IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES; GENERAL SERVICES ADMINISTRATION Defendants.	Civ. Action No. 17-1320 (CKK)

REPLY IN SUPPORT OF PLAINTIFF'S EMEREGNCY MOTION FOR A TEMPORARY RESTRAINING ORDER

The Court should grant Plaintiff's motion for a Temporary Restraining Order because the Commission seeks to obtain sensitive personal data from state election officials that may not be lawfully disclosed and because the Commission has failed to establish necessary privacy safeguards for the collection of personal information.

Notwithstanding the Commission's claims to the contrary, EPIC has established standing on multiple grounds. First, the Commission seeks all of the records of registered voters in the United States and EPIC is an organization, based in the United States, comprised of registered voters. That alone is sufficient to establish standing. Second, EPIC has obtained affidavits from individual members that make clear that specific members of EPIC are subject to the actions of

the Commission. Third, as an organization established in 1994 to "focus public attention on emerging privacy issues," there is hardly an issue of greater concern to EPIC, as an organization, than a proposal to build a database, maintained in the White House, of the nation's registered voters.

EPIC has also satisfied the requirements for the emergency relief sought. The Commission has asked state election officials to transfer massive amounts of sensitive personal data, protected by state privacy law, to an insecure website without authentication. EPIC's computer science expert confirms that popular web browsers warn users that their information may be stolen ("for example, passwords, messages or credit cards") and that the website "could put your confidential information at risk." It is difficult to construct an example of "irreparable harm" that is more self-evident.

EPIC has multiple ways in which it will prevail on the merits. Even though the Commission now seeks to hide its FACA obligations from the Court, the Commission's Charter and case law makes clear that that the Commission is subject to FACA and is an agency for purposes of the E-Government Act. And there is no effort by the Commission to deny that it failed to complete a Privacy Impact Assessment or to post a FACA notice, as EPIC alleged. Further, EPIC's claims for a violation of the constitutional right to information privacy are particularly strong in this case. The Commission has sought to compel the release of sensitive personal information, at the heart of democratic institutions and protected under state law. The Commission has proposed an insecure website to gather personal data and has denied any obligations to safeguard the data it seeks, notably disclaiming the need to conduct a Privacy Impact Assessment or to comply with the Privacy Act. The Commission has even attempted to put itself beyond the reach of the FACA and the APA. These are the circumstances, anticipated

by the Supreme Court in *Whalen v. Roe* and *NASA v. Nelson,* where a constitutional privacy claim would be paramount.

The public interest analysis also favors EPIC because the Commission is only authorized to "study" issues concerning 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." Executive Order No. 13,799, 82 Fed. Reg. 22,389, 22,389 (May 11, 2017). By the terms of the Commission's purpose and the actions undertaken by the Commission, the order EPIC seeks should be granted.

Finally, the Commission ties itself in knots when it represents to the Court that the information sought is "publicly available" (and therefore no privacy interest attaches) while simultaneously providing assurances for the Court that privacy will be protected. In a declaration for the Court, the Commission Vice Chair states, (1) that the transmission methods for the voter data is "tested and reliable," (2) that the "Commission intends to deidentify any such data prior to any public release of documents," and (3) that "the voter rolls themselves will not be released to the public by the Commission." If the data is "publicly available," why is the Commission seeking to assure the Court that privacy protections will be established?

The Commission has conceded the obvious: the privacy implications of this unprecedented demand for voter roll data from across the country are staggering. This Court

should do no less. An order should issue enjoining the Commission from obtaining the personal information of registered voters.

ARGUMENT

In its opposition to EPIC's motion for a TRO, the Commission takes the extraordinary position that it can create a database, stored in the White House, containing sensitive personal data about every registered voter in the United States without complying with any of the laws enacted to protect personal privacy. The Commission cites decisions rejecting injunctions in circumstances that bear no resemblance to this case. The Commission does not cite a single example of a government entity that was permitted to collect and aggregate sensitive personal information without first conducting a privacy impact assessment as required under the E-Government Act. There is no such example, because government agencies are not above the law. State officials, unlike the Commission, understand the inherently sensitive nature of voter roll data, which is why many have opposed the Commission's unlawful demand. This Court should grant EPIC's emergency motion for a temporary restraining order and prohibit the collection of personal voter data pending resolution of a preliminary injunction.

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).[1] The merits of EPIC's claim are clear and simple: the Commission violated federal law when it initiated collection of personal voter data without first conducting a PIA as required under the E-Government Act and posting a FACA notice. The Commission's excessive and unprecedented collection of personal data without adequate privacy

[1] As this Court noted in *Dimondstein*, the injunction factors have traditionally been evaluated on a "sliding scale" in this Circuit. 964 F. Supp. 2d at 41.

safeguards would violate voters' constitutional right to informational privacy, which the Supreme Court recently acknowledged in *NASA v. Nelson*, 562 U.S. 134 (2011).

EPIC has also satisfied the other requirements for injunctive relief because EPIC has shown that the Commission's unlawful collection of personal voter data would cause an immediate and irreparable injury to EPIC and EPIC's members, and because the balance of the equities and the public interest favor injunctive relief. This Court has made clear that issuance of a TRO is appropriate, as in this case, in order "to preserve the status quo and to prevent irreparable harm." *CAIR v. Gaubatz*, 667 F. Supp. 2d 67, 79 (D.D.C. 2010).

I. The Commission has not shown that the unprecedented collection of personal voter data would be consistent with the Constitution or with federal law.

A. The Commission has failed to show that it does not fit within the clear statutory definition of "agency" and has conceded that PIA's are required under federal law.

The Commission claims 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 not supported by any of the cases cited in the opposition. *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 Soucie v. David*, 448 F.2d 1067, 1073 (D.C. Cir. 1971) (establishing the "substantial independent authority" test and finding that the Office of Science and Technology was an "agency" for the purposes of the APA); *McKinney v. Caldera*, 141 F. Supp. 2d 25, 31–34 (D.D.C. 2001) (reviewing cases applying the APA agency definition). 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.

The Commission acknowledges at the outset the definition of "agency" in the APA is broad. Mem. Op. 10 ("The APA defines 'agency' as 'each authority of the Government of the United States,' subject to several limitations not applicable here."). But rather than accept the plain text, the Commission attempts to rely on cases that have provided narrow exemptions for (1) the President specifically, *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992), and (2) certain close advisors to the President, *Meyer v. Bush*, 981 F.2d 1288 (D.C. Cir. 1993); *Armstrong v. Exec. Office of the Pres.*, 90 F.3d 553, 558 (D.C. Cir. 1996); *CREW v. Office of Admin.*, 566 F.3d 219, 223–23 (D.C. Cir. 2009). These cases are inapposite and do not apply to an entity such as the Commission.

Here, as in *Energy Research Foundation v. Defense Nuclear Facilities Safety Board*, 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 v. David*, 448 F.2d 1067, 1075 (D.C. Cir. 1971)) ("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. Kobach Letter 1–2. The Commission cannot credibly characterize this behavior as incidental to its advisory role: it is acting with the force and effect of an agency.

Eight days ago, the Commission undertook to assemble a database of personal voter information covering at least 157 million registered voters across 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), Pl. Mot. TRO Ex. 3; U.S. Census Bureau, Voting and Registration in the Election of November 2016 at tbl. 4a (May 2017).[2] This sweeping depository of personal data would put the Internal Revenue Service—with its yearly haul of just 149 million individual returns—to shame. *SOI Tax Stats - Tax Stats at a Glance*, IRS (2016).[3] The Commission launched this remarkable data collection program with no apparent direction from the President, other than an instruction two months earlier to "study the registration and voting processes used in Federal elections." Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017).

It is simply not true, let alone "well-established," that a president's "close advisors" are categorically immune from APA review. Def. Opp'n 10 (citing a lone case, *Franklin v. Massachusetts*, 505 U.S. 788, 800–01 (1992), which says nothing about presidential advisors). The determination of whether an entity within the Executive Office of the President constitutes an agency depends on several factors:

> These tests have asked, variously, "whether the entity exercises substantial independent authority," *Armstrong v. Executive Office of the President,* 90 F.3d 553, 558 (D.C. Cir. 1996) (internal quotation mark omitted), "whether ... the entity's sole function is to advise and assist the President," *id.* (internal quotation mark omitted), and in an effort to harmonize these tests, "how close operationally the group is to the President," "whether it has a self-contained structure," and "the nature of its delegat[ed]" authority, *Meyer v. Bush,* 981 F.2d 1288, 1293 (D.C. Cir. 1993).

Citizens for Responsibility & Ethics in Washington (CREW) v. Office of Admin., 566 F.3d 219, 222 (D.C. Cir. 2009).

This Commission is doing far more than "advis[ing] and assist[ing];" rather, it is taking substantive steps and exercising "substantial[] independen[ce]" from the President. *Meyer*, 981

[2] https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html.
[3] https://www.irs.gov/uac/soi-tax-stats-tax-stats-at-a-glance.

F.2d at 1293. Restating the word "advisory," as the Commission does, cannot erase this conclusion, because "the record evidence regarding [the Commission]'s actual functions" proves otherwise. *Citizens for 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. The Commission is creating a new database, demanding and collecting vast sums of personal voter data to place in that database, and threatening to publish that information. Kobach Letter 1–2. This is the work of an agency engaged in substantive activity, not an advisor helping the President choose between difference courses of action. *See Armstrong*, 90 F.3d at 558 (noting that the Office of Science and Technology is an "agency" because "not withstanding its proximity to the President" it exercised certain forms of "independent authority") (quoting *Soucie v. David*, 448 F.2d 1067, 1075 (D.C. Cir. 1971)). The Commission is thus an agency under the APA.

Because the Commission is an "agency" under the APA, it necessarily meets the definition under the E-Government Act as well. § 3502(1). As the Commission itself concedes, the definition of "agency" used in the FOIA is broader than that of the APA, Def. Opp'n 10, and the definition of "agency" in the E-Government Act is 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, 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).[4]

Privacy Impact Assessments are a critical step that all agencies must take prior to initiating collection of personal information. In many cases, these assessments lead to changes in

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

or abandonment of the agency programs under review, which are necessary to avoid inherent privacy risks. For example, the Department of Homeland Security cancelled a controversial national license plate tracking program following the initiation of a Privacy Impact Assessment. *See* Dep't of Homeland Sec., DHS-ICE-PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service (2015);[5] Ellen Nakashima & Josh Hicks, *Department of Homeland Security Cancels National License-Plate Tracking Plan*, Washington Post (Feb. 19, 2014).[6] Similarly, the TSA was forced by Congress to shutter a controversial passenger screening program after an initial privacy assessment raised significant issues. Ryan Singel, *Congress Puts Brakes on CAPPS II*, Wired (Sept. 26, 2003) ("Congress moved Wednesday to delay the planned takeoff of a controversial new airline passenger-profiling system until an independent study [by the GAO] of its privacy implications and effectiveness at stopping terrorism can be completed.").[7]

The Commission's failure to undertake the Privacy Impact Assessment, required of all federal agencies, places at risk the privacy interests of registered voters across the country.

B. The Commission ignores the factors in this case that implicate the constitutional right to information privacy.

The Commission asserts that EPIC's claim that a constitutional right to informational privacy fails because "neither the Supreme Court nor the D.C. Circuit has held that a federal right to informational privacy exists." But that is not what the Court has said.[8] In *NASA v. Nelson*, Justice Alito, writing for the Court, said:

---

[5] https://www.dhs.gov/publication/dhs-ice-pia-039-acquisition-and-use-license-plate-reader-data-commercial-service.

[6] https://www.washingtonpost.com/world/national-security/dhs-cancels-national-license-plate-tracking-plan/2014/02/19/a4c3ef2e-99b4-11e3-b931-0204122c514b_story.html.

[7] https://www.wired.com/2003/09/congress-puts-brakes-on-capps-ii/.

[8] Even the Commission's analysis of D.C. Circuit law is misleading. In fact, in *Am Fed. Of Gov't Emps., AFL-CIO v. Dep't of House & Urban Dev.* 118 F.3d 786, 791 (D.C Cir. 1997), the Court observed:

> 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.*

> [S]everal of our sister circuits have concluded based on *Whalen* and *Nixon* that there is a constitutional right to privacy in the nondisclosure of personal information. *See United States v. Westinghouse Electric Corp*., 638 F.2d 570, 577-580 (3d Cir. 1980) (holding that there is a constitutional right to privacy of medical records kept by an employer, but that the government's interest in protecting the safety of employees was sufficient to permit their examination); *Plante v. Gonzalez*, 575 F.2d 1119, 1132, 1134 (5th Cir. 1978), *cert. denied*, 439 U.S. 1129 (1979) (identifying a "right to confidentiality" and holding that balancing is necessary to weigh intrusions); *Barry v. City of New York*, 712 F.2d 1554, 1559 (2d Cir. 1983), *cert. denied,* 464 U.S. 1017 (1983) (applying an intermediate standard of review to uphold a financial disclosure requirement). *See also, Hawaii Psychiatric Soc'y Dist. Branch v. Ariyoshi*, 481 F. Supp. 1028, 1043 (D. Hawaii 1979) (holding that disclosure of psychiatric records implicates the constitutional right to confidentiality); *McKenna v. Fargo,* 451 F. Supp. 1355, 1381 (D.N.J. 1978) ("The analysis in *Whalen* … compels the conclusion that the defendant … must justify the burden imposed on the constitutional right of privacy by the required psychological evaluations.").

118 F.3d at 792.

The court in *AFGE* concluded:

> Having noted that numerous uncertainties attend this issue, we decline to enter the fray by concluding that there is no such constitutional right because in this case that conclusion is unnecessary. Even assuming the right exists, the government has not violated it on the facts of this case. Whatever the precise contours of the supposed right, both agencies have presented sufficiently weighty interests in obtaining the information sought by the questionnaires to justify the intrusions into their employees' privacy.

AFGE v. HUD, 326 U.S. App. D.C. 185, 118 F.3d 786, 793 (1997). In this matter, the Commission has presented no such "sufficiently weighty interests" to justify the intrusion in the privacy of hundreds of millions of registered voters.

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.

II. The Commissions unlawful and insecure collection of personal voter data would cause an irreparable injury

In response to EPIC's motion, the Commission has submitted irrelevant and self-contradictory statements regarding the irreparable harm posed by the unlawful collection of voter data, and the Commission has failed to address the obvious data security risks created by their actions. EPIC has presented evidence to show that disclosure of personal voter data would create a "great, actual, and imminent" injury, *Dimondstein*, 964 F. Supp. 2d at 49, including sworn statements by privacy and security experts. *See, e.g.*, Pl. Mot. TRO Ex. 6; Second Decl. of Harry Lewis, Ex. 11; EPIC Member Declarations, Exs. 1–9. In contrast, the Commission has submitted a declaration from a named defendant in this case with no stated background in computer science or privacy law, which includes unsupported assertions about the "security" of "file transfer" methods. *See* Decl. of Kris W. Kobach.

Absent the issuance of a TRO in this case, the Commission's actions will cause irreparable harm to EPIC and its members for three independent and distinct reasons, none of which are "speculative." First, the Commission's reliance on insecure data transfer methods poses an obvious threat to the integrity and security of the voter data. Second, the Commission itself has conceded that the personal voter data it is collecting should not be made publicly available. And third, any post-collection remedies available to voters are not adequate to address the misuse and mishandling of their personal data by the Commission.

Vice Chair Kobach concedes in his declaration that he sent "identical letters" to "secretaries of state or chief election officers in each of the fifty states and the District of Columbia," which demanded that those state officials submit personal voter data and stated that

the officials could "submit [their] responses electronically to ElectionIntegrityStaff@ovp.eop.gov *or by* utilizing the Safe Access File Exchange" system. Kobach Decl., Ex. 3, at 2 (emphasis added). In his declaration, Kobach contradicts his own letter by claiming that he "intended" for the states to use the File Exchange website (rather than an email address) to send personal voter data to the Commission. Kobach Decl. ¶ 5. While Kobach did not offer any explanation for this discrepancy, his statement makes clear he is aware that email is not a secure method to be used for transferring personal voter data. Kobach Decl. ¶ 5. But even if state officials follow the "intent" rather than the text of Kobach's letter, voters personal data will not be secure.

As Harry Lewis, a distinguished professor of computer science at Harvard University, explains, the website referred to in the Commission's letter ("safe.amrdec.army.mil") is "not a secure website for the transfer of personal data." Second Decl. of Harry Lewis ¶ 9. In fact, when Professor Lewis attempted to access the website using common internet browsers, he was directed to clear warnings that the site was not secure. *Id*. ¶ 7–8. In Google Chrome, the warning read "Your connection is not private—Attackers might be trying to steal your information from safe.amrdec.army.mil (for example, passwords, messages, or credit cards)." *Id.* ¶ 7. In Safari, the website returned an error message that stated "Safari can't verify the identity of the website 'safe.amrdec.army.mil.' The certificate for this website is invalid. You might be connecting to a website that is pretending to be 'safe.amrdec.army.mil,' which could put your confidential information at risk." *Id*. ¶ 8.

Even the Commission's own description of the File Exchange website acknowledges that it was not designed to maximize security. Vice Chair Kobach states that the system is used "routinely by the military for large, *unclassified* data sets." Kobach Decl. ¶ 5 (emphasis added).

The Commission has not provided any evidence that the File Exchange system is designed, or even permitted, to be used to transfer sensitive personal information. The Commission also has not established that it has the authority to use the File Exchange system for this purpose, or that it has the authority to use "the White House computer system" to store the personal data of hundreds of millions of voters. Kobach Decl. ¶ 5.

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).[9] 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.

Even the Commission concedes that the personal voter data it seeks is sensitive and should not be released to the public. Vice Chair Kobach states in his declaration that, contrary to the text of the letter, the personal voter data submitted to the Commission "will not be released to the public." Kobach Decl. ¶ 5. But even this statement is contradicted by the sentence that

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

proceeds it: "With respect to voter roll data, the Commission intends to de-identify any such data prior to any public release of documents." Kobach Decl. ¶ 5. It is not clear whether Vice Chair Kobach believes that voter roll data is a "document" subject to his blanket promise of public disclosure. But regardless of Kobach's semantic confusion, it is clear that the Commission will release voter data to the public. The fact that the Commission "intends" to "de-identify" the data is woefully insufficient, especially where there is no evidence that the Commission is capable of deidentifying personal data of hundreds of millions of American voters.[10] The fact that Commission "intends to maintain the data on the White House computer system"[11] does not provide any meaningful assurance of security.[12]

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

[10] De-identification is a complex subject of research for computer science experts, and not something that can be implemented by the Commission on a whim. *See generally* Nat'l Inst. of Standards and Tech., NISTIR 8053, *De-Identification of Personal Information* (2015), http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf.

[11] 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), http://www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/index.htm; Ellen Nakashima, *Hackers Breach Some White House Computers*, Wash. Post (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html; Sean Gallagher, *"Hacked" E-Mail Account of White House Worker Exposed in 2013 Password Breach*, Ars Technica (Sept. 23, 2016), https://arstechnica.com/security/2016/09/hacked-e-mail-account-of-white-house-worker-exposed-in-2013-password-breach/; Lily Hay Newman, *That Encrypted Chat App the White House Liked? Full of Holes*, Wired (Mar. 9, 2017), https://www.wired.com/2017/03/confide-security-holes/.

[12] Privacy risks to voters would arise no matter what database the government stored the information in. *See, e.g.*, Tom Vanden Brook & Michael Winter, *Hackers penetrated Pentagon email*, USA Today (Aug. 6, 2015), https://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/; Office of Pers. Mgmt, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015), https://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/; Elise Viebeck, *Russians hacked DOD's unclassified networks*, The Hill (Apr. 23, 2015), http://thehill.com/policy/cybersecurity/239893-russians-hacked-dods-unclassified-networks; Nicole Perlroth, *State Department Targeted by Hackers in 4th Agency Computer Breach*, N.Y. Times (Nov. 16 2014); *Veterans Affairs Data Theft*, EPIC.org (2006), https://epic.org/privacy/vatheft/.

provide the Commission with little more than name and address of registered voters without running afoul of state law.[13] A study by the Brennan Center also finds numerous restrictions on the release of state voter rolls. Brennan Center for Justice, Examples of Legal Risks to Providing Voter Information to Fraud Commission (Jul. 2017).[14]

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).[15] 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.*[16]

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

[13] *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.").

[14] https://www.brennancenter.org/sites/default/files/analysis/Legal_Implications_of_Kobach_Request.pdf.

[15] http://www.ncsl.org/Documents/Elections/The_Canvass_ February_2016_66.pdf.

[16] *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.").

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."[17]

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 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 the public interest favor granting EPIC's motion.

The Commission's argument that preserving the status quo by issuing a TRO would be against the public interest is illogical and contrary to well established precedent. The public interest weighs heavily against permitting an unlawful governmental action, because the public interest lies in having government agencies follow the law. *League of Women Voters*, 838 F.3d at 12. The Commission has no legitimate interest in violating the law or individuals' constitutional rights, no matter how important their governmental responsibilities. *See, e.g. Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013). While the Commission alleges that collecting personal voter

[17] 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.

data from the states is a "necessary first step" for its work, it provides no evidence to show that there is urgency to that request. The Executive Order makes clear that the Commission must operate in a way "consistent with applicable law." Exec. Order No. 13,799, § 7(f). Without the PIA as required under the E-Government Act, and in violation of the constitutional right to privacy, the Commission's collection of sensitive voter data is unlawful, and thus contrary to its stated mission.

The Commission is not tasked with enforcing election law nor empowered to investigate specific election-related crimes. The Commission is only authorized to "study" the issues outlined in the Order. Exec. Order No. 13,799, § 3. Therefore, its interest in collecting particular voter information is distinctly attenuated from its purpose, lowering its interests against the restraining order. The Commission has also failed to allege precisely how the collection and aggregation of sensitive voter data is necessary to "study" and "submit a report." Exec. Order No. 13,799, § 3.

Thus, while preventing the collection of sensitive private voter data will prevent a clear violation of federal law and an infringement of the essential constitutional right of informational privacy of voters, halting this unlawful act would not cause any harm to the Commission or the public.

IV. EPIC has standing to bring this suit.

Because EPIC has clearly demonstrated an injury in fact both to itself as an organization and to its members, EPIC has Article III standing. The Commission's arguments to the contrary are based on a misreading of the record and a misinterpretation of the law.

EPIC has organizational standing to bring this suit because the Commission's unlawful collection of personal voter data directly impairs EPIC's mission and activities: "protect[ing]

privacy, free expression, [and] democratic values . . . ." *See About EPIC*, EPIC. org (2015).[18] EPIC's mission includes, in particular, the promotion of privacy safeguards for voter data. *See, e.g.*, *Voting Privacy*, EPIC.org (2017);[19] EPIC, Comment Letter on U.S. Election Assistance Commission Proposed Information Collection Activity (Feb. 25, 2005).[20] The Commission's failure to carry out a Privacy Impact Assessment and disregard for the informational privacy rights of U.S. voters have thus injured EPIC by making EPIC's "activities more difficult" and creating a "direct conflict between the [Commission's] conduct and [EPIC's] mission." *Nat'l Treasury Empls. Union v. United States*, 101 F.3d 1423, 1430 (D.C. Cir. 1996).

Like the plaintiffs in *PETA v. USDA*, 797 F.3d 1087 (D.C. Cir. 2015), EPIC has had to expend organizational resources "in response to, and to counteract, the effects of defendants' alleged [unlawful conduct]." *Id.* at 1097. Simply to preserve the status quo—wherein the federal government was *not* illegally aggregating the personal voter data of nearly 200 million Americans—EPIC has been forced to expand its long-running efforts to protect voter privacy. For example, EPIC has had (1) to draft and seek expert sign-ons for a letter urging state election officials to "protect the rights of the voters . . . and to oppose the request from the PACEI," Letter from EPIC et al. to Nat'l Ass'n of State Sec'ys (July 3, 2017);[21] (2) to seek records from the Commission concerning its collection of voter data, Letter from Eleni Kyriakides, EPIC Law Fellow, to the PACEI (July 4, 2017);[22] (3) to develop a webpage with extensive information on the Commission's activities. *Voter Privacy and the PACEI*, EPIC.org (2017); [23] and (4) respond

[18] https://epic.org/about.
[19] https://epic.org/privacy/voting/.
[20] https://epic.org/privacy/voting/register/eac_comments_022505.html.
[21] https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.
[22] https://epic.org/privacy/voting/EPIC-17-07-04-PACEI-20170704-Request.pdf.
[23] https://epic.org/privacy/voting/pacei/.

to numerous requests from state election officials, citizen organizations, and news organizations concerned about the impact of the Commission's request for voter data on personal privacy.

The Commission's direct impact on EPIC's mission and work concerning voter privacy is precisely the type of "concrete and demonstrable injury to" EPIC's "organizational activities" that courts have long deemed sufficient for standing. *Havens*, 455 U.S. at 379; *see also PETA*, 797 F.3d 1087 (holding that a non-profit animal protection organization had standing under *Havens* to challenge the USDA's failure to promulgate bird-specific animal welfare regulations); *Abigail All. for Better Access to Developmental Drugs v. Eschenbach*, 469 F.3d 129 (D.C. Cir. 2006) (finding that a health advocacy organization had organizational standing under *Havens* to challenge an FDA regulation). EPIC has thus adequately demonstrated organizational standing.

Contrary to the Commission's assertions, EPIC has also demonstrated an injury in fact to its members which is traceable to the Commission's conduct. EPIC therefore has associational standing.

First, EPIC can assert associational standing on behalf of numerous EPIC members whose privacy is threatened by the Commission's unlawful collection of personal voter data. Voter Declaration of Kimberly Bryant, Ex. 1; Voter Declaration of Julie E. Cohen, Ex. 2; Voter Declaration of William T. Coleman III, Ex. 3; Declaration of Harry R. Lewis, Ex. 4; Voter Declaration of Pablo Garcia Molina, Ex. 5; Voter Declaration of Peter G. Neumman, Ex. 6; Voter Declaration of Bruce Schneier, Ex. 7; Voter Declaration of James Waldo, Ex. 8; Voter Declaration of Shoshana Zuboff, Ex. 9. As each of the above-named EPIC members has attested: "The disclosure of my personal information—including my name, address, date of birth, political party, social security number, voter history, active/inactive or cancelled status, felony

convictions, other voter registrations, and military status or overseas information—would cause me immediate and irreparable harm." *See* Voter Declarations, Exs. 1–9.

Second, EPIC's members will necessarily suffer injuries in fact if the Commission is allowed to carry out its plans. As EPIC has explained, the unlawful collection and aggregation of state voter data, standing alone, constitutes an injury in fact. Pl. Mem. 17; *Council on Am.-Islamic Relations v. Gaubatz*, 667 F. Supp. 2d 67, 76 (D.D.C. 2009) (holding that the wrongful disclosure of confidential information is a form of injury); *Hosp. Staffing Sols., LLC v. Reyes*, 736 F. Supp. 2d 192, 200 (D.D.C. 2010) ("This Court has recognized that the disclosure of confidential information can constitute an irreparable harm because such information, once disclosed, loses its confidential nature."). Though it is unlawful for the Commission to obtain voter data without (1) conducting a PIA and (2) adhering to constitutional strictures on the collection of personal information, that is *precisely* what the Commission promises to do—and by a date certain (July 14). The injuries to EPIC's members are thus "certainly impending." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 (2013). The Government cannot confidently assert that it will do something yet dismiss the inevitable result as pure "speculati[on]." Def. Opp'n 6.

Third, the Commission's characterization of the data it seeks ("publicly available") is meaningless in the Article III standing context. The Commission has no legal authority to collect the personal voter data it has requested. *See* § 3501 note. If it nevertheless collects that data, the Commission has broken the law and caused an injury in fact. *See CAIR*, 667 F. Supp. 2d at 76; *Hosp. Staffing Sols*, 736 F. Supp. 2d at 200. It does not matter that a particular state might disclose its voter data to some *other* requester under some *other* circumstances: *this* requester—the Commission—is barred by law from gathering this data without sufficient constitutional and

statutory privacy safeguards. Nor can the Commission use the existing vulnerability of voter data at the state level to justify an even greater risk to voter privacy at the federal level. Def. Opp'n 7. A lesser harm does not excuse a greater one, and it certainly does not erase an injury in fact.

This Court consequently has jurisdiction to decide this case under Article III.

CONCLUSION

Plaintiff has satisfied the necessary elements to obtain the relief sought and has standing to bring this claim. Plaintiff specifically asks this Court to issue a Temporary Restraining Order to maintain the status quo so that this Court may have the opportunity to determine whether the Commission's proposed collection of personal voter data is lawful.

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

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

Dated: July 6, 2017