the outcome of our elections. Numerous current and former national security officials and cybersecurity experts have highlighted the urgent need to prevent similar activities—or worse—from occurring in the next election cycle. Our election infrastructure is a continuing target for foreign adversaries, including Russia, and these adversaries are capable of, and increasingly intent on, waging sophisticated cyber campaigns against core U.S. democratic institutions.

The stated mission of the Presidential Advisory Commission on Election Integrity (the “Commission”) is to ensure the integrity of our electoral systems. But given the advanced cyber threats posed by foreign adversaries, there is a serious risk that the Commission’s activities will ultimately make U.S. election systems more susceptible to compromise and abuse. The Commission has aggregated and continues to aggregate large volumes of data about American voters, including names, addresses, partial social security numbers, and voting history, into one centralized database stored, operated, and maintained by the White House. That database may be a compelling target for foreign adversaries seeking to interfere in future elections through a variety of means, as well as for cyber criminals and other malicious actors. Yet, despite this grave vulnerability, the Commission chose to move the database from a network administered by the Department of Defense to an ad hoc system built by White House personnel. *Amici*, who have a wealth of experience as national security and cybersecurity officials, have authored this brief in order to highlight the substantial risks that assembling and maintaining such a database could create.

For all of the vulnerabilities demonstrated during last year’s elections, one feature of our state-based election system that poses challenges to would-be attackers is the extent of its

decentralization—including the degree to which information that could be used to exploit potential vulnerabilities is widely dispersed across numerous systems, formats, and regions. That strength is critically undermined by the Commission’s conduct and will continue to be undermined so long as the Commission’s database is maintained. Because the Commission’s maintenance of this database could enable malicious actors to inflict significant harms on the nation’s electoral process as well as on individual voters, *amici* seek to inform the Court’s understanding of these potential harms as it evaluates Plaintiffs’ complaint and the Government’s motion to dismiss.

ARGUMENT

I. THE COMMISSION’S AGGREGATION OF SENSITIVE VOTER DATA AND ITS STORAGE OF THAT DATA AT THE WHITE HOUSE CREATES SUBSTANTIAL CYBERSECURITY VULNERABILITIES

By aggregating large volumes of personal data in one centralized location, the Commission has created and continues to maintain a compelling target for foreign adversaries and other malicious actors. Personally identifiable information (“PII”) about millions of American voters would be extremely valuable to foreign adversaries seeking to interfere in future elections. This data would also be a valuable target for criminal organizations seeking to steal it for purposes of identity theft or to sell on the black market. Moreover, the Commission has compounded these risks by hosting the database on a White House system that has never been used to store information of this kind and may lack core safeguards.

A. Aggregating Vast Amounts Of Personal Data Poses A Substantial Risk For Cyberattacks

1. *Large-scale databases containing personal information are particularly attractive targets for malicious cyber actors*

A database that contains large volumes of PII is an extremely attractive target for cyberattacks. Hackers seek to exploit this type of information for a number of reasons, ranging

from ordinary criminal profiteering (e.g., to commit identity theft or to sell the information on the black market for others to commit identity theft) to intelligence collection by hostile nation states or non-state actors. The bigger the database, the greater the payoff from a potential breach.

A large database aggregating PII of millions of American voters in one place, as the Commission has compiled and continues to compile, would constitute a treasure trove for malicious actors. One need only examine some of the most recent high-profile data breaches to understand the extent to which information of this nature is regularly targeted by a wide range of actors and the potential harm that could ensue from a breach. The recent attack against Equifax, for example, compromised the information of up to 143 million people, including their names, addresses, dates of birth, credit card information, social security numbers, and driver's license numbers.² Major breaches against health care providers and retail companies have demonstrated similar patterns. For example, the 2015 Anthem breach compromised names, birth dates, social security numbers, e-mail addresses, and income information of a reported 79 million people.³ In 2016, Weebly, a web-hosting service, experienced a hack that exposed the IP addresses, usernames and/or e-mail addresses, and hashed passwords of some 43 million users.⁴ Government databases with large volumes of PII have also been the subject of significant

² Seena Gressin, "The Equifax Data Breach: What to Do," Federal Trade Commission (Sept. 8, 2017), available at <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>.

³ Brendan Pierson, "Anthem to Pay Record \$115 Million to Settle U.S. Lawsuits Over Data Breach," *Reuters* (June 23, 2017), available at <https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML>.

⁴ George R. Lynch, "Website Creating Company Faces Data Breach Affecting Over 40 Million Users," *Bloomberg BNA* (Oct. 24, 2016), available at <https://www.bna.com/website-creating-company-b57982079041/>.

breaches—including the infamous breach of the federal Office of Personnel Management, which resulted in the theft of highly sensitive information about more than 20 million Americans.

The proliferation of such attacks poses profound challenges to many facets of our election system. The Department of Homeland Security has warned that “[v]oter registration databases present a unique target for cyber threat actors” and that “[i]t is vital that security professionals take precautions to defend [these systems] against intrusion.”⁵ The information that the Commission has requested and continues to aggregate contains basic PII such as names, addresses, and dates of birth, as well as more sensitive information such as partial social security numbers, voting history, criminal records, and military status. See Pls.’ Amended Compl. ¶ 62, ECF No. 21 (describing information requested by the Commission); Pls.’ Opp. to Mot. to Dismiss Exh. G-2, at 8-9, ECF No. 30 (listing various states that have provided data to the Commission).⁶ Even if some of this information may already be publicly available, it becomes far more valuable to malicious actors when centralized and combined with other public and non-public information.

That risk is particularly grave in the event that the data is acquired by hostile nation-states, which may be capable of culling through large volumes of information and combining that information with data already in their possession in order to assemble more comprehensive files about American citizens for espionage and counter-intelligence purposes. As the Court of Appeals for the D.C. Circuit has noted in the context of national security information, new disclosures of information must be viewed in light of a broader “mosaic” because “[w]hat may

⁵ United States Computer Emergency Readiness Team, “Securing Voter Registration Data” (last revised Sept. 30, 2016), available at <https://www.us-cert.gov/ncas/tips/ST16-001>.

⁶ Copies of the underlying letters from the Commission’s Vice Chair, Kris W. Kobach, seeking information from all 50 states and from the District of Columbia are available at <https://www.whitehouse.gov/sites/whitehouse.gov/files/docs/information-requests-to-states-06282017.pdf>.

seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.” *Ctr. for Nat’l Sec. Studies v. Dep’t of Justice*, 331 F.3d 918, 928 (D.C. Cir. 2003) (quoting *CIA v. Sims*, 471 U.S. 159, 178 (1985)) (alterations in original); see also *Am. Civil Liberties Union v. Dep’t of Justice*, 655 F.3d 1, 9 (D.C. Cir. 2011) (“an individual’s privacy interest in limiting disclosure or dissemination of information does not disappear just because it was once publicly released” (citing *Dep’t of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 762-63 (1989))). In recent years, electoral politics and campaigning have been transformed by the trend toward intensively compiling and mining seemingly innocuous bits of user data—including the very types of data that the Commission seeks to ingest—in search of hidden insights about voter behavior.⁷ This trend has not gone unnoticed by America’s sophisticated foreign adversaries.

2. The Commission’s database would likely be targeted by hostile nation-states seeking to interfere in U.S. elections

The 2016 election cycle teaches a critical lesson: American voters and the integrity of our election systems are targets for hostile nation-states. By interfering with our nation’s electoral process, foreign adversaries can seek to undermine not only particular candidates but also our democracy as a whole. That was Russia’s clear goal in 2016. The United States Intelligence Community concluded unanimously that “Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election.” “Intelligence Community Assessment: Assessing Russian Activities and Intentions in Recent US Elections,” at ii (Jan. 6, 2017) (“ICA”).⁸ This influence campaign “followed a Russian messaging strategy that blends covert intelligence operations—such as cyber activity—with overt efforts by Russian Government

⁷ See generally Sasha Issenberg, *The Victory Lab: The Secret Science of Hidden Campaigns* (2013) (discussing rising use of data analysis in political campaigns).

⁸ Available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

agencies, state-funded media, third-party intermediaries, and paid social media users or ‘trolls.’”

Id.

The ICA highlights multiple aspects of Russia’s influence campaign, including its hacking and leaking of e-mails, its intrusions into state and local electoral boards, and its social media efforts that sought to drive propaganda. ICA at 2-4. News reports continue to shed light on these social media efforts, and Congress has recently heard testimony about Russia’s extensive efforts to purchase advertising, to maintain fake social media accounts and “troll farms,” and to target particular types of voters.⁹

Voter targeting efforts, in particular, could benefit from access to the types of information maintained by the Commission. Armed with names, addresses, and voting histories—including information about individuals’ party registration and frequency of voting—a foreign adversary such as Russia could conduct targeted information campaigns against particular subsets of voters. It could even seek to undermine voters’ access to the polls by, for example, targeting individuals of one party or another (or perhaps of all parties) with disinformation about the locations or hours of polling places or false reports that an election has been postponed or

⁹ Video Recording, Hrg. before the Senate Select Comm. on Intelligence at 00:53:09 – 00:57:20 (Sen. Richard Burr describing how “Russia trolls” created two competing Facebook groups that encouraged “both sides to battle in the streets,” a tactic intended to create “divisions between real Americans.”), available at <https://www.intelligence.senate.gov/hearings/open-hearing-social-media-influence-2016-us-elections>; Testimony of Colin Stretch before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism, at 6 (Oct. 31, 2017) (stating that approximately 126 million people may have seen Russian-sponsored content on Facebook between 2015 and 2017), available at <https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Stretch%20Testimony.pdf>; Scott Shane, “These Are the Ads Russia Bought on Facebook in 2016,” *N.Y. Times* (Nov. 1, 2017), available at https://www.nytimes.com/2017/11/01/us/politics/russia-2016-election-facebook.html?_r=0; Daisuke Wakabayashi & Scott Shane, “Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election,” *N.Y. Times* (Sept. 27, 2017) (describing Russia’s use of fake Twitter accounts to influence the 2016 elections and to continue sowing political and social discord since), available at <https://www.nytimes.com/2017/09/27/technology/twitter-russia-election.html>.

canceled. In short, a national database containing this type of information constitutes a particularly attractive target for Russia or other adversaries seeking to conduct these types of hostile activities. Even if it is correct that some of the information is available in disparate locations and formats across the United States, such as in states' voter registration records or in political parties' databases, and indeed even if private actors, such as the Republican and Democratic National Committees, have reportedly already attempted to compile a wide range of data on American voters—an effort that may have itself created vulnerabilities¹⁰—the Federal Government should be seeking ways to mitigate those risks, not to compound and exacerbate them. Aggregating a comprehensive and official set of such data onto one high-profile, widely publicized server maintained by the White House may reduce the technical and practical barriers to a foreign adversary acquiring such information and making use of it without detection.

Additionally, if a foreign adversary or other malicious actor were capable of *altering* the information contained in the database, the results could have other serious implications for future elections. To choose one example, an adversary could manipulate records to create phony irregularities (such as by altering social security numbers or criminal histories) in the hopes of spawning baseless inquiries and investigations that could result in the wrongful removal of legitimate voters from registration rolls. The events of 2016 demonstrate that Russia did in fact target voter registration rolls as part of its active measures campaign. The Intelligence Community concluded that “Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards”—though they did not access systems involved in vote tallying. ICA at iii; *see also id.* at 3. Thomas Hicks, Chairman of the United States

¹⁰ See Taylor Hatmaker, “Exposed GOP Database Demonstrates the Risks of Data-Hungry Political Campaigns,” *TechCrunch* (June 19, 2017), available at <https://techcrunch.com/2017/06/19/deep-root-gop-data-leak-upguard/>.

Election Assistance Commission, testified before Congress last fall that hackers had breached Arizona and Illinois' voter registration lists.¹¹ More recently, the Department of Homeland Security reportedly notified officials in 21 states that their states' electoral systems were targeted by Russian hackers during the 2016 election.¹² Notably, Mr. Hicks observed in his testimony that a key strength of our electoral system is its decentralization, because "there is no national system that a hacker or bad actor can infiltrate to affect the American elections as a whole."¹³ A centralized voter registration database creates just such a target.

A number of current and former government officials have further warned that Russia and other foreign adversaries will seek to interfere in future elections and that such behavior may even escalate. Admiral Michael Rogers, director of the National Security Agency, testified before Congress that "[w]e have seen states seeking to shape the policies and attitudes of democratic peoples, and we are convinced such behavior will continue for as long as autocratic regimes believe they have more to gain than to lose by challenging their opponents in cyberspace."¹⁴ James Clapper, the former Director of National Intelligence, similarly testified that Russia is now "emboldened to continue" its election interference activities, "and to do so

¹¹ See Transcript, "Cybersecurity: Ensuring the Integrity of the Ballot Box," Hrg. before the House Comm. on Oversight and Gov't Reform, Subcomm. on Information Technology (Sept. 26, 2016), Statement of Thomas Hicks ("Hicks Statement"), at 17, available at <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg26124/pdf/CHRG-114hhrg26124.pdf>.

¹² Sari Horowitz et al., "DHS Tells States About Russian Hacking During 2016 Election," *Wash. Post* (Sept. 22, 2017), available at https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html?utm_term=.56fba78532a2.

¹³ Hicks Statement at 12.

¹⁴ Statement of Adm. Michael S. Rogers, Commander, United States Cyber Command, before the Senate Comm. on Armed Services, at 2 (May 9, 2017), available at https://www.armed-services.senate.gov/imo/media/doc/Rogers_05-09-17.pdf.

even more intensely.”¹⁵ Members of Congress, meanwhile, have repeatedly expressed concerns about future election interference and the adequacy of existing measures to protect against further attacks, including potential tampering with voter registration systems.¹⁶

Finally, hostile nation-states could attempt to breach the Commission’s database for espionage purposes not directly related to election interference. For example, the Justice Department has charged two officers belonging to the Russian Federal Security Service (as well as two other individuals) with orchestrating a massive breach of Yahoo’s networks and accessing information regarding more than 500 million Yahoo user accounts.¹⁷ The indictment alleges that the conspirators used this information to target particular victims of interest to Russian intelligence as well as to orchestrate various scams.¹⁸ It has also been reported that other hacked files pertaining to American citizens are being used by foreign intelligence services, including in China and Russia, to assemble and cross-index databases that could be used to identify and even blackmail U.S. intelligence operatives.¹⁹

¹⁵ Statement of James R. Clapper before the Senate Comm. on the Judiciary, Subcomm. on Crime and Terrorism, at 5 (May 8, 2017), available at <https://www.judiciary.senate.gov/imo/media/doc/05-08-17%20Clapper%20Testimony.pdf>.

¹⁶ See, e.g., Video Recording, Hrg. before the Senate Comm. on Homeland Security and Governmental Affairs (Sept. 27, 2017) at 01:41:45 – 01:42:33 (questions from Sen. Claire McCaskill to Elaine Duke, Acting Secretary of DHS, and Christopher Wray, Director of the FBI, concerning measures to prevent interference in future elections); *id.* at 01:49:55 – 01:50:22 (question from Sen. James Lankford expressing concerns about tampering with voter registration lists), available at <https://www.c-span.org/video/?434411-1/senior-officials-testify-homeland-security-threats&start=6178>.

¹⁷ See Indictment, *United States v. Dokuchaev*, No. 3:17-cr-103, ECF No. 1 (N.D. Cal. Feb. 28, 2017).

¹⁸ *Id.* ¶¶ 34-39.

¹⁹ See Brian Bennet & W.J. Hennigan, “China and Russia Are Using Hacked Data to Target U.S. Spies, Officials Say,” *Los Angeles Times* (Aug. 31, 2015), <http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html>.

3. *The Commission's database could also be targeted by criminal actors seeking to sell personal data for profit*

Aggregating large volumes of PII also creates a target for malicious actors seeking to sell such information for profit. This information is valuable to cybercriminals because it can be used to commit identity theft and other acts of fraud. Indeed, there is a sophisticated global black market for stolen PII that reflects the value of this information.²⁰ The demand for stolen PII, in turn, fuels incentives for malicious actors to target networks with large data sets.

This reality has led courts to recognize that individuals whose personal data is stolen are at risk of identity theft. *See Attias v. CareFirst, Inc.*, 865 F.3d 620, 627-29 (D.C. Cir. 2017) (finding that plaintiffs established a “substantial risk” of identity theft after hackers breached the network of a healthcare provider and stole various types of PII); *Remijas v. Nieman Marcus Group, LLC*, 794 F.3d 688, 692-94 (7th Cir. 2015) (noting a similar risk and suggesting that, “[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers’ identities”). While credit card information may be in greater demand by some actors than the types of PII at issue here, malicious actors can use other types of information—particularly including names, addresses, and social security numbers—to sell for profit or to combine and cross-reference with other datasets to assemble more complete profiles of individuals targeted for identity theft.

There is also a distinct possibility that “ordinary” criminals who breach networks in order to obtain and sell PII could sell that information to parties with more hostile and dangerous ends

²⁰ See, e.g., Lillian Ablon et al., *Markets for Cybercrime Tools and Stolen Data*, RAND Corporation (2014), available at https://www.rand.org/pubs/research_reports/RR610.html; Jaikumar Vijayan, “The Identity Underworld: How Criminals Sell Your Data on the Dark Web,” *Christian Science Monitor* (May 6, 2015), available at <https://www.csmonitor.com/World/Passcode/2015/0506/The-identity-underworld-How-criminals-sell-your-data-on-the-Dark-Web>.

in mind. Last year, for example, Ardit Ferizi, a hacker who obtained PII about hundreds of U.S. citizens and provided this information to ISIS, pleaded guilty to hacking and providing material support for terrorism. See Statement of Facts, *United States v. Ferizi*, No. 1:16-cr-42, ECF No. 36 (E.D. Va. June 15, 2016) (describing facts admitted by Ferizi as part of a plea agreement). Ferizi admitted that he gained access to the server of a retail company based in the United States that contained the PII of tens of thousands of customers and culled that information to identify government employees and military service members. *Id.* at 3. He then passed that information to a well-known member of ISIS who posted it online and used it to call for attacks against specific individuals. *Id.* at 3-5.²¹

In this case, cyber criminals could conclude that a successful breach of the Commission's database would be rewarded by a substantial bounty from whatever buyer is most interested in obtaining and/or altering the information, and could seek to sell to the highest bidder this information or the tools that could be used to penetrate the database.

B. Storing Sensitive Personal Data on White House Systems Introduces Heightened Vulnerabilities

Federal networks are regularly targeted for attacks by malicious actors, including by nation-states and other sophisticated adversaries seeking precisely the type of information that the Commission is aggregating. As former Secretary of Homeland Security Michael Chertoff has warned in reference to the activities of the Commission:

We know that a database of personal information from all voting Americans would be attractive not only to adversaries seeking to affect voting but to criminals who could use the identifying information as a wedge into identity theft. We also know that foreign intelligence agencies seek large databases on Americans for intelligence and counterintelligence purposes. That is why the theft of more than 20 million personnel

²¹ Ferizi appears to have provided the information to ISIS free of charge. But other criminal actors could just as easily sell this type of information to a terrorist organization or hostile nation-state.

files from the U.S. Office of Personnel Management and the hacking of more than half a billion Yahoo accounts were such troubling incidents.²²

The Office of Personnel Management breach to which Secretary Chertoff referred was reported in 2015 and resulted in the exposure of the personal information of more than 20 million Americans. The Government Accountability Office (“GAO”) has repeatedly observed that breaches of federal networks are on the rise and that these attacks are evolving and becoming more sophisticated. *See, e.g.*, GAO, “Information Security: DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System” (Jan. 2016) (noting that “[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive”).²³

Similarly, the White House has reported that federal agencies experienced 30,899 “reportable” cyber incidents for the 2016 fiscal year, 16 of which rose to the threshold of a “major incident” (meaning the incident involved certain types of critical information or that records were compromised on a large scale).²⁴ An Executive Order signed earlier this year took

²² Michael Chertoff, “Trump’s Voter Data Request Poses An Unnoticed Danger,” *Wash. Post* (July 15, 2017), available at https://www.washingtonpost.com/opinions/trumps-voter-data-request-poses-an-unnoticed-danger--to-national-security/2017/07/05/470efce0-60c9-11e7-8adc-fea80e32bf47_story.html?tid=a_inl&utm_term=.c07d23da07ef.

²³ Available at <https://www.gao.gov/assets/680/674829.pdf>. *See also* GAO, “Cybersecurity: Actions Needed to Strengthen U.S. Capabilities” (Feb. 2017), available at <https://www.gao.gov/assets/690/682756.pdf>

²⁴ *See* “Federal Information Security Modernization Act of 2014: Annual Report to Congress for Fiscal Year 2016,” at 111, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf.

note of these risks, highlighting among other findings that “[t]he executive branch has for too long accepted antiquated and difficult-to-defend [information technology].”²⁵

The Commission’s seemingly last-minute decision to move the database from the control of the Department of Defense (“DOD”) to the White House only exacerbates the database’s vulnerability. The Commission initially intended to use DOD’s Safe Access File Exchange (“SAFE”), which Vice Chair Kobach described in another lawsuit as a “tested and reliable method to secure file transfer used routinely by the military for large, unclassified data sets.” Decl. of Kris W. Kobach ¶ 5, *Elec. Privacy Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity* (“EPIC”), EFC No. 8, No. 1:17-cv-1320 (D.D.C. July 5, 2017). Just five days later, after the plaintiffs in that case amended their complaint to name DOD as a defendant, see ECF No. 21, *EPIC* (July 7, 2017), Vice Chair Kobach issued a new declaration stating that the Commission no longer intended to use DOD’s SAFE system and would instead “repurpos[e]” a White House system to accept the voter data. Third Decl. of Kris W. Kobach ¶ 1, ECF No. 24-1, *EPIC* (July 10, 2017) (“Third Kobach Declaration”).²⁶ The only explanation offered for the move was a somewhat cryptic statement that it was intended “not to impact the ability of other customers to use the DOD [SAFE] site.” *Id.* The Commission has also not disclosed which White House system has been “repurposed” to accept the PII of millions of Americans or what measures are in place to protect that data adequately, underscoring the importance of further factfinding on these matters. Based on what is already known, however, there is substantial

²⁵ Exec. Order No. 13800, “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure” (May 11, 2017), available at <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.

²⁶ These declarations have also been filed as exhibits to the Government’s Motion to Dismiss in this case. See ECF No. 27, Exhs. B and C.

reason to believe that the Commission has gone about its work in ways that subject the data to significant vulnerabilities and indeed exacerbate those vulnerabilities.

As an initial matter, this White House system has been newly developed—apparently within a matter of days. See Third Kobach Declaration ¶ 1 (stating that the new White House system was expected to be operational by later that day). As such, this new platform is effectively being tested for the first time through the ingestion of millions of data points about American voters. Additionally, the White House’s Information Technology staff does not have the same technical resources at its disposal to maintain large-scale databases as the Department of Defense.²⁷ Indeed, the Government has expressly affirmed that other White House components, such as the Executive Committee for Information Technology and the U.S. Digital Service, will have “no role” in administering the Commission’s database and that only a “limited number of [] technical staff” will be involved. Mot. to Dismiss, Exh. E, Decl. of Charles Christopher Herndon ¶ 6, ECF No. 27 (“Herndon Declaration”).

These limitations may well have been put in place in an effort to reduce the number of government officials with access to the information. But from a cybersecurity standpoint, the limited extent of information technology resources and personnel available to support the Commission’s work is alarming insofar as White House systems and personnel are regularly the subject of cyberattacks from sophisticated adversaries that require resource-intensive

²⁷ See, e.g., Michael Shear, “Technology Upgrades Get White House Out of the 20th Century,” *N.Y. Times* (Apr. 3, 2016) (noting that “[u]ntil very recently, West Wing aides were stuck in a sad and stunning state of technological inferiority” and describing ongoing challenges), available at <https://www.nytimes.com/2016/04/04/us/politics/technology-upgrades-get-white-house-out-of-the-20th-century.html>.

responses.²⁸ Moreover, there is no indication that the Commission has taken the appropriate additional measures, and allocated the necessary additional resources, to fortify its database against these risks. Given that attempted attacks against White House unclassified networks are regularly reported in the media (and therefore should be well known to the Commission), this suggests an overall lack of attentiveness to the magnitude and gravity of the cybersecurity risks posed.²⁹

Mr. Herndon's Declaration describes certain basic measures that he avows have been taken or will be taken to secure the Commission's database, such as his assertion that the data will be encrypted and that Commission members will be able to access it through dedicated laptops with secure connection mechanisms. Herndon Declaration ¶ 5. But, on numerous other fronts, Mr. Herndon's Declaration is silent, leaving open the very real possibility that serious vulnerabilities remain in the way that the Commission is going about its work. Most notably, there is no indication that there are measures in place—including steps consistent with previous DHS recommendations for securing voter databases—that would: (1) restrict access only to Commission members as opposed to their staffs, or perhaps only those staff members specifically involved in analyzing the raw data; (2) restrict administrative privileges; (3) conduct

²⁸ Jennifer Martinez, "White House Thwarts Hacker Attack on Unidentified Computer System," *The Hill* (Oct. 1, 2012), available at <http://thehill.com/policy/technology/259461-hackers-attack-white-house-computer-system>; Demetri Sevastopvlo, "Chinese Hack Into White House Network," *Financial Times* (Nov. 6, 2008), available at <https://www.ft.com/content/2931c542-ac35-11dd-bf71-000077b07658> (subscription required). See also Devlin Barrett & Siobhan Gorman, "Gmail Hack Targeted White House," *Wall St. J.* (June 3, 2011) (describing how Chinese hackers breached Gmail systems and targeted White House employees), available at <https://www.wsj.com/articles/SB10001424052702304563104576361863723857124> (subscription required).

²⁹ See, e.g., Ellen Nakashima, "Hackers Breach Some White House Computers," *Wash. Post* (Oct. 28, 2014), available at https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html?utm_term=.7888768cd42e.

penetration testing and security audits; and (4) provide basic cybersecurity training to Commission members and their staffs, including training to avoid phishing attempts.³⁰ The need for basic cybersecurity training appears especially heightened in light of reports that a voter database previously created by Vice Chair Kobach is riddled with vulnerabilities, including through human errors such as officials sending passwords through email and even exposing them publicly.³¹ Finally, because no assurance has been given that the Commission's database would be wholly cut off from other White House systems, a breach of those other systems could provide a platform from which intruders could penetrate the database.

II. THE COMMISSION'S CREATION OF THIS DATABASE RUNS CONTRARY TO THE PURPOSES OF THE PRIVACY ACT AND COULD CAUSE SIGNIFICANT ONGOING HARM

A. The Commission's Conduct Runs Counter To The Privacy Act's Purpose Of Ensuring That Personal Data Handled By The Federal Government Receives Appropriate Protections

The Privacy Act expressly recognizes that the Government's ability to protect individual privacy is intertwined with its ability to provide security for personal information that it retains. The Privacy Act contains an extensive set of record-keeping requirements for covered records. Government agencies must maintain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency." 5 U.S.C. § 552a(e)(1). They must establish certain "rules of conduct" for personnel who have a role in administering records

³⁰ See United States Computer Emergency Readiness Team, "Securing Voter Registration Data" (last revised Sept. 30, 2016), available at <https://www.us-cert.gov/ncas/tips/ST16-001>.

³¹ See Dell Cameron, "Even a Novice Hacker Could Breach Network Hosting Kris Kobach's Bogus Voter Fraud Program," *Gizmodo.com* (Nov. 9, 2017), available at <https://gizmodo.com/even-a-novice-hacker-could-breach-the-network-hosting-k-1820263699>; Jessica Huseman & Derek Willis, "The Voter Fraud Commission Wants Your Data—But Experts Say They Can't Keep It Safe," *ProPublica* (Oct. 23, 2017), available at <https://www.propublica.org/article/crosscheck-the-voter-fraud-commission-wants-your-data-keep-it-safe>.

systems. *Id.* § 552a(e)(9). And, critically, agencies charged with handling covered records must establish “appropriate . . . safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.” *Id.* § 552a(e)(10).

When Congress enacted the statute in 1974, it was acutely aware that technological advances, including the ability to maintain large volumes of personal data on computer systems, posed new challenges for securing personal information retained by the Government. A study by the National Academy of Sciences that substantially informed the legislative process listed among the major priorities for public action the need to “increase[] work by the computer industry and professionals on security measures to make it possible for organizations to keep their promises of confidentiality.” S. Rep. No. 93-1183, at 6 (1974). Congress specifically sought to ensure “that certain computer hardware and software used to operate the information systems of government should provide features which will promote the necessary security of” those systems. *Id.* at 16. Although the Privacy Act does not mandate any specific set of technical standards, the Senate Committee Report explained that the term “adequate . . . standards” was meant to incorporate “safeguards which represent current state-of-the-art procedures at any given time.” *Id.* at 54; *see also id.* at 55 (noting that computer experts gave testimony about concerns such as “tapped transmissions” and that the National Academy of Sciences predicted that “the payoff in sensitive personal information to be obtained by . . . outsiders breaching system security is going to increase in the coming years”).

The facts in this case raise grave concerns that precisely mirror those considered by Congress in 1974. The Commission is aggregating a large-scale database that includes (or is

intended to include) voters' names, addresses, dates of birth, partial social security numbers, voting history, criminal records, and military status. *See supra* p. 5. That data is being ingested into a system designed by and accessible to Commission members as well as at least some White House personnel. *See* Herndon Declaration ¶¶ 3, 6. As already described, this aggregated information would be an extraordinarily valuable target for hackers—including hackers acting on behalf of foreign intelligence services as well as those operating for profit. Yet, apart from providing a months-old and generally vague declaration from another case describing how the database was *anticipated* to operate, the Government has provided no meaningful assurances about the measures that it is now using to secure this pool of data. *See* Herndon Declaration n.1 (noting that the declaration was originally filed on July 17, 2017 in a prior case).

Indeed, it is not even clear from the materials provided by the Government whether any specific person or entity is accountable for the security of the database. Mr. Herndon, who serves as the Director of White House Information Technology, stated that he was asked to “assist” in creating a mechanism to store this data on White House computer systems and that members of his technical staff would “assist” in the data collection process. Herndon Declaration ¶¶ 3, 6. Mr. Herndon also stated that White House network monitoring tools would log access to the database. *Id.* ¶ 6. Yet—in sharp contrast to the requirements of the Privacy Act—the Commission does not appear to have established any rules or procedures governing access to the database or any rules governing ongoing safeguards. *Cf., e.g., Doe v. Dep’t of Justice*, 660 F. Supp. 2d 31, 43 (D.D.C. 2009) (noting that the Department of Justice has “promulgated extensive regulations . . . that safeguard its Privacy Act-protected records”) (internal quotations omitted); Memorandum from Jonathan R. Cantor, “DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information”

(Apr. 27, 2017) (providing guidance with respect to the handling of PII in the Department of Homeland Security, including information security requirements and restrictions on disseminating such information outside the Department).³² The Commission's operations thus stand at odds with the Privacy Act's clear purpose of ensuring that federal databases containing records about individuals maintain certain minimum safeguards to protect the security of those records.

B. The Commission's Aggregation Of This Data Could Cause Ongoing Harms That Would Be Difficult To Remedy

Due to the nature of data breaches, the Commission's aggregation of voter information could cause ongoing harms that would be difficult to remedy after they have occurred. Some states have already complied (or partially complied) with the Commission's requests, *see supra* p. 5, and others have indicated their intent to do so.³³ Whatever the extent of this compliance, the potential for harm can only increase so long as the database remains on White House systems and continues to grow. Voter data can become vulnerable to attack as soon as it is placed on White House systems. Once a network has been penetrated, hostile actors can begin exfiltrating data, often without the network administrator even becoming aware of the incident. In the case of the breach against OPM, for example, the intrusions were detected only after OPM installed new security systems, long after huge quantities of sensitive personal information had been stolen.³⁴ If the voter data at issue here is copied, it can never be fully erased or returned from the

³² Available at https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf

³³ See Associated Press, "How States Are Handling Trump's Voter Information Request," (Aug. 2, 2017) (cataloguing states' responses), available at <https://elections.ap.org/content/how-states-are-handling-trumps-voter-information-request>.

³⁴ See transcript, "OPM: Data Breach," Hrg. before the House Comm. on Oversight and Gov't Reform, at 42-43 (June 16, 2015), available at <https://www.gpo.gov/fdsys/pkg/CHRG-114hhrg99659/pdf/CHRG-114hhrg99659.pdf>.

possession of those who gain improper access to it. Moreover, if it is altered, that alteration could be difficult to detect and could cause widespread confusion for months or years to come.

CONCLUSION

The Court should deny the Government’s motion to dismiss. In the alternative, the Court should grant Plaintiffs’ request to conduct jurisdictional discovery.

Respectfully submitted,

/s/ _____
JOSHUA A. GELTZER (D.C. Bar No. 1018768)
INSTITUTE FOR CONSTITUTIONAL
ADVOCACY AND PROTECTION
Georgetown University Law Center
600 New Jersey Ave., N.W.
Washington, D.C. 20001
Telephone: 202.661.6728
JG1861@Georgetown.edu

ROBERT S. LITT*
DAVID A. NEWMAN*
SOPHIA M. BRILL*
MORRISON & FOERSTER LLP
2000 Pennsylvania Ave., N.W.
Washington, D.C. 20006

ROBERT TAJ MOORE*
MORRISON & FOERSTER LLP
250 West 55th Street
New York, N.Y. 10019

Counsel for Amici Curiae

* *pro hac vice* motions pending

APPENDIX: LIST OF AMICI CURIAE

1. James R. Clapper served as the U.S. Director of National Intelligence (DNI) from 2010 to January 20, 2017. Prior to becoming the DNI, he served for over three years in two administrations as the Under Secretary of Defense for Intelligence, where he was dual-hatted as the Director of Defense Intelligence for the DNI and as the Director of the National Geospatial-Intelligence Agency from 2001 to 2006.

2. Dipayan Ghosh served as Senior Advisor on Technology Policy at the Office of Science and Technology Policy and National Economic Council in the White House from 2013 to 2015, and until recently served as a privacy and public policy advisor at Facebook.

3. Andrew J. Grotto served as the Senior Director for Cybersecurity Policy at the White House from 2016 to 2017. He previously served as Senior Advisor for Technology Policy at the Department of Commerce.

4. Nancy Libin served as Chief Privacy Officer at the U.S. Department of Justice from 2009 to 2012.

5. Alex Macgillivray was Deputy United States Chief Technology Officer from 2014 to 2017. He previously served as General Counsel at Twitter and Deputy General Counsel at Google.

6. Matthew G. Olsen served as Director of the National Counterterrorism Center from 2011 to 2014. He previously served as the General Counsel for the National Security Agency and in various national security-related roles at the Department of Justice.

7. Christopher Painter served as the Coordinator for Cyber Issues at the Department of State from 2011 to 2017.

8. Paul Rosenzweig is a Senior Fellow at the R Street Institute. He teaches Cybersecurity Law and Policy at George Washington University School of Law. He served as Deputy Assistant Secretary for Policy at the Department of Homeland Security from 2006 to 2009.

9. Suzanne Spaulding served from 2011 to 2017 as the Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security, which is charged with strengthening cybersecurity and protecting the nation's critical infrastructure.

CERTIFICATE OF SERVICE

I hereby certify that on December 5, 2017, I filed this Motion with the United States District Court for the District of Columbia using the CM/ECF system, which will cause it to be served on all counsel of record.

Dated: December 5, 2017

Respectfully submitted,

/S/

JOSHUA A. GELTZER (D.C. Bar No. 1018768)
INSTITUTE FOR CONSTITUTIONAL
ADVOCACY AND PROTECTION
Georgetown University Law Center
600 New Jersey Ave. NW
Washington D.C. 20001
Telephone: 202.661.6728
JG1861@Georgetown.edu

EXHIBIT K

subsidiary's liabilities under applicable accounting standards. The Federal Reserve used information collected on the Capital and Asset Report for Foreign Banking Organizations (FR Y-7Q), the FR Y-9C and the FR XX-1 to calculate liabilities of these institutions.

The Board granted a request from one financial company to use an accounting standard or method of estimation other than GAAP to calculate liabilities. The requesting company is an insurance company that reports financial information under Statutory Accounting Principles ("SAP"). The Board approved a method of estimation for this company that is based on line items from SAP reports, with adjustments to reflect certain differences in accounting treatment between GAAP and SAP.

By order of the Board of Governors of the Federal Reserve System, acting through the Director of Supervision and Regulation under delegated authority, June 28, 2017.

Ann E. Misback,
Secretary of the Board.

[FR Doc. 2017-14011 Filed 7-3-17; 8:45 am]

BILLING CODE 6210-01-P

GENERAL SERVICES ADMINISTRATION

[Notice-MK-2017-01; Docket No. 2017-0002; Sequence 11]

The Presidential Commission on Election Integrity (PCEI); Upcoming Public Advisory Meeting

AGENCY: Office of Government-wide Policy (OGP), General Services Administration (GSA).

ACTION: Meeting notice.

SUMMARY: The Presidential Advisory Commission on Election Integrity (Commission), a Federal Advisory Committee established in accordance with the Federal Advisory Committee Act (FACA), 5 U.S.C. App., and Executive Order 13799, (<https://www.federalregister.gov/documents/2017/05/16/2017-10003/establishment-of-presidential-advisory-commission-on-election-integrity>) will hold its first meeting on Wednesday, July 19, 2017. This meeting will consist of a ceremonial swearing in of Commission members, introductions and statements from members, a discussion of the Commission's charge and objectives, possible comments or presentations from invited experts, and a discussion of next steps and related matters.

DATES: *Meeting Date:* The first Commission meeting will be held on Wednesday, July 19, 2017, from 11:00

a.m., Eastern Daylight Time (EDT) until no later than 5:00 p.m., EDT.

ADDRESSES: The meeting will be held at the Eisenhower Executive Office Building, Room 350, located at 1650 Pennsylvania Avenue NW., Washington, DC 20502. It will be open to the public through livestreaming on <https://www.whitehouse.gov/live>.

FOR FURTHER INFORMATION CONTACT: To obtain information about the Commission or to submit written comments for the Commission's consideration, contact the Commission's Designated Federal Officer, Andrew Kossack, via email at ElectionIntegrityStaff@ovp.eop.gov or telephone at 202-456-3794. Please note the Commission may post written comments publicly, including names and contact information, in accordance with the provisions of FACA. There will not be oral comments from the public at this initial meeting.

The Commission will provide individuals interested in providing oral comments the opportunity to do so at subsequent meetings. Requests to accommodate disabilities with respect to livestreaming or otherwise should also be sent to the email address listed above, preferably at least 10 days prior to the meeting to allow time for processing.

SUPPLEMENTARY INFORMATION: The Commission was established in accordance with E.O. 13799 of March 11, 2017, the Commission's charter, and the provisions of FACA. The Commission will, consistent with applicable law and E.O. 13799, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President of the United States 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 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.

Dated: June 30, 2017.

Jeffrey A. Koses,

Director, Office of Acquisition Policy, Office of Government-wide Policy.

[FR Doc. 2017-14210 Filed 7-3-17; 8:45 am]

BILLING CODE 6820-61-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Centers for Disease Control and Prevention

[30Day-17-1146]

Agency Forms Undergoing Paperwork Reduction Act Review

The Centers for Disease Control and Prevention (CDC) has submitted the following information collection request to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act of 1995. The notice for the proposed information collection is published to obtain comments from the public and affected agencies.

Written comments and suggestions from the public and affected agencies concerning the proposed collection of information are encouraged. Your comments should address any of the following: (a) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility; (b) Evaluate the accuracy of the agencies estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (c) Enhance the quality, utility, and clarity of the information to be collected; (d) Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses; and (e) Assess information collection costs.

To request additional information on the proposed project or to obtain a copy of the information collection plan and instruments, call (404) 639-7570 or send an email to omb@cdc.gov. Written comments and/or suggestions regarding the items contained in this notice should be directed to the Attention: CDC Desk Officer, Office of Management and Budget, Washington, DC 20503 or by fax to (202) 395-5806. Written comments should be received within 30 days of this notice.