IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civ. Action No. 17-1320 (CKK)

PLAINTIFF'S AMENDED MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

Pursuant to the Court's July 11, 2017, Order and to Federal Rule of Civil Procedure 65 and LCvR 65.1, EPIC hereby moves this Court for a Temporary Restraining Order and Preliminary Injunction prohibiting Defendants from collecting voter roll data from state election officials prior to the completion and public release of a Privacy Impact Assessment as required by the E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), and prior to the publication of a Federal Advisory Committee Act notice concerning the Privacy Impact Assessment, and prior to the resolution of EPIC's constitutional privacy claims.

The proposed collection and aggregation of state voter roll data by the Commission is without precedent. The Commission's pending action would place at risk the privacy of millions of registered voters—including military families and victims of stalking, whose home addresses would be revealed—and would undermine the integrity of the federal election system. Further, the request for partial Social Security Numbers that are often used as default passwords for commercial services, coupled with the Commission's plan to make voter records "publicly available," is both without precedent and crazy. The new facts that have come to light since

EPIC's original motion – including, (1) upon the Commission's instigation, the disclosure of Arkansas state voter records, contrary to state law and to a website not certified for personal information; (2) widespread concerns about the risks of the Commission's endeavor; and (3) the Commission stated intent to press on, pending this Court's decision -- underscore the need for injunctive relief.

This motion is supported by the attached Memorandum of Points and Authorities and exhibits, as well as the declarations and exhibits previously submitted,[1] and any additional submissions that may be considered by the Court.

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC
** Pro hac vice motion pending*

Dated: July 13, 2017

[1] For the Court's convenience, attached to this motion are copies of all declarations and exhibits previously filed by EPIC in its motion, reply, and supplemental response.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civ. Action No. 17-1320 (CKK)

MEMORANDUM IN SUPPORT OF PLAINTIFF'S AMENDED MOTION FOR A TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

In the original emergency motion to this Court, EPIC explained that "the failure to safeguard personal data gathered by government agencies is a national crisis." EPIC pointed to the massive data breach at the Office of Personnel Management in 2015, and warned that the Commission's effort to gather state voter records, without regard for privacy, placed at risk the rights of millions of voters across this country. We respectfully asked this Court to issue a Temporary Restraining Order to enjoin the Commission from collecting state voter data.

Since EPIC filed the motion, there has been a substantial change in the factual record. The Commission went forward with its plan. It did not complete or publish a Privacy Impact Assessment. It did not publish a Federal Advisory Committee Act notice. It did not consider whether the extraordinary and unreasonable request for personal data without adequate privacy protection violated the constitutional right to privacy. It did not establish a method to securely receive personal data. It did not make any effort to work with the agency, the General Services Administration, designated in the Executive Order and the Commission Charter to provide "facilities," "equipment," and "administrative support" for the Commission. And it ignored calls from state election officials, experts in election system security, and twenty-four members of the United States Senate to end the program.

Further, upon the Commission's instigation, the State Secretary of Arkansas, over the objection of the Governor, turned over the state voter data to the Commission in violation of state law. No designation of appropriate data elements was made. No fees were received by the state. The state procedures for transferring state voter data were not followed. The Arkansas "Data Request Form" was never completed. The data was sent to a military website, designated by the Commission, that was not authorized to receive personal data from the general public.

Once these facts came to light, and upon the initiation of this litigation, the Commission did an about face. First, the Commission notified the states that it would suspend the data collection pending the Court's decision on this motion. Second, the Commission discontinued the

use of the military website to receive voter data. Third, the Commission stated it would delete the data that had been received from the state of Arkansas.

These are the events that have occurred since the filing of EPIC's initial complaint on July 3, 2017.

But the threat to voter privacy and democratic institutions remains. The Commission intends to move forward, pending this Court's determination. It has established a new server within the White House to receive the voter data. It has advised state election officials that further communications regarding this undertaking are forthcoming. But the Commission has given no indication that it will undertake a Privacy Impact Assessment, publish a FACA notice, or consider the Constitutional implications of this extraordinary request for personal data by the federal government. And the actual experience with the State of Arkansas makes clear that other states, by intent or inadvertence, may disclose to the Commission personal voter data, otherwise protected in law.

EPIC therefore respectfully renews its request for an injunction that would prohibit the Commission from collecting state voter record data pending resolution of this case. The requirements for an injunction are satisfied: (1) EPIC is likely to succeed on the merits of its claim; (2) EPIC and its members will be irreparably harmed; and (3) the balance of the equities and the public interest favors EPIC.

FACTUAL BACKGROUND

I. The Privacy Threat of Massive Voter Databases

Computer experts have long raised concerns about the collection of sensitive voter information in insecure databases. *E.g.*, Barbara Simons, *Voter Registration and Privacy* (2005);[1] EPIC, Comment Letter on U.S. Election Assistance Commission Proposed Information Collection Activity (Feb. 25, 2005).[2] Election officials "face many technical challenges in implementing [voter registration] databases in a secure, accurate, and reliable manner, while protecting sensitive

[1] https://epic.org/events/id/resources/simons.ppt.
[2] https://epic.org/privacy/voting/register/eac_comments_022505.html.

information and minimizing the risk of identity theft." Simons, *supra*, at 10. Voter registration databases "are complex systems," and "[i]t is likely that one or more aspects of the technology will fail at some point." Ass'n for Comput. Machinery, *Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues* 6 (Feb. 2006), Ex. 26.[3] Moreover, merging data from multiple sources "can, if not properly handled, undermine the accuracy of the voter registration data." Simons, *supra*, at 12.

Recent events underscore the privacy risks inherent in assembling a nationwide voter database. In a recent hearing before the Senate Intelligence Committee, both federal and state election officials made clear that malicious hackers attack voter registration databases. *See Russian Interference in the 2016 U.S. Elections: Hearing Before the S. Select Comm. on Intelligence* (2017) (testimony of Jeanette Manfra, Acting Deputy Undersecretary for Cybersecurity & Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security) [hereinafter *SSCI 2016 Elections Hearing*], Ex. 27; *SSCI 2016 Elections Hearing* (testimony of Michael Haas, Administrator, Wisconsin Elections Commission), Ex. 28; *SSCI 2016 Elections Hearing* (statement of Hon. Connie Lawson, Secretary of State, Indiana), Ex. 29; *SSCI 2016 Elections Hearing* (statement of Steve Sandvoss, Executive Director, Illinois State Board of Elections), Ex. 30.

State officials recognize "the need for constantly enhancing the security of voter registration databases," especially due to the "confidential" nature of data held that can include "the voter's date of birth, the driver's license number, the last four digits of the social security number." *SSCI 2016 Elections Hearing* (transcript of panel 2), Ex. 32, at 4. The threats to state voter data are acute, and state officials have taken steps to keep that data secure within their own databases. For example, following the malicious cyber attack on the Illinois Voter Registration System database last year, the state began "introducing security enhancements" to their "web servers and databases." Ex. 30, at 1.

[3] https://people.eecs.berkeley.edu/~daw/papers/vrd-acm06.pdf.

States are well aware that "the 2016 elections reinforced the need for constantly enhancing the security of voter registration databases." Ex. 28, at 4. Already representatives from 27 states have joined an "Election Cybersecurity Task Force" within the National Association of Secretaries of State ("NASS") in order to "combat threats" and fostering "technical forums for those who are directly responsible for protecting digital election processes and systems." Ex. 29, at 7–8. The states are continuing "to increase protection for their own systems." Ex. 29, at 9. But election systems face unique threats that require special expertise and protective measures, which make them "fundamentally different from any other sector or subsector of critical infrastructure." Ex. 29, at 6.

The Commission's plan to aggregate all state voter roll data into a single database would do nothing to mitigate these threats and, in fact, it would only introduce new vulnerabilities. Indeed, the Georgia state Director of Elections said, in response to the Commission's June 28, 2017, letter that the Commission's instructions were not consistent with state "security protocol." Letter from Chris Harvey, Director of Elections, Georgia Secretary of State's Office, to Kris W. Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity (July 3, 2017), Ex. 20.

II. The Establishment of the Commission

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017. Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017), Ex. 1. The Vice President is named as the Chair of the Commission, "which shall be composed [sic] of not more than 15 additional members." *Id*. Additional members are appointed by the President, and the Vice President may select a Vice Chair of the Commission from among the members. *Id*. Vice President Pence has named Kansas Secretary of State Kris Kobach to serve as Vice Chair of the Commission.

The Commission was asked to "*study* the registration and voting processes used in Federal elections." *Id.* (emphasis added). The Commission was further asked to identify "(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." *Id*.

There is no authority in the Executive Order to subpoena records, to undertake investigations, or to demand the production of state voter records from state election officials.

III. The Role of the General Services Administration

The Executive Order provides that the 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 on a reimbursable basis." 82 Fed. Reg. at 22,390, Ex. 1, at 2. The Commission Charter designates the GSA as the "Agency Responsible for Providing Support," and similarly orders that the 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 on a reimbursable basis." Charter, Presidential Advisory Commission on Election Integrity ¶ 6, First Kobach Decl., Ex. 2.

The GSA routinely conducts and publishes Privacy Impact Assessments when it collects, maintains, and uses personal information on individuals. Gen. Serv. Admin., *Privacy Impact Assessments* (Apr. 13, 2017), Ex. 18. There is no authority in the Executive Order of the Commission Charter for any other entity to provide "administrative services," "facilities," or "equipment" to "carry out [the Commission's] mission."

IV. The Role of Other Government Agencies and Officials

The Commission revealed for the first time in its supplemental brief that the Director of White House Information Technology is now in charge of "repurposing an existing system" within the "White House Information Technology enterprise." Def.'s Supp. Br. 2, ECF No. 24.

Although the Commission did not provide the name of the current Director of White House Information Technology, EPIC was able to identify that individual as Mr. Charles C. Herndon, and name him as a codefendant in the Second Amended Complaint. Second Am. Compl. ¶ 10, ECF No. 33.

The "information resources and information systems" in the Executive Office of the President, which the Director has primary authority to oversee, include the resources of the U.S. Digital Service, which is housed within the Office of Management and Budget. U.S. Digital Serv., *Report to Congress — December 2016* at 4 (2016), Ex. 36. The U.S. Digital Service is responsible for "improving performance and cost-effectiveness of important government digital services." *Id.* The Director of White House Information Technology, the Executive Committee for Presidential Information Technology, and the U.S. Digital Service are all components within the EOP and thus subject to both the APA and the E-Government Act.

In addition, one of the Commission members, Christy McCormick is also a member of the Election Assistance Commission ("EAC"). Kobach Second Decl. 2, ECF No. 11-1. The EAC is an agency under the APA and is subject to the E-Government Act.

V. The Commission's Demand for State Voter Records

On June 28, 2017, the Commission undertook an unprecedented effort to collect detailed voter records from all fifty states and the District of Columbia. For example, the Commission sent a letter to North Carolina Secretary of State Elaine Marshall. Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), Ex. 3 ("Commission Letter"). In the letter, Kobach asked Marshall to provide to the Commission

> 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. at 1–2.

The fact that the Commission demanded State election officials to turn over sensitive personal information that raises many privacy concerns. For example, the improper collection and use of Social Security Numbers ("SSNs") is a major contributor to identity theft in the United States. Soc. Sec. Admin., *Identity Theft and Your Social Security Number* (Feb. 2016).[4] "An estimated 17.6 million Americans—about 7% of U.S. residents age 16 or older—were victims of identity theft in 2014." Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* at 1 (Sept. 2015).[5] U.S. victims of identity theft lost a collective total of $15.4 billion in the same year. *Id.* at 7.

Collecting and publishing the home addresses of current and former military personnel also poses privacy and security risks. The U.S. Military routinely redacts "names, social security numbers, personal telephone numbers, home addresses and personal email addresses" of military personnel in published documents, "since release would constitute a clearly unwarranted invasion of their personal privacy." U.S. Pacific Fleet, *Report of the Court of Inquiry* (2001);[6] *see also* Def. Logistics Agency, *Defense Logistics Agency Instruction 6303* (2009)[7] (noting that military home addresses are "For Official Use Only" and must be redacted prior to public release of documents); Jason Molinet, *ISIS Hackers Call for Homegrown 'Jihad' Against U.S. Military, Posts Names and Addresses of 100 Service Members*, N.Y. Daily News (Mar. 21, 2015).[8]

[4] https://www.ssa.gov/pubs/EN-05-10064.pdf.
[5] https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[6] http://www.cpf.navy.mil/subsite/ehimemaru/legal/GREENEVILLE_FOIA_exemption.pdf.
[7] http://www.dla.mil/Portals/104/Documents/J5StrategicPlansPolicy/PublicIssuances/i6303.pdf.
[8] http://www.nydailynews.com/news/national/isis-hackers-call-jihad-u-s-military-article-1.2157749.

In the Commission Letter, the Kobach warned that "any documents that are submitted to the full Commission w[ould] also be made available to the public." Commission Letter 2. Kobach later stated that "the Commission intends to de-identify any such data prior to public release of the documents." First Kobach Decl. ¶ 5. However, the Commission has given "no identification or description of the process or technique, no explanation of what the Commission hopes to protect and how they can ensure they have done so, and no description of the reason for publishing anything." Decl. of Cynthia Dwork ¶ 7, Ex. 23. There is an "inherent contradiction" in the Commission's simultaneous statements that there is no privacy interest in the voter data and that the Commission will take steps to protect the privacy of the data.

Kobach stated that he expected a response from the states by July 14, 2017—approximately ten business days after the date of the request—and instructed that the State Secretary could submit her responses "electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange" system. *Id*. Neither the email address nor the file exchange system proposed by the Commission provides a secure mechanism for transferring sensitive personal information. In fact, an attempt to access the File Exchange system linked in the letter leads to a warning screen with a notification that the site is insecure. *See* Second Decl. of Harry R. Lewis, Ex. 17; Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Site (July 3, 2017 12:02 AM), Ex. 6.

Similar letters were sent to election officials in the other 49 states and the District of Columbia. First Kobach Decl. ¶ 4.

VI. Relationship Between the Commission's Request and the Vice Chair's Interstate Voter Registration Crosscheck Program

The Commission's request for state voter records also raises significant privacy concerns because of the Vice Chair's previous attempts to collect and match state voter records, an activity that if undertaken by a federal agency, would trigger numerous requirements under the federal Privacy Act. 5 U.S.C. § 552a *et seq*. Beginning in 2011, the Vice Chair of the Commission, acting as the Secretary of State of Kansas, "made it one of [his] highest priorities to increase the number

of participating states" in the Interstate Voter Registration Crosscheck Program ("Crosscheck Program"). Sec'y of State, Kansas, *Interstate Crosscheck Program Grows* 2 (2013), Ex. 33. The "Crosscheck Program," which "began as an arrangement between Kansas, Iowa, Nebraska, and Missouri, involves the collection of voter information including 13 data elements—status, date generated, first name, middle name, last name, suffix name, date of birth, voter id number, last 4 digits of SSN, mailing address, county, date of registration, and voting history. Presentation by Kris W. Kobach to the National Ass'n of State Election Dirs., *Interstate Voter Registration Crosscheck Program* 8 (Jan. 26, 2013), Ex. 34. The voter data elements requested by Kobach in the Crosscheck program are nearly identical to the data elements demanded by Kobach in June 28, 2017, letter to the states.

The Vice Chair's attempt to gather voter data from 50 states and the District of Columbia appears to be an attempt to extend the Crosscheck program under federal authority but outside law. One indication of the intent to run Crosscheck from the Commission is that the FTP site for the Crosscheck program is "hosted by Arkansas," Ex. 34, at 11, and Arkansas was the first state to submit voter data to the Commission in response to Kobach's June 28, 2017, demand. TRO Hr'g Tr. 41, July 7, 2017.

Reviews of the Crosscheck system have shown that it generates false positives and can lead to improper removal of voters from the active rolls. A 2016 investigation conducted by Rolling Stone, including a review of Crosscheck lists from Virginia, Georgia, and Washington, showed more than "1 million matches – and Crosscheck's results seemed at best deeply flawed." Greg Palast, *The GOP's Stealth War Against Voters*, Rolling Stone (Aug. 24, 2016), Ex. 35. A grid based on the 2012 Crosscheck data, provided in Kobach's 2013 presentation to the National Association of State Election Directors, shows more than 1 million "potential duplicate voters" in 15 states. Ex. 34, at 10. A database expert who reviewed the data from three states as part of the Rolling Stone investigation said that "he was shocked by Crosscheck's 'childish methodology'" which "spews out little more than a bunch of common names." Ex. 35. Oregon abandoned the

Crosscheck program after 2014 because, as the secretary of state explained, "the data we received was unreliable." Ex. 35.

VII. Developments Since the Commission Sent Its June 28, 2017, Letter to the States

There have been several significant developments since Kobach sent the June 28th letter demanding that all states transfer personal voter data to the Commission by July 14, 2017. First, in response to EPIC's Emergency Motion, Kobach stated that, "as of July 5, 2017, no Secretary of State had yet provided to the Commission any of the information requested in [his] letter." First Kobach Decl. ¶ 6. Then counsel for Defendants subsequently revealed at the July 7, 2017, hearing that Arkansas had submitted data via the Department of Defense file exchange system. TRO Hr'g Tr. 41, July 7, 2017. Counsel for the Defendants was unable to provide the Court with any details concerning where the voter data would be stored, whether it would be secured, and what government entities would be involved in the collection and storage of the data. Hr'g Tr. 33–36.

Prior to the hearing, EPIC located and submitted to the Court a copy of the Privacy Impact Assessment that the Army had conducted and published for the file exchange system. *See* Ex. 22. According to the Department of Defense PIA, the file exchange system was not authorized to be used to "collect, maintain, use, and/or disseminate" personally identifiable information from "members of the general public." Ex. 22, at 1. After EPIC filed an amended complaint adding the Department of Defense as a codefendant, the Defendants announced in a supplemental brief that the Commission intended to "use alternative means for transmitting the requested data." Def.'s Supp. Br. 1, ECF No. 24. The Defendants stated that "[t]he Commission will not download the data that Arkansas already transmitted" to the file exchange system and that the "data will be deleted from the site." *Id*. The Defendants have not confirmed that the data has, in fact, been deleted.

The Defendants also revealed for the first time in their supplemental brief that the "Director of White House Information Technology is repurposing an existing system" to be used for the collection of personal voter data that the Commission demanded from the states. *Id*. The

Defendants claimed that "[t]he system is anticipated to be fully functional by 6:00 pm EDT [on July 10, 2017]." *Id*. The Commission did not provide any indication it would complete a Privacy Impact Assessment prior to a subsequent request for data from the states. The Commission did not provide any indication it would publish the Privacy Impact Assessment pursuant to the FACA. The Commission did not explain how it could delegate White House personnel to manage the facilities for the Commission when both the Executive Order and the Commission Charter make clear that the General Services Administration ("GSA") is the "agency responsible" for this function.

VIII. The States Have Opposed the Commission's Request

As of July 6, 2017, only one state in the country had complied with the Commission's request. The vast majority of states have refused to turn over the voter data the Commission is seeking. *Forty-four states and DC have refused to give certain voter information to Trump commission,* CNN (July 5, 2017).[9] California Secretary of State Alex Padilla stated on June 29, 2017, that "[t]he President's commission has requested the personal data and the voting history of every American voter–including Californians. As Secretary of State, it is my duty to ensure the integrity of our elections and to protect the voting rights and privacy of our state's voters." Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017).[10] Nebraska Secretary of State John Gale stated on July 6, 2017 that "I also have a concern about data privacy. I have no clear assurances about the security that this national database will receive. In light of the domestic and foreign attacks in 2016 on state voter registration databases, the commission will need to assure my office

[9] http://www.cnn.com/2017/07/03/politics/kris-kobach-letter-voter-fraud-commission-information/index.html.

[10] http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

of a high level of security." Press Release, Sec. Gale Issues Statement on Request for NE Voter Record Information (July 6, 2017).[11] Arizona Secretary of State Michele Reagan said:

> I share the concerns of many Arizona citizens that the Commission's request implicates serious privacy concerns. […] Since there is nothing in Executive Order 13799 (nor federal law) that gives the Commission authority to unilaterally acquire and disseminate such sensitive information, the Arizona Secretary of State's Office is not in a position to fulfill your request. […]
> Centralizing sensitive voter registration information from every U.S. state is a potential target for nefarious actors who may be intent on further undermining our electoral process. […] Without any explanation how Arizona's voter information would be safeguarded or what security protocols the Commission has put in place, I cannot in good conscience release Arizonans' sensitive voter data for this hastily organized experiment.

Letter from Michele Reagan, Arizona Sec. of State, to Kris Kobach (July 3, 2017).

IX. Defendants' Failure to Conduct a Privacy Impact Assessment

Under the E-Government Act of 2002, any 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. Pub. L. 107–347, 116 Stat. 2899, Title II § 208 (codified as amended at 44 U.S.C. § 3501 note). The agency must:

> (i) [C]onduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or 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. The Privacy Impact Assessment would require the agency to state:

> (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;

[11] http://www.sos.ne.gov/admin/press_releases/pdf-2017/nr-20170707.pdf.

> (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
> (VI) how the information will be secured; and
> (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the ''Privacy Act'').

Id. § 208 (b)(2)(B)(ii).

That assessment is particularly important here because the E-Government Act also requires the agency to "ensure that":

> a privacy impact assessment is 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; and

Id. § 208 (b)(2)(B)(ii).

It is certainly conceivable that a proper Privacy Impact Assessment would have led to the conclusion that the Commission simply could not request and collect state voter record information. Moreover, under the Federal Advisory Committee Act, the Defendants would have been required to make available the Privacy Impact Assessment to the Public. 5 U.S.C. app. 2 § 10(b).

But none of the Defendants have conducted a privacy impact assessment for the Commission's proposed collection of state voter data or the Director of White House Information Technology's development of a system to collect the data. None of the Defendants have ensured review of a PIA by any Chief Information Officer or equivalent official. The Commission has not made any PIA available to the public. Complaint ¶¶ 32–34.

STANDARD OF REVIEW

In order to obtain a temporary restraining order or preliminary injunction, a plaintiff must show that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm in the absence of preliminary relief, (3) that the balance of the equities tips in their favor, and (4) that an injunction is in the public interest. *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011) (quoting *Winter v. NRDC*, 555 U.S. 7, 20 (2008)). This Court has held that plaintiff's are entitled

to preliminary injunctive relief where, as here, they "have shown a clear likelihood of success on the merits and have satisfied the other requirements for a preliminary injunction." *Dimondstein v. American Postal Workers Union*, 964 F.Supp.2d 37, 41 (D.D.C. 2013). The D.C. Circuit has adopted a "sliding scale" approach when evaluating these injunction factors. *Sherley*, 644 F.3d at 392. Thus if the "movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make a strong showing on another factor." *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291–92 (D.C. Cir. 2009). *But see League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 7 (D.C. Cir. 2016) (noting that the court has "not yet decided" whether the sliding scale approach applies post-*Winter*). Preliminary injunctive relief is especially appropriate where, as here, it is necessary "to preserve the status quo and to prevent irreparable harm." *CAIR v. Gaubatz*, 667 F. Supp. 2d 67, 79 (D.D.C. 2010).

ARGUMENT

This case presents the type of extraordinary circumstance that justifies preliminary injunctive relief. Absent a prohibition from this Court, the Commission will begin collecting and aggregating the sensitive, personal information of voters across the country without establishing any procedures to protect voter privacy or the security and integrity of the state voter data. There is already evidence that the Commission has placed and will place voter data at risk.

First and foremost, this proposed collection violates a core provision of the E-Government Act of 2002, which requires that agencies establish sufficient protections *prior* to initiating any new collection of personal information using information technology. The Commission's actions also violate voters' Fifth Amendment right to informational privacy and, through their implementation, violate the Administrative Procedure Act (APA). Second, this collection and aggregation of sensitive personal information, as well as the exposure of this voter data through insecure systems, will cause irreparable harm to EPIC and its members. The Commission has demanded that states provide confidential voter information, the improper transfer of which is a *per se* harm. In addition, the collection and aggregation of this sensitive data will exacerbate the

already acute risks to voter data, and create a new target for malicious hackers. If this data were to be hacked, there would be no way to control its spread. Third, the balance of the equities favors relief because the Commission will suffer no hardship if the collection is enjoined pending resolution of the case; indeed the Commission has already conceded this point by halting collection pending resolution of EPIC's motion. Fourth, granting the injunction would be in the public interest. The Commission's mandate is to "study" election integrity. There is nothing in the Executive Order or the Commission's Charter that provides authority to gather hundreds of millions of voter records from the states or to create a secret database stored in the White House. The Commission's actions, apart from its stated role, far exceed a solely "advisory" function. As evidenced by the response of state officials of both political parties to the Commission's June 28, 2017 letter, the Commission's request has in fact undermined "the American's people's confidence in the integrity of the voting processes used in federal elections." Ex. 1. By the terms of the Commission's purpose and the actions undertaken by the Commission, the order EPIC seeks should be granted.

I. EPIC is likely to succeed on the merits of its claims.

A. Defendants Proposed Collection of State Voter Data Violates the E-Government Act and the APA

The Defendants have made no attempt to comply with the Privacy Impact Assessment requirements of Section 208 of the E-Government Act of 2002, Pub. L. 107-347, 115 Stat. 2899, Title II § 208 (codified at 44 U.S.C. § 3501 note), which are clearly applicable to the collection of sensitive, personal information from state voter databases. The Defendants' actions therefore violate the Administrative Procedures Act ("APA"), 5 U.S.C. § 706(2)(A). EPIC is likely to succeed on its statutory claims.

As the Department of Justice has explained, "Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing

information technology that manages information in identifiable form." Office of Privacy & Civil Liberties, U.S. Dep't of Justice, *E-Government Act of 2002* (June 18, 2014).[12] A Privacy Impact Assessment is "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." Joshua B. Bolten, Director, Office of Mgmt. & Budget, Executive Office of the President, M-03-22, Memorandum for Heads of Executive Departments and Agencies, Attachment A (Sept. 26, 2003) [hereinafter Bolten Memo], Ex. 5.

The E-Government Act requires that an agency "shall take actions described under subparagraph (B)" of Section 208 "before . . . 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, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government." E-Government Act § 208(b)(1)(A)(ii). The actions described in subparagraph (B), which the Commission must take *before* collecting this information, include "(i) conduct[ing] a privacy assessment; (ii) ensur[ing] the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), mak[ing] the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." E-Government Act § 208(b)(1)(B).

The Commission has already "initiated a new collection" of personal information, but it has not complied with any of these requirements. The APA prohibits federal agencies from taking

[12] https://www.justice.gov/opcl/e-government-act-2002.

any action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2). The Commission's actions are "not in accordance with law." The APA authorizes this Court to "compel agency action unlawfully withheld." 5 U.S.C. § 706(1). Such a claim may proceed "where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required to take.*" *Norton v. S. Utah Wildlife Alliance*, 542 U.S. 55, 64 (2004). An agency's failure to comply with the PIA requirements of the E-Government Act is reviewable under both provisions of APA § 706. *Fanin v. Dep't of Veteran Affairs*, 572 F.3d 868, 875 (11th Cir. 2009).

The E-Government Act defines "information technology" as "any equipment or interconnected system . . . used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly . . . ." 40 U.S.C. § 11101(6); *see* E-Government Act § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 US.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). Courts have found that a "minor change" to "a system or collection" that does not "create new privacy risks," such as the purchasing of a new external hard drive, would not require a PIA. *Perkins v. Dep't of Veteran Affairs*, No. 07-310, at *19 (N.D. Ala. Apr. 21, 2010) (quoting Bolten Memo § II.B.3.f). However, an agency is obligated to conduct a PIA before initiating a new collection of data that will be "collected, maintained, or disseminated using information technology" whenever that data "includes any information in identifiable form permitting the physical or online contacting of a specific individual" and so long as the questions have been posed to 10 or more persons. E-Government Act § 208(b)(1)(A)(ii). The term "identifiable form" means "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." E-Government Act § 208(d).

There is no question that the PIA requirement applies in this case. The Commission's decision to initiate collection of comprehensive voter data by requesting personal information

from Secretaries of State of all 50 states and the District of Columbia, including sensitive, personal information about hundreds of millions of voters, triggers the obligations of § 208(b)(1)(A)(ii). The letter sent by Commission Vice Chair Kobach requests that the Secretary of State provide "voter roll data" 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 information." Commission Letter 1–2. The states are instructed to submit their "responses *electronically* to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE")," a government website used to transfer files. *Id.* (emphasis added).[13] This sensitive voter roll data is precisely the type of "personal information" in "identifiable form" that the PIA provision was intended to protect, and the transfer of large data files via email or otherwise clearly involves the use of information technology.

As the court explained in *Perkins*, PIAs are necessary to address "(1) what information is collected and why, (2) the agency's intended use of the information, (3) with whom the information would be shared, (4) what opportunities the [individuals] would have to decline to provide information or to decline to share the information, (5) how the information would be secured, and (6) whether a system of records is being created." *Perkins v. Dep't of Veteran Affairs*, No. 07-310, at *19 (N.D. Ala. Apr. 21, 2010). *See* E-Government Act § 208(b)(2)(B); Bolten Memo § II.C.1.a. These types of inquiries are "certainly appropriate and required" when an agency "initially created" a new database system and "began collecting data." *Perkins*, No. 07-310, at *19–20.

[13] The government file exchange website is not actually "safe." In fact, any user who follows the link provided in the Commission Letter will see a warning that the site is insecure. Ex 6.

B. The Executive Office of the President, the Commission, and the Director of White House Information Technology are Agencies Subject to the Administrative Procedure Act and the E-Government Act

The Commission has claimed that it is not subject to either the APA or the E-Government Act, but these arguments are contrary to the plain text of the statutes and unsupported by case law or legislative history. *See* Mem. Op. 9-13. The Commission fits squarely within the broad statutory definition of an "agency" in both the APA and the E-Government Act. *See* 5 U.S.C. § 551(1); 44 U.S.C. § 3502. The Commission does not dispute that if the APA and E-Government Act apply, the failure to conduct a PIA violates federal law. EPIC has therefore established a clear likelihood of success on the merits, which justifies entry of a TRO or injunction.

1. The EOP and its subcomponents are agencies under the APA.

The Executive Office of the President ("EOP") and its constituent offices are "agenc[ies]" within the meaning of the Administrative Procedure Act ("APA"). Under the APA, "each authority of the Government of the United States" is an agency "whether or not it is within or subject to review by another agency[.]" 5 U.S.C. § 551(1). "[T]he APA inquiry into agency status is . . . focused on the functions of the entity, and flexible enough to encompass the 'myriad organizational arrangements for getting the business of government done.'" *Meyer v. Bush*, 981 F.2d 1288, 1304 (D.C. Cir. 1993) (quoting *Washington Research Proj., Inc. v. HEW,* 504 F.2d 238, 246 (D.C. Cir. 1974)). "The legislative history of the APA indicates that Congress wanted to avoid a formalistic definition of 'agency' that might exclude any authority within the executive branch that should appropriately be subject to the requirements of the APA." *Armstrong v. Bush*, 924 F.2d 282, 291 (D.C. Cir. 1991).

The EOP is emphatically an "authority of the government" for "getting the business of government done." 5 U.S.C. § 551(1); *Meyer*, 981 F.2d at 1304; *see Executive Office of the President*, The White House (2017)[14] ("The EOP has responsibility for tasks ranging from communicating the President's message to the American people to promoting our trade interests

[14] https://www.whitehouse.gov/administration/eop.

abroad."). The EOP consists of a dozen or more major subcomponents that oversee and carry out vital government functions, including the National Security Council (charged with "integrating all aspects of national security policy as it affects the United States"); the Office of Management and Budget (charged with "supervis[ing] and control[ling] the administration of the budget"); and the Office of the United States Trade Representative (an office headed by a "Cabinet-level official" who "acts as the chief representative of the United States in all General Agreement on Tariffs and Trade activities"). *The Executive Office of the President*, The United States Government Manual.[15] The EOP is clearly a "center of gravity in the exercise of administrative power" wielding "substantial independent authority," and thus an "agency" under § 551(1). *Dong v. Smithsonian Inst.*, 125 F.3d 877, 881–882 (D.C. Cir. 1997); *cf. Pub. Citizen v. Carlin*, 2 F. Supp. 2d 1, 9 (D.D.C. 1997), *rev'd on other grounds*, 184 F.3d 900 (D.C. Cir. 1999) ("The EOP's status as an agency is also evidenced by the authority it possesses to impose requirements on all of the EOP components in certain matters.").

The EOP subcomponents named in EPIC's suit are likewise "agenc[ies]" under the APA. The Commission, which includes both the Vice President and a principal member of the Election Assistance Commission, is authorized to "study[] registration and voting processes" and to identify "which laws, rules, policies, activities, strategies, and practices that enhance or undermine Americans' confidence in the integrity of the federal election process." First Kobach Declaration 1, 3, ECF No. 8-1; Second Kobach Declaration 1, ECF 11-1. In practice, the Commission has gone well beyond its mandate to engage in substantive conduct that "affect[s] the rights" of individuals. *Dong*, 125 F.3d at 881 (quoting James O. Freedman, *Administrative Procedure and the Control of Foreign Direct Investment*, 119 U. Pa. L. Rev. 1, 9 (1970)).

Two weeks ago, the Commission undertook to assemble a database of personal voter information that directly implicates the privacy rights of least 157 million registered voters across

[15] https://www.usgovernmentmanual.gov/(S(zqmgxvxx0zutkos5uua3cyc4))/Agency.aspx?EntityId=p0fnvDxExmY=&ParentEId=+klubNxgV0o=&EType=jY3M4CTKVHY (last visited July 12, 2017).

50 states and the District of Columbia. Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), Ex. 3; U.S. Census Bureau, Voting and Registration in the Election of November 2016 at tbl. 4a (May 2017).[16] This sweeping depository of personal data would put the Internal Revenue Service—with its yearly haul of just 149 million individual returns—to shame. Internal Revenue Serv., *SOI Tax Stats - Tax Stats at a Glance* (2016).[17] "[A]ny authority within the executive branch" engaged in such far-reaching conduct is "appropriately subject to the requirements of the APA." *Armstrong*, 924 F.2d at 291; *cf. Meyer*, 981 F.2d at 1298 (Wald, J., dissenting) ("Congress contemplated that 'agency' would encompass entities, like the Task Force, which are created solely by executive order.").

Defendant Charles C. Herndon, Director of White House Information Technology ("the Director"), also oversees an "authority of the Government" that is a "center of gravity in the exercise of administrative power."[18] 5 U.S.C. § 551(1); *Dong*, 125 F.3d at 881; Def. Resp. to Pl. Mot. to Amend, ECF No. 32. The Director and his staff enjoy "primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP." Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology § 1, 2015 Daily Comp. Pres. Doc. 185 (Mar. 19, 2015), Ex. 25. This authority includes:

> [providing] policy coordination and guidance for, and periodically review[ing], all activities relating to the information resources and information systems provided to the President, Vice President, and EOP by the Community, including expenditures for, and procurement of, information resources and information systems by the Community. Such activities shall be subject to the Director's coordination, guidance, and review in order to ensure consistency with the Director's strategy and to strengthen the quality of the Community's decisions through integrated analysis, planning, budgeting, and evaluating process.

[16] https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html.
[17] https://www.irs.gov/uac/soi-tax-stats-tax-stats-at-a-glance.
[18] The White House Office ("WHO"), of which the Director is a part, also qualifies as an agency. The WHO is charged with the authority to "facilitate[] and maintain[] communication with the Congress, the heads of executive agencies, the press and other information media, and the general public." *The Executive Office of the President*, *supra*.

Id. § 2(c). The Director may also "advise and confer with appropriate executive departments and agencies, individuals, and other entities as necessary to perform the Director's duties . . . ." *Id.* § 2(d). These grants of authority and responsibility are quintessential features of an APA "agency."

Moreover, the actions of the EOP and its component offices have long been subject to APA review. *Pub. Citizen v. U.S. Trade Representative*, 5 F.3d 549, 551 (D.C. Cir. 1993) ("Public Citizen must rest its claim for judicial review [of U.S. Trade Representative's action] on the Administrative Procedure Act."); *Armstrong v. Bush*, 924 F.2d 282, 291 (D.C. Cir. 1991) ("[W]e find that there is APA review of the [National Security Council]'s recordkeeping guidelines and instructions . . . ."); *Armstrong v. Exec. Office of the President*, 810 F. Supp. 335, 338 (D.D.C. 1993) (citing *Armstrong*, 924 F.2d at 291–293) ("The Court of Appeals . . . approved of this Court's holding that the APA provides for limited review of the adequacy of the NSC's and EOP's recordkeeping guidelines and instructions pursuant to the FRA."); *Citizens for Responsibility & Ethics in Washington (CREW) v. Exec. Office of President*, 587 F. Supp. 2d 48, 57–58, 63 (D.D.C. 2008) (holding that the EOP was properly named as a defendant in an APA and Federal Records Act suit); *Pub. Citizen Health Research Grp. v. Comm'r, Food & Drug Admin.*, 724 F. Supp. 1013, 1023 (D.D.C. 1989) (reviewing OMB inaction under the APA). Indeed, the only part of the EOP that courts have categorically excluded from APA review is the President himself—an official who is not named in this suit. *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992).

The legislative history of the APA further confirms that the EOP and its subcomponents are "agenc[ies]" under the statute. The APA empowers a court to review the actions of a government authority unless there is a "showing of clear and convincing evidence of a legislative intent to restrict access to judicial review." *Citizens to Pres. Overton Park, Inc. v. Volpe*, 401 U.S. 402, 410 (1971) (quotation marks omitted), *abrogated on other grounds by Califano v. Sanders*, 430 U.S. 99 (1977). Yet the legislative history of the APA reveals no Congressional desire at all to shield the actions of the EOP and its subcomponents from judicial review. Quite the opposite.

As Congress has explained, the term "agency" under the APA is "defined substantially" as it was in the Federal Reports Act of 1942, Pub. L. No. 77-831, § 7(a), 56 Stat. 1078, 1079–80 (1942) (current version at 44 U.S.C. § 3502), and the Federal Register Act, Pub. L. No. 74-220, § 4, 49 Stat. 500, 501 (1935) (current version at 44 U.S.C. § 1501). Administrative Procedure Act, Legislative History, S. Doc. No. 248, at 12–13 (1946); *see also In re Fid. Mortg. Inv'rs*, 690 F.2d 35, 38 (2d Cir. 1982). The Federal Reports Act defined "agency" in exceptionally broad terms: "any executive department, commission, independent establishment, corporation owned or controlled by the United States, board, bureau, division, service, office, authority, or administration in the executive branch of the Government . . . ." § 7(a), 56 Stat. at 1079–80 (emphases added). The Federal Register Act's definition of "agency" even encompassed "the President of the United States," as well as "any executive department, independent board, establishment, bureau, agency, institution, commission, or separate office of the administrative branch of the Government of the United States[.]" § 4, 49 Stat. at 501 (emphases added). Because Congress has made clear that the meaning of "agency" under the APA is "substantially" coextensive with these earlier enumerated definitions, it follows that the EOP, the Commission, and the Director's office are all agencies themselves.

Notably, even if the Defendant subcomponents of EOP did not qualify as agencies themselves, the EOP would be answerable for their actions under the APA because it is a parent agency. *N. Slope Borough v. Andrus*, 642 F.2d 589, 605 (D.C. Cir. 1980) (ascribing actions by National Oceanic and Atmospheric Administration to parent agency Secretary of the Interior in an APA case); *Nat'l Wildlife Fed'n v. Burford*, 835 F.2d 305, 308 (D.C. Cir. 1987) (ascribing actions by Bureau of Land Management to parent agency Department of the Interior in an APA case); *Beverly Health & Rehab. Servs., Inc. v. Thompson*, 223 F. Supp. 2d 73, 75 (D.D.C. 2002); (ascribing actions by Health Care Financing Administration to parent agency Department of Health and Human Services in an APA case); *Indian River Cty. v. Rogoff*, 201 F. Supp. 3d 1, 19 (D.D.C. 2016) (ascribing actions by Federal Railroad Administration to parent agency Department of Transportation in an APA case).

And even if the Commission were solely an advisory committee—which, to be clear, it is not—the EOP would remain its parent agency for the purposes of both the APA and the FACA. *See* TRO Hr'g Tr. 29:14–17 (statement of Elizabeth J. Shapiro that Commission is located in "the Office of the Vice President, since the vice president is chair of the Committee"); *The Executive Office of the President*, *supra* (identifying the Office of the Vice President as a subcomponent of the EOP). The EOP would thus be subject to APA review for the Commission's unlawful nondisclosure of records under FACA. *Ctr. for Biological Diversity v. Tidwell*, No. CV 15-2176 (CKK), 2017 WL 943902, at *9 (D.D.C. Mar. 9, 2017) ("[T]he Court finds that Plaintiff has pleaded a viable claim under the APA for a violation of section 10(b), as the Complaint plausibly alleges that the [committee] was a FACA advisory committee, and that the [parent agency] failed to disclose the materials required by section 10(b).").

2. The Soucie 'sole function' exception does not apply to the APA's definition of 'agency.'

The "sole function" exception, which excuses a small circle of presidential advisors from the FOIA's "agency" disclosure requirements, simply does not apply to the APA's definition of "agency." This is apparent from the FOIA-specific origins of the "sole function" exception and the legislative history of the 1974 FOIA amendments.

The "sole function" exception derives from *Soucie v. David*, 448 F.2d 1067 (D.C. Cir. 1971), a case that highlighted potential conflicts between FOIA's presumption of openness and the President's power to assert executive privilege. In *Soucie*, the D.C. Circuit held that a subcomponent of the EOP, the Office of Science and Technology ("OST"), was an agency "subject to the public information provisions of the APA, i.e., the Freedom of Information Act."[19] *Id.* at 1073, 1075. But the court—wary of how an assertion of executive privilege might play out "in the context of a congressional command to disclose information"—added a narrow caveat in

[19] In the early years of the FOIA, the statute was sometimes characterized as a subpart of the APA. *E.g., Nat'l Parks & Conservation Ass'n v. Kleppe*, 547 F.2d 673, 678 n.16 (D.C. Cir. 1976) (citing Statement by the President Upon Signing Bill Revising Public Information Provisions of the Administrative Procedure Act, Weekly Comp. Pres. Doc. 895 (July 4, 1966)).

dicta: "If the OST's sole function were to advise and assist the President, that might be taken as an indication that the OST is part of the President's staff and not a separate agency." *Id.* at 1071 n.9, 1075 (emphasis added).

Whatever the force of this statement in a FOIA context, it certainly does not preclude APA review where, as here, the EOP is engaged in substantive conduct directly "affecting the rights and obligations of individuals. . . ." *Dong*, 125 F.3d at 881. Rather, the *Soucie* court was concerned about the EOP's nondisclosure of records under FOIA and the "[s]erious constitutional questions [that] would be presented by a claim of executive privilege as a defense to a suit under the Freedom of Information Act." *Soucie*, 448 F.2d at 1071. In other words: *Soucie* addressed the public availability of EOP records and the President's qualified privilege to withhold them, whereas APA review addresses the legality of substantive actions that the EOP takes. The two are distinct.

Congress sharpened this point when it passed the 1974 FOIA amendments, formally distinguishing the FOIA's definition of "agency" from that of the APA. *Compare* 5 U.S.C. § 551(a), *with* 5 U.S.C. § 552(f)(1). Though Congress broadened the textual definition of "agency" under the FOIA in several ways—e.g., making it explicit that the "Executive Office of the President" is subject to the statute—Congress also adopted the *Soucie* court's narrowing construction:

> With respect to the meaning of the term "Executive Office of the President" the conferees intend the result reached in *Soucie v. David* . . . . The term is not to be interpreted as including the President's immediate personal staff or units in the Executive Office whose sole function is to advise and assist the President.

H.R. Rep. No. 93-1380, at 232 (1974) (Conf. Rep.); *see also Kissinger v. Reporters Comm. for Freedom of the Press*, 445 U.S. 136, 156 (1980) (interpreting the House report to mean that the words "Executive Office" in the FOIA did "not include the Office of the President"). But in amending the FOIA, Congress left the definition of "agency" under the APA entirely untouched. It thus remains as broad as it ever was.

Courts have repeatedly declined to carve out a "sole function" exception in the APA's definition of "agency" when reviewing the conduct of EOP units. *Pub. Citizen*, 5 F.3d at 551 (applying APA to U.S. Trade Representative ("USTR") without invoking "sole function" test); *Armstrong*, 924 F.2d at 291 (applying APA to NSC without invoking "sole function" test); *CREW v. EOP*, 587 F. Supp. 2d at 57–58, 63 (applying APA to EOP without invoking "sole function" test); *Pub. Citizen Health Research Grp. v. Comm'r, Food & Drug Admin.*, 724 F. Supp. 1013, 1023 (D.D.C. 1989) (applying APA to OMB without invoking "sole function" test).

In *Alexander v. FBI*, 971 F. Supp. 603 (D.D.C. 1997), the court explained that statutes which "provide citizens with better access to government records" and statutes that "provide certain safeguards for an individual against an invasion of personal privacy" serve "very different purposes." *Id.* at 606. Exceptions that would apply to the definition of "agency" in the former case would thus not apply in the latter case:

> When passing FOIA, Congress was addressing the need for individuals to have access to government information. When passing the Privacy Act, Congress was addressing the need for individuals to have protection for their privacy concerns. In interpreting the word "agency" to exclude, under FOIA, the immediate staff of the President, the courts recognize, as Congress did, that the access provided by FOIA must be limited. However . . . there is no evidence that the privacy protections provided by Congress in the Privacy Act must also be necessarily limited. . . . Thus there is no need to ignore the plain language of the statute and limit the word "agency" as has been done under FOIA . . . .

Id.

This Court's holding in *Sculimbrene v. Reno*, 158 F. Supp. 2d 26 (D.D.C. 2001), is not to the contrary. First, *Sculimbrene* concerned a plaintiff "seeking access, under the Privacy Act, to records pertaining to himself"—effectively a FOIA request styled as a Privacy Act request. *Sculimbrene*, 158 F. Supp. 2d at 28. *Sculimbrene* did not concern substantive conduct that "inva[ded] personal privacy," such as the "improper maintenance of [private] files" at issue in *Alexander* or the unlawful collection of personal voter data at issue here. *Alexander*, 971 F. Supp. at 605. These "very different" circumstances warranted different interpretations of the term "agency." *Id.* at 606. Second, unlike the APA, the Privacy Act relies on precisely the same

statutory provision as the FOIA to define "agency." 5 U.S.C. § 552a(a)(1) (citing § 552(e)). By contrast, because the APA's definition of "agency" does not reference the FOIA's definition, the APA cannot be said to have incorporated any of FOIA's implicit limitations on that term.

If Congress intended for the APA and FOIA definitions of "agency" to be coextensive, it has had ample opportunity to amend the APA since the 1974 FOIA amendments were enacted. It has not done so. There is no basis in statute, legislative history, or case law to apply the "sole function" exception to the APA's definition of "agency."

3. Even if the 'sole function' exception applied, the EOP and its subcomponents would be agencies under the APA.

The EOP, the Commission, and the Director's office do far more than just "advise and assist the President." Soucie, 448 F.2d at 1075. Thus even if the "sole function" exception applied to the APA, these entities would still be agencies.

The EOP, as noted, carries out a wide array of functions that extend well beyond the immediate needs of the President. *See supra* Part I.B.1. The EOP consists of numerous subcomponents that oversee and carry out vital government functions, many of which—including the NSC, the OMB, and the USTR—have been deemed agencies under the APA in their own right. *See id*. Moreover, the EOP is expressly named as an agency by the FOIA definition from which the "sole function" exception arises. 5 U.S.C. § 552(e). It cannot be seriously contended that the EOP eludes the APA's definition of "agency."

The same is true of the Director's office. As noted, the Director and his staff enjoy "primary authority to establish and coordinate the necessary policies and procedures for operating and maintaining the information resources and information systems provided to the President, Vice President, and EOP." Memorandum on Establishing the Director of White House Information Technology and the Executive Committee for Presidential Information Technology § 1, 2015 Daily Comp. Pres. Doc. 185 (Mar. 19, 2015), Ex. 25. An entity that has primary authority to set policy and procedures for an agency is doing far more than just assisting the President. The Director's authority even extends beyond the EOP. The Director is required to "provide policy

coordination and guidance for, and periodically review, all activities relating to the information resources and information systems provided to" both the EOP and the Presidential Information Technology Community ("the Community"), including "expenditures for, and procurement of, information resources and information systems by the Community." *Id.* § 2(c). The Community, in turn, consists of multiple high-level officials: "the Assistant to the President for Management and Administration; the Executive Secretary of the National Security Council; the Director of the Office of Administration; the Director of the United States Secret Service; and the Director of the White House Military Office." *Id.* Notably, the Director of the Secret Service is a Department of Homeland Security official. *Overview*, United States Secret Service.[20] Given the broad, interagency reach of the Director's oversight authority, the "sole function" exception is likewise inapplicable to his office.

Finally, the Commission's functions also extend well beyond "advis[ing] and assist[ing]" the President. Here, as in *Energy Research Foundation v. Def. Nuclear Facilities Safety Bd.*, the Commission satisfies the definition of "agency" because it (1) investigates, (2) evaluates, and (3) makes recommendations. 917 F.2d 581, 585 (D.C. Cir. 1990) (citing *Soucie*, 448 F.2d at 1075) ("The Board of course performs precisely these functions. It investigates, evaluates and recommends[.]"); *see* Kobach Decl. 1, 3 (Commission is charged with "studying registration and voting processes"); Kobach Decl. 1 (Commission's report is to identify "which laws, rules, policies, activities, strategies, and practices that enhance or undermine Americans' confidence in the integrity of the federal election process"). Of course the Commission does a great deal more than that, too. It has announced plans to collect, store, and publish the personal data of every registered voter in the country, thereby implicating every voter's individual privacy rights. Kobach Letter 1–2, Ex. 3. The Commission cannot credibly characterize this behavior as incidental to its advisory role: it is acting with the force and effect of an agency. "the record evidence regarding [the Commission]'s actual functions" proves it to be so. *Citizens for*

[20] https://www.secretservice.gov/about/overview/ (last visited June 13, 2017).

Responsibility & Ethics in Washington (CREW) v. Office of Admin., 559 F. Supp. 2d 9, 26 (D.D.C. 2008), *aff'd*, 566 F.3d 219.

Thus the "sole function" exception, even if applicable to the APA, poses no bar to judicial review of Defendants' actions.

4. The EOP and its subcomponents are 'agencies' under the E-Government Act.

Because the Commission is an "agency" under the APA, it necessarily meets the definition under the E-Government Act as well. 44 U.S.C. § 3502(1). As the Commission itself concedes, the definition of "agency" used in the FOIA is textually broader than that of the APA, Def. Opp'n 10, and the definition of "agency" in the E-Government Act is effectively the same as that of the FOIA. § 3502(1); Def. Opp'n 11. Thus, the E-Government Act's PIA requirement applies with full force to the Commission, just as it would to any other similar Commission. For example, prior to collecting personal data by the Commission on Presidential Scholars ("a group of eminent private citizens appointed by the President to select and honor the Presidential Scholars"), a Privacy Impact Assessment was conducted and Privacy Act notices were issued. U.S. Dep't of Education, U.S. Presidential Scholars Privacy Policy and Impact Assessment (2017).[21]

The FOIA "sole function" exception is also inapplicable here. Although the textual definition of "agency" is essentially the same in the FOIA and the E-Government Act, neither Congress nor any court has said that parts of the EOP should be excused from the plain terms of the E-Government Act. That stands in marked contrast to the FOIA, where Congress and the Supreme Court have accorded a special contextual meaning to the otherwise unambiguous phrase "including the Executive Office of the President." *See supra* Part I.B.2; *Energy Research Found.*, 917 F.2d at 583 ("It is of course possible that identical phrases may carry different meanings in different statutes."). Absent any binding authority to the contrary, the plain text of the E-Government Act controls in this case. *Honeycutt v. United States*, 137 S. Ct. 1626, 1635 n.2

[21] https://www2.ed.gov/programs/psp/applications/privacy.pdf.

(2017) (emphasizing that courts "cannot construe a statute in a way that negates its plain text"). That text leaves no doubt: the Executive Office of the President, without exception, is subject to the E-Government Act. § 3502(1).

5. The General Services Administration, which is unquestionably an agency under the APA, is obligated to provide the data storage used by the Commission.

None of the above analysis would be necessary if the General Services Administration ("GSA") had provided equipment and facilities for the Commission's proposed storage of personal voter data, just as the GSA was required to do. The President's Executive Order and the Commission's Charter clearly establish that the GSA—not the White House—"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 . . . ." Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017), Ex. 1. The GSA is undeniably an agency whose actions are subject to judicial review. *AT&T Info. Sys., Inc. v. GSA*, 810 F.2d 1233 (D.C. Cir. 1987) (applying both the APA and the FOIA to the GSA). To the extent that the Commission might evade the E-Government Act's PIA requirement by using non-GSA facilities to collect voter data, EPIC would face certain informational injury due to the non-disclosure of a PIA. The Court must hold such action unlawful and restrain it.

C. The publication of voters' personal information violates the constitutional right to informational privacy

The Supreme Court has long recognized that individuals have a constitutionally protected interest in "avoiding disclosure of personal matters." *Whalen v. Roe*, 429 U.S. 589, 599 (1977); *accord Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457 (1977). The constitutionality of a "government action that encroaches upon the privacy rights of an individual is determined by balancing the nature and extent of the intrusion against the government's interest in obtaining the information it seeks." *United States v. District of Columbia*, 44 F. Supp. 2d 53 (D.D.C. 1999); *see also Senior Execs. Ass'n v. United States*, 891 F. Supp. 2d 745, 750–51 (D. Md. 2012) (granting a motion for a preliminary injunction to prohibit disclosure of financial information from executive

branch and military officials under the STOCK Act). The "individual interest in protecting the privacy of information sought by the government" is more important when that information is to be "disseminated publicly." *Am. Fed'n of Gov't Emps., AFL-CIO v. HUD*, 118 F.3d 786, 793 (D.C. Cir. 1997) [hereinafter *AFGE v. HUD*] (assuming without concluding that the right exists).

In *NASA v. Nelson*, Justice Alito, writing for the Court, said:

> As was our approach in *Whalen*, we will assume for present purposes that the Government's challenged inquiries implicate a privacy interest of constitutional significance. 429 U.S., at 599, 605. We hold, however, that, whatever the scope of this interest, it does not prevent the Government from asking reasonable questions of the sort included on SF-85 and Form 42 in an employment background investigation that is subject to the Privacy Act's safeguards against public disclosure.

NASA v. Nelson, 562 U.S. 134, 147–48 (2011).

The actual holding in *Nelson* is significant in this matter for several reasons. First, the Court in *NASA v. Nelson* observed that in *Whalen v. Roe,* "the Court pointed out that the New York statute contained 'security provisions' that protected against "[p]ublic disclosure" of patients' information." 562 U.S. at 145. "The [Whalen] Court thus concluded that the statute did not violate 'any right or liberty protected by the Fourteenth Amendment.'" *Id.* (citing *Whalen v. Roe*, 429 U.S. at 606). Second, the Court in *Nelson* relied on the Privacy Act's safeguards to prohibit public disclosure. Third, the Supreme Court in both *Whalen* and in *Nelson* deemed the request for information to be "reasonable."

Here the sensitive voter data sought from the states, including felony convictions and partial SSNs, is on par with the personal information at issue in *Whalen* and *Nelson,* though whether it is "reasonable" is broadly contested by state election officials across the country. *See, e.g,* Editorial, *Texas and Other States Are Right to Refuse Trump Panel's Request for Private Voter Information*, Dallas Morning News (July 7, 2017) ("Conservatives and liberals alike should be appalled that a commission brought into existence by a presidential executive order wants such sensitive personal data on the thinnest of pretexts."). It bears emphasizing that this opposition to

the Commission's is from a bipartisan group of public officials most expert in the data sought and the laws that apply.

Moreover, contrary to the security methods mandated by the state statute in *Whalen*, the Commission has (1) proposed an unsecure server to receive sensitive data and (2) has disclaimed any responsibility to undertake a Privacy Impact Assessment. Most critically, the Commission has given no indication that its data collection practices are subject to the strictures of the Privacy Act, which was the key reason in *Nelson* that the Court did not reach the informational privacy claim. As Justice Alito explained in the holding for the Court:

> In light of the protection provided by the Privacy Act's nondisclosure requirement, and because the challenged portions of the forms consist of reasonable inquiries in an employment background check, we conclude that the Government's inquiries do not violate a constitutional right to informational privacy.

NASA, 562 U.S. at 764–65.

The Commission has presented this Court with informational privacy risks comparable to those that were before the Supreme Court in *Whalen v. Roe* and *NASA v. Nelson*, but with none of the privacy safeguards or practices that provided the Court with sufficient assurances and little evidence that the request is "reasonable." These are the circumstances where the claim of informational privacy are most compelling. The Supreme Court explained in Whalen that the "interest in avoiding disclosure of personal matters" is an aspect of the right of privacy, and intimated "a sufficiently grievous threat" may establish a "constitutional violation." *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977). Without a "successful effort to prevent abuse and limit access to the personal information at issue," which the disclosure amounts to to "a deprivation of constitutionally protected privacy interests" requiring the state to prove the measures are "necessary to promote a compelling state interest." *Id.* at 607 (Brennan, W., concurring).

If there were any information worthy of a constitutional shield from disclosure, it is personal information shared for the limited purpose of exercising of the right to vote. The right to vote is referenced by the U.S. Constitution five times, more than any other right. U.S. Const. amends. XIV § 5, XV § 1, XIX, XXIV § 1, XXVI § 1. The right to vote, secured only

through robust voter privacy measures, is foundational to American democracy. That the Commission attempts to collect personal *voter* data en masse raises the constitutional stakes. And, without a "successful effort prevent abuse and limit access to" that data—such as the Commission's direction to use an unsecured website for the data transfer—the state must demonstrate to the Court the "necess[ity]" of the collection "to promote a compelling state interest." *Whalen*, 429 U.S. at 607. A proposal to establish a national database of sensitive voter data, gathered contrary to state privacy law, and with no assurance of privacy protection makes clear the right of informational privacy. There is little in the Supreme Court's decisions in *NASA v. Nelson* and *Whalen v. Roe*, or even the D.C. Circuit's *AFGE* opinion, to suggest otherwise. And regardless of whether the Commission considers itself outside of the FACA or the APA, it is not beyond the reach of the federal Constitution.

The Government has previously survived right to informational privacy challenges where it implemented measures to protect the confidentiality and security of the personal information that it was collecting or there was a federal law that provided substantial protection. *See id.* (upholding collection of personal information by HUD on the SF 85P form); *NASA v. Nelson*, 562 U.S. 134, 156 (2011). But when no such safeguards exist, when the Government has not "evidence a proper concern" for individual privacy, the individual's interest in prohibiting the collection of their information by an agency is strongest. *NASA*, 562 U.S. at 156. That is especially true when the data includes identifying and sensitive information such as addresses, date of birth, SSNs, and political affiliations.

The Commission has taken no steps to protect this sensitive personal information that they are seeking to collect. Instead, they have disclaimed all responsibility for maintaining the security and confidentiality of these records. In the letter to Secretaries of State, Vice Chair Kobach tells the states to "be aware that any documents that are submitted to the full Commission will also be made available to the public." Ex. 3, at 2. The Commission has provided no justification for such broad collection and disclosure of voters' personal information. In the letter, the Vice Chair claims, without any supporting evidence, that the data will be used to "analyze vulnerabilities and

issues related to voter registration and voting." Ex. 3, at 1. But the Office of the Vice President and the Commission have no authority to oversee state voter registration, and the Executive Order makes clear that the purpose of the Commission is to "study" election integrity.

Informational privacy claims merit heightened scrutiny. *See, e.g.*, *Eisenbud v. Suffolk County*, 841 F.2d 42, 45 (2d Cir. 1988); *Fraternal Order of Police, Lodge 5, v. City of Philadelphia*, 812 F.2d 105, 110 (3d Cir. 1987). This requires a "delicate task of weighing competing interests," *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980). *See Doe v. Attorney General*, 941 F.2d 780 (9th Cir. 1991). In order to overcome the constitutional obligation to protect personal information from disclosure, the government must demonstrate "sufficiently weighty interests in obtaining the information sought" and "justify the intrusions into the individuals' privacy." *AFGE v. HUD*, 118 F.3d at 793. The Commission has not identified any legitimate interests that would justify such a sweeping and unprecedented public disclosure of voter records.

II. EPIC's members will suffer irreparable harm if relief is not granted.

If the Court does not enjoin the Commission's unlawful collection, aggregation, and public disclosure of voter data, EPIC's members will be irreparably harmed. Individual voter data is not broadly available to the public; otherwise there would be no need for the Commission to request it from the states. These records are collected by the states for a specific purpose—voter registration—and voters have not authorized its dissemination to or by the Commission for an entirely different, and undisclosed, purpose.

There is no doubt that the categories of data listed in the Commission's unlawful demand: date of birth, last four digits of the social security number, and political affiliation, paired with full name and address are sensitive and confidential. The unauthorized disclosure of this sensitive personal information would cause immeasurable harm for three reasons. First, a violation of an individual's constitutional rights is a *per se* harm. Second, disclosure of confidential information is a *per se* harm, especially where that disclosure is unlawful and monetary damages are not

available. And third, creation of a unified federal voter registration database without any privacy or security protections would put members' personal information at risk; voter data has already been targeted at the state level, and the Commission has none of the tools or experience that states have deployed to protect that data from unauthorized access.

A violation of the constitutional right to informational privacy, alone, is sufficient to satisfy the irreparable harm test. *Fort Wayne Women's Health v. Bd. of Comm'rs, Allen County, Ind.*, 735 F. Supp. 2d 1045, 1061 (N.D. Ind. 2010). *See Am. Fed'n of Gov't Emps., AFL-CIO v. Sullivan*, 744 F. Supp. 294, 298 (D.D.C. 1990); *Senior Execs. Ass'n v. United States*, 891 F. Supp. 2d 745, 750–51 (D. Md. 2012). The Commission has made clear that it will publicly release the voter data in some form. First Kobach Decl. ¶ 5. The Commission claims it will "de-identify" this data, but has given "no identification or description of the process or technique, no explanation of what the Commission hopes to protect and how they can ensure they have done so, and no description of the reason for publishing anything." Decl. of Cynthia Dwork ¶ 7, Ex. 23. There is an "inherent contradiction" in the Commission's simultaneous statements that there is no privacy interest in the voter data and that the Commission will take steps to protect the privacy of the data. And the disclosure of personal identifying information itself also gives rise to an irreparable injury. *Does v. Univ. of Wash.*, No. 16-1212, 2016 WL 4147307, *slip op.* at *2 (W.D. Wash. Aug. 3, 2016). "In the age of the internet, when information is made public quickly and without borders, it is nearly impossible to contain an impermissible disclosure after the fact, as information can live on in perpetuity in the ether to be shared for any number of deviant purposes." *Wilcox v. Bastiste*, No. 17-122, 2017 WL 2525309, *slip op.* at *3 (E.D. Wash. June 9, 2017); *see also Pacific Radiation Oncology, LLC v. Queen's Medical Center*, 47 F. Supp. 3d 1069, 1076 (D. Haw. 2014) (noting that it is "beyond dispute that the public disclosure of that information" in medical files would subject patients "to potential irreparable harm").

The unlawful disclosure of confidential or proprietary information is a *per se* harm and should, by itself, justify enjoining the Commission's collection of personal voter data in this case. *See CAIR v. Gaubatz*, 667 F. Supp. 2d 67, 76 (D.D.C. 2009) (granting a temporary restraining

order to prevent disclosure of CAIR's "proprietary, confidential, and privileged information); *see also Ruckelshaus v. Monsanto Co.*, 463 U.S. 1315, 1317 (1983) (Blackmun, J., in chambers) (denying the government's petition for a stay pending appeal on the grounds that disclosure of Monsanto's proprietary information could "cause irreparable harm"). The Commission cannot seriously contend that disclosure of the voter data elements listed in their June 28, 2017, letter would be permissible under federal or state law, and yet they nevertheless has demanded that the states turn over that confidential voter data.

There is evidence that the Commission will collect the voter data absent an injunction from this court because the state of Arkansas already submitted data via the insecure Department of Defense portal *after this suit was already pending*. TRO Hr'g Tr. 41, July 7, 2017. Arkansas officials have since revealed that the data that they sent to the Commission included "names, addresses, dates of birth, political party affiliations, voter history since 2008, registration status, email addresses and phone numbers." Bill Bowden & Brian Fanney, *U.S. Tells Arkansas to Delete Files on Voter Data*, Arkansas Online (July 13, 2017), Ex. 37. Arkansas did this despite the fact that Governor Asa Hutchinson said that the state should not provide the data " and did not "want to facilitate the providing of that information to a federal database." *Id*. This is clear evidence that the Commission is using its power to influence states to release data that should be kept confidential.

The Commission also cannot credibly claim that they do not intend to collect confidential voter data such as the last four digits of the SSN. In fact, Vice Chair Kobach has used the same data elements that he requested in his June 28, 2017, Commission letter as part of his Kansas-based "Interstate Voter Registration Crosscheck Program." Ex. 33, at 8. The last four digits of the SSN are a core part of the "matching" algorithm used in the Crosscheck program. Yet Kobach's efforts to create a federal Crosscheck program through the Commission's request are designed to circumvent and undermine federal privacy law. Congress passed the Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (Oct. 18, 1988), in order to amend the Privacy Act to limit the improper use of computer matching algorithms by federal

agencies. Congress passed further amendments to strengthen the due process provisions in the Computer Matching and Privacy Protection Amendments of 1990, Pub. L. No. 101-508, 104 Stat. 1388 (Nov. 5, 1990). Yet Kobach and the Commission now intend to collect voter data to extend their Crosscheck matching program while ignoring the privacy and due process requirements imposed by federal law. This unlawful secondary use of EPIC's members' personal voter data will cause immediate and irreparable harm.

Even the mere collection and aggregation of the state voter data itself would cause an irreparable harm to EPIC's members because the Commission has taken no steps to ensure the security and integrity of the data. States recognize that they face an acute and increasing risk that their voter data will be targeted by malicious hackers and, in response, are taking special measures to protect this sensitive data. *See* Exs. 26–31. Even federal government officials recognize that voter data is uniquely vulnerable due to its sensitive nature and the fact that it is a high value target. *Id*. Yet, despite these clear risks, the Commission intends to put all the eggs in one basket, creating a irresistible target for hackers. The fact that this data will be stored within the EOP does not provide any reassurance. The White House's track record for information security is alarming in its own right. Evan Perez & Shimon Prokupecz, *How the U.S. Thinks Russians Hacked the White House*, CNN (Apr. 8, 2015);[22] Ellen Nakashima, *Hackers Breach Some White House Computers*, Wash. Post (Oct. 28, 2014);[23] Sean Gallagher, *"Hacked" E-Mail Account of White House Worker Exposed in 2013 Password Breach*, ArsTechnica (Sept. 23, 2016);[24] Lily Hay Newman, *That Encrypted Chat App the White House Liked? Full of Holes*, Wired (Mar. 9, 2017).[25] Given the recent history of data breaches in federal government systems

[22] http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.htm.
[23] https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.
[24] https://arstechnica.com/security/2016/09/hacked-e-mail-account-of-white-house-worker-exposed-in-2013-password-breach/.
[25] https://www.wired.com/2017/03/confide-security-holes/.

that house sensitive information, the lack of planning and foresight on the part of the Commission poses an immediate and inexcusable risk to the privacy of all voters.

Not only do the Commission's proposed insecure data transfer methods create serious *security* risks for the sensitive personal voter data that the Commission requested, these methods are incapable of ensuring the *integrity* and accuracy of the data that the Commission receives. The Commission has not provided any evidence that the email address or the File Exchange website are capable of verifying the source and authenticity of the documents and data submitted. Criminals and other unauthorized parties are known to send fake emails "that are made to appear as if they are coming from" government accounts, including accounts within the Pentagon's "Defense Security Service." Jenna McLaughlin, *Pentagon Email Addresses Being Used in Cyber Spoofing Campaign*, Foreign Policy (May 12, 2017).[26] Nothing would stop a malicious actor—perhaps even a foreign government—from submitting fake "voter roll" data to the Commission to degrade the accuracy of the database. These are precisely the types of issues that would have been identified during a Privacy Impact Assessment, but the Commission failed to conduct one prior to initiating this proposed collection.

The Commission goes to great lengths to emphasize that it is only seeking "publicly available" information. But in fact the vast majority of personal data sought by the Commission is protected by state voter privacy laws. According to a preliminary survey by EPIC, states could provide the Commission with little more than name and address of registered voters without running afoul of state law.[27] A study by the Brennan Center also finds numerous restrictions on

[26] http://foreignpolicy.com/2017/05/12/pentagon-email-addresses-being-used-in-cyber-spoofing-campaign/.

[27] *See e.g.* Alaska Stat. § 15.07.195 ("The following information set out in state voter registration records is confidential and is not open to public inspection: (1) the voter's age or date of birth; (2) the voter's social security number, or any part of that number; (3) the voter's driver's license number; (4) the voter's voter identification number; (5) the voter's place of birth; (6) the voter's signature."); *see also e.g.* Ind. Code § 3-7-26.4-8 (2017) ("The election division shall not provide information under this section concerning any of the following information concerning a voter: (1) Date of birth. (2) Gender. (3) Telephone number or electronic mail address. (4) Voting history. (5) A voter identification number or another unique field established to identify a voter. (6) The date of registration of the voter.").

the release of state voter rolls. Brennan Center for Justice, Examples of Legal Risks to Providing Voter Information to Fraud Commission (Jul. 2017).[28]

The Commission contends that it "has only requested data that is already public available," Def. Opp'n 8, and cites to a 2016 report of the National Conference of State Legislatures ("NCSL"). But as the NCSL actually explained, "Generally, all states provide the name and address or the registered voter. From there is gets complicated. At least 25 states limit access to social security numbers, date of birth or other identifying factors such as a drivers license number." *See* National Conference of State Legislatures, States and Election Reform (Feb. 2016).[29] The 2016 NCSL report notes also that "Texas specifically restricts the residential address of any judge in the state" and several states have a general prohibition on "information of a personal nature." *Id.*[30]

The 2016 NCSL report, cited by the Commission, goes on to explain the limitation on access to voter data, use of voter data, and costs for obtaining voter data. The NCSL explains "Beyond candidates and political parties, who can access voter lists varies state by state. Eleven states do not allow members of the public to access voter data." *Id.* at 2. Further, several states restrict the use of voter data. Several states limit "the use to just political purposes or election purposes." *Id.* States also typically charge requesters costs for the production of data. According to the NCSL, "the average cost for a voter list is approximately $1,825."[31]

Even names and address are not always available. The NCSL report notes that "thirty-nine states maintain address confidentiality programs designed to keep the addresses of victims of

---

28 https://www.brennancenter.org/sites/default/files/analysis/Legal_Implications_of_Kobach_Request.pdf.

29 http://www.ncsl.org/Documents/Elections/The_Canvass_ February_2016_66.pdf.

30 *See e.g.* Kan. Stat. Ann. § 45.221(30) (exempting from the Kansas Open Records Act any "Public records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy.").

31 The Commission made no offer in its letter to the states to pay any of the costs associated with the production of the voter roll data. The Commission instructed the state officials to provide the data by email or to an insecure website.

domestic violence or abuse, sexual assault or stalking out of public records for their protection." *Id.* at 2. The NCSL describes additional restrictions on the release on name and address information who are preregistered but are also minors. *Id.* at 2-3.

What then to make of a request from a Commission charged with "promoting election integrity" that asks state election officials to turn over Social Security Numbers, military status, felony convictions records, party affiliation and state voting history? The answer is provided by the response of the state officials who simply refused to release the personal data sought by the Commission.

III. The balance of the equities and public interest favor relief.

The balance of the equities and public interest factors favor entry of the temporary restraining order that EPIC seeks. This purpose of temporary relief is to preserve, not "upend the status quo." *Sherley v. Sebelius*, 644 F.3d 388, 398 (D.C. Cir. 2011); *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 43 (2008). Preserving the status quo is the purpose of EPIC's motion. Currently there is no single federal database that houses state voter roll data. The Commission now seeks in an unprecedented shift to change that fact without prior review of the privacy implications as required by law. The public interest and balance of the equities favor EPIC's request to preserve the status quo pending review by this Court.

There are no countervailing interests that weigh against the relief EPIC seeks. The Commission would not be harmed by a temporary halt to its plans, as it has no valid interest in violating the PIA requirements in the E-Government Act. "There is generally no public interest in the perpetuation of unlawful agency action." *League of Women Voters*, 838 F.3d at 12 (citing *Pursuing America's Greatness v. FEC*, 831 F.3d 500, 511-12 (D.C. Cir. 2016); *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013). In fact, "there is a substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations." *Id.* at 12.

The Commission's actions cut directly against the stated mission to "identif[y] areas of opportunity to increase the integrity of our election systems." Ex. 3, at 2. By collecting and aggregating detailed, sensitive personal voter information without first conducting a PIA, the Commission is threatening the security and integrity of the entire voting system. This action will not only put voter data at risk; it will risk disincentivizing voters in a way similar to the restrictive documentation requirements in *League of Women Voters*. Indeed, there are already reports of citizens cancelling their voter registration out of concern for their privacy. Andrew Gumbel, *Trump Election Commission Backs Away from Its Request for Voter Data After Outcry*, Guardian (July 13, 2017).[32] The court the found that the requirement to reveal "sensitive citizenship documents" in order to register to vote caused the voter registration numbers to "plummet[]" and found that there was a strong public interest in favor of enjoining the change. *League of Women Voters*, 838 F.3d at 4, 9, 13. The right to vote is "preservative of all rights" and of "most fundamental significance under our constitutional structure." *Id.* at 12. The Commission has not provided any evidence that the collection and aggregation of sensitive voter data would "increase the integrity of our election systems." More likely, it will have the opposite effect.

CONCLUSION

The Emergency Motion for a Temporary Restraining Order should be granted, and Defendants should be restrained from collecting state voter data prior to the completion of a Privacy Impact Assessment.

[32] https://www.theguardian.com/us-news/2017/jul/13/donald-trump-election-integrity-commission-voter-data-backlash.

Respectfully Submitted,

/s/ Marc Rotenberg
MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

CAITRIONA FITZGERALD*
EPIC Policy Director

JERAMIE D. SCOTT, D.C. Bar # 1025909
EPIC Domestic Surveillance Project Director

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

** Pro hac vice motion pending*

Dated: July 13, 2017